Satellite Network Hacking & Security Analysis

Adam Ali.Zare Hudaib *adamhudaib@gmail.com*
Licensed Penetration Tester | *EC-Council*
Certified Ethical Hacker | *EC-Council*
Certified Security Analyst | *EC-Council*
Certified Network Analyst | *WireShark University*
Information & Cyber Security Expert
CEH , ECSA , LPT , WCNA
Switzerland

Abstract

Satellites play a significant role in communication, early warning systems, global broadcasting, meteorology, navigation, reconnaissance, remote sensing, and surveillance.Satellite services cover practically every sector, from mobile cellular communication to telemedicine, so any interference with them could have a serious effect. Satellites are a strategic asset for any country and are considered as “critical infrastructure,” therefore they are considerable as privileged targets for a possible cyber attack.

Keywords: Satellite Network, Satellite Communications, Satellite Network Security, Satellite Network Treats, Satellite Network Vulnerabilities, Satellite Security Analysis, Satellite Hacking.

1. INTRODUCTION

Satellites have assumed a crucial role in our contemporary society; they are used in both private and public sectors for numerous purposes, from communication to research.

Satellites provide many significant services, including communication, navigation, remote sensing, imaging, and weather and meteorological support. Satellites support direct radio communication and provide television broadcast and cable relay services, as well as home reception. Satellite services also support applications such as mobile and cellular communication, telemedicine, cargo tracking, point-of-sale transactions, and Internet access. Satellites also provide redundancy and backup capabilities to ground-based communications.

Unfortunately, with the diffusion of this complex system, the interest of governments and hackers also increased; their security is today a pillar of the cyber security strategy of the most advanced government. The wave of cyber threats has evolved rapidly in the last years in the pace of technological evolution.

This paper introduce such questions of the satellite network and communications security analysis: satellite network architecture operation design and technologies, satellite network treats and security analysis, satellite network vulnerabilities, satellite network hacking and satellite cybercrime statistics.

2. SATELLITE NETWORK SECURITY

This chapter describes the technical fundamentals of satellite networks; examines security vulnerabilities; and explores initiatives for protecting the integrity of satellite network transmissions and operations from cyber incursions and physical attacks.

2.1 Satellite network architecture operation design and technologies

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. TT&C ground stations "perform tracking and control functions to ensure that satellites remain in the proper orbits… and to monitor their performance [1;21].

Communications ground stations process imagery, voice, or other data and provide, in many cases, a link to ground-based terrestrial network interconnections". These ground-based terrestrial network interconnections communicate to and from the communications ground station but not directly to the satellite [1;21].

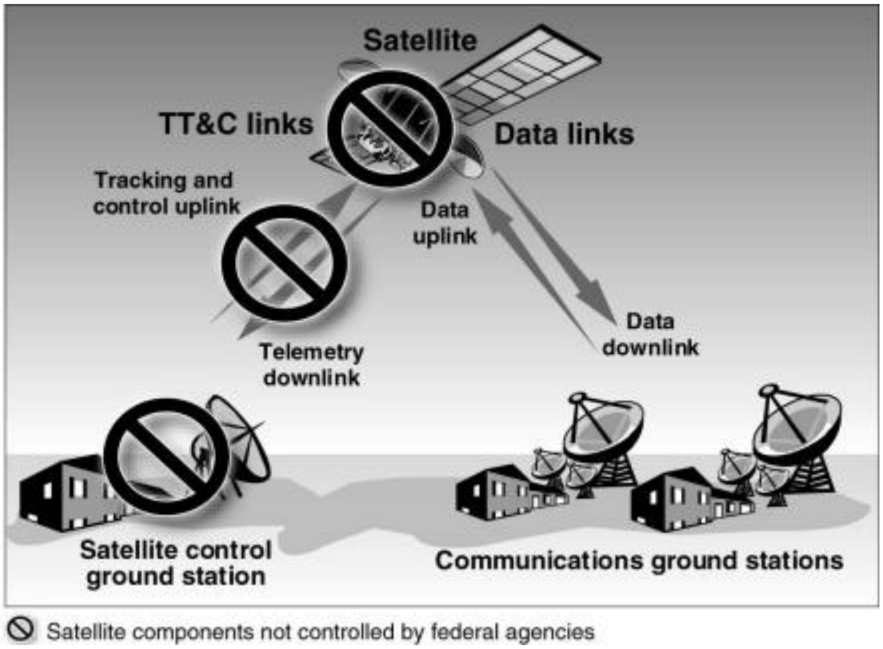

Satellite
TT&C links
Data links
Tracking and control uplink
Data uplink
Data downlink
Telemetry downlink
Satellite control ground station
Communications ground stations
⃠ Satellite components not controlled by federal agencies

FIGURE 1: Setellite Components [1;22].

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" [3]. 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 [1;22].

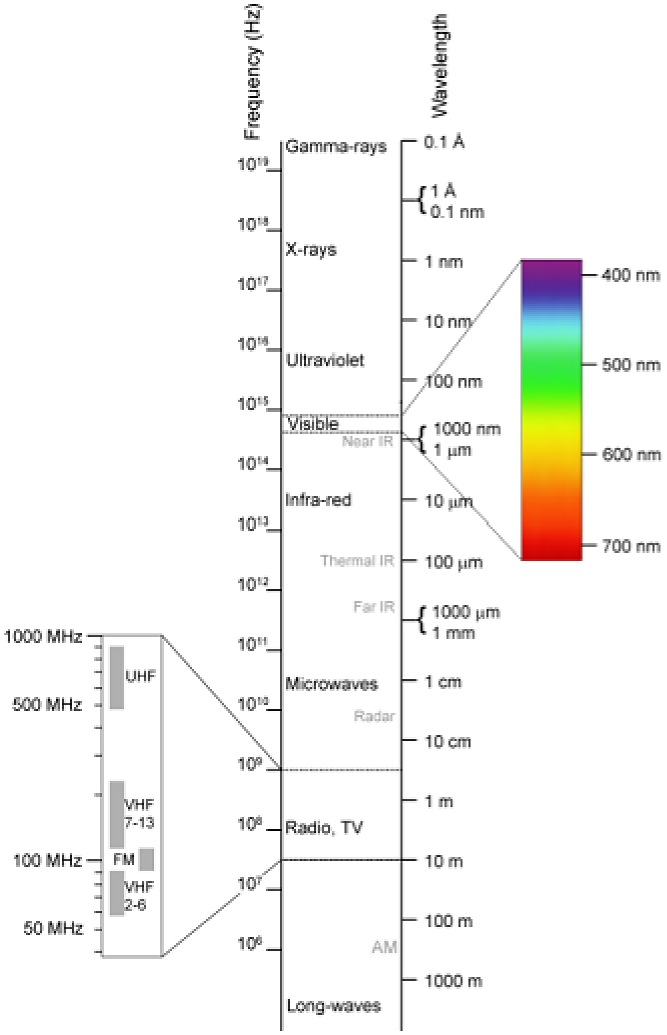


FIGURE 2: The predominant means of satellite transmission (radio and microwave signals) [1; 22].

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 [1;23].

For surveillance or weather satellites, geosynchronous orbits provide 24 hour coverage of a target. Nongeosynchronous satellites can obtain 24 hour access to downlinks by means of relay links (or crosslinks) 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". Different states have similar optimal orbits they seek to obtain, which often overlap with other state's interests [1;23].

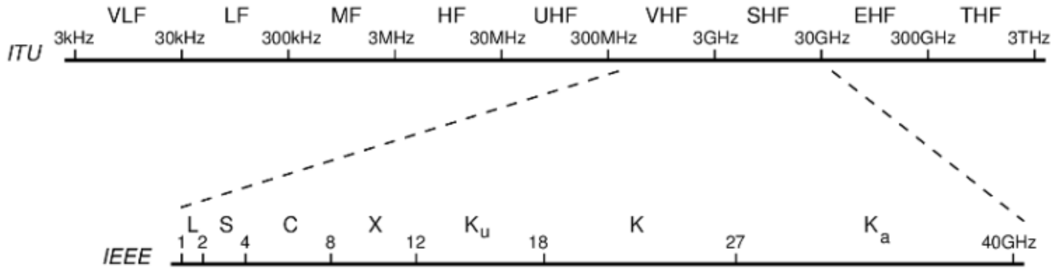


FIGURE 3: [1;23].

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. 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 [1;23-24].

*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. [1;24].*

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. 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 *[1;24].*

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. 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. In this way, a hub is comparable to a TT&C ground station *[1;24].*

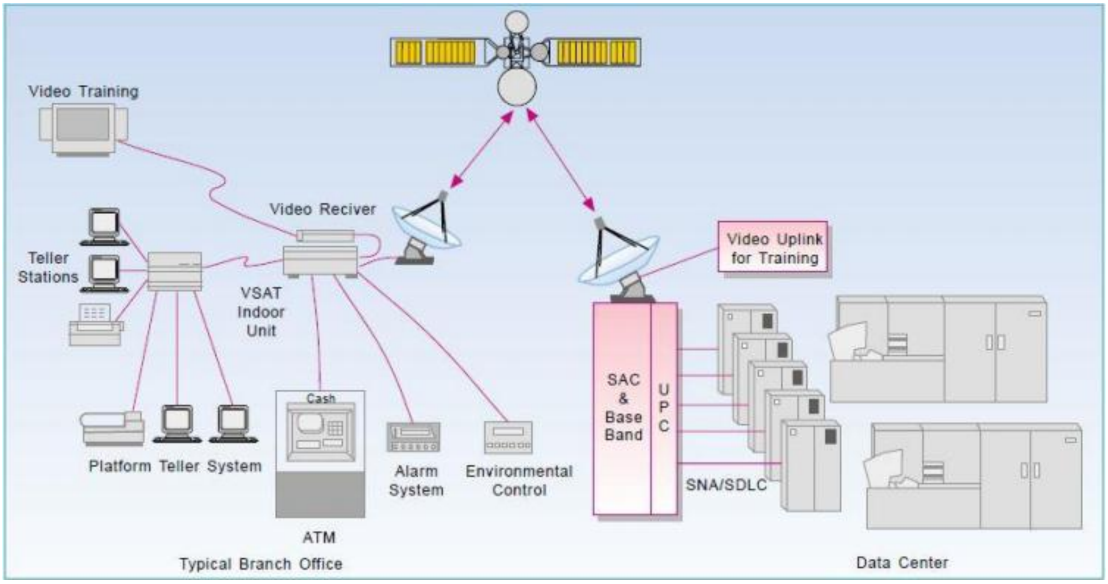


FIGURE 4B An example of a VSAT network in a Banking Environment *[1;25]*.

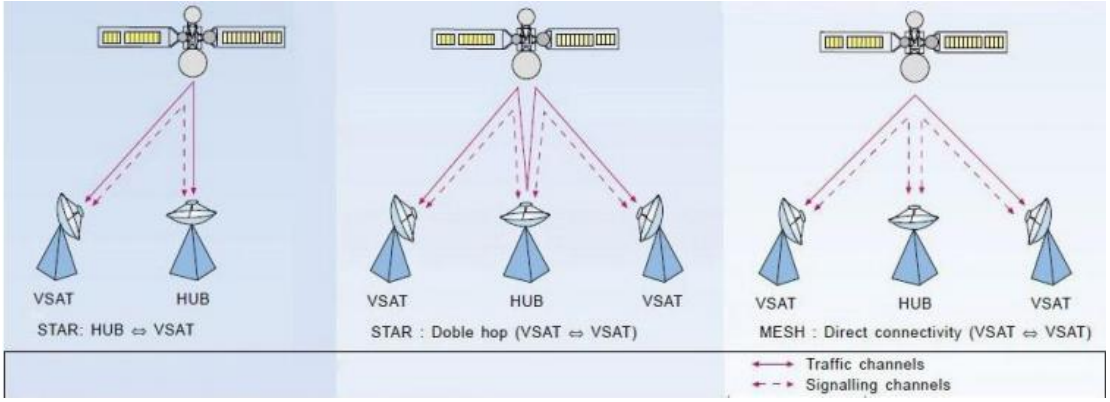


FIGURE 5: VSAT System Topologies *[1;25].*

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. 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. An increase in unsecure data being transmitted via satellites may pique the interest of hackers *[1;25].*

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 [14]. 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 *[1;25].*

2.2. Satellite network treats & security analysis

Security expresses the analysis of threats and solutions in a integral manner, defining policies, procedures and hardware and software solutions to ensure an optimal level of support, maximizing the use of resources and protecting the highest level of information.

Security services are the procedures and mechanismsused to secure the possible identified threats. The security services globally accepted are: authentication, integrity, nonrepudiation, access control, availability and privacy.

Redundancy

Redundancy is one security measure against disruption of service. For GPS there is currently a constellation of 31 satellites in orbit, roviding 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- ide, and/or the off-line ground station, can take over *[1;26].*

Changing the formation of a network of satellites, or engaging secondary systems, to compensate for a disruption can even be set to engage autonomously. 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 *[1;26].*

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" [3]. 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 *[1;26].*

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 [1;26].

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. 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 [1;27]. :

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* [1;27].

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”. As with hardening the other nodes in a satellite network, the major drawback is increased cost [1;27]:

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[1;27].

Enhanced manoeuvring and stealth capabilities of satellites, an emerging area of defensive capacity, can also be placed under the category of hardening [1;27].

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” [1;28].

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. “[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”. 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 [1;28].

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. 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 [1;29].

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" [3]. 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 [1;30].

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 [1;30]. *.*

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 [1;30]. .

2.3 Satellite Network Threats

Threats Both the ground-segment and the space-segment nodes are tied together by information conduits called links. These links are identified as control or mission links. Control links command the satellite and its sensors. Mission links describe the operational data transmitted to or from the satellite. These links are vulnerable to multiple types of electronic attack.

Electronic Attack

Electronic attack is defined as any action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack an adversary [19]. US space systems could be functionally neutralized by jamming and/or spoofing.

Jammers usually emit noise-like signals in an effort to mask or prevent the reception of desired signals. All military and commercial satellite systems are susceptible to uplink and downlink jamming. In either case, the jammer must operate in the same radio band as the system being jammed. Uplink jammers on the ground must be roughly as powerful as the ground-based emitter associated with the link being jammed. However, ground-based downlink jammers can often be much less powerful and still be effective. Since most satellites rely on uplinked command and control information from the ground for station keeping, payload management, and satellite health and status, attacking a satellite's uplink during critical commanding periods could seriously degrade mission performance. The effectiveness of electronic jamming, however, is limited because of line-of-sight restrictions and increased satellite autonomy. Therefore, attacking the downlink is usually easier and more reliable [20].

Uplink Jamming

There are two types of satellite uplink signals: signals for retransmission (payload signals such as TV and communications) and the command uplinks to the satellite. Uplink jamming against a payload signal is an attractive EA strategy because all recipients of the target transmission are affected. The jamming uplink signal is a radio frequency (RF) signal of approximately the same frequency as the target uplink signal. It is transmitted up to the satellite onto the same transponder as the target signal and affects the transponder’s ability to distinguish the true signal from the jamming signal. Note that the target uplink source and signal are not affected; the inability of the satellite’s transponder to distinguish between the signals results in a loss of downlink or corrupted downlink. The effectiveness of uplink jamming is extremely dependent on obtaining detailed information on the target signal. This can be done through formal signals intelligence (SIGINT) processes or (in some cases) open-source intelligence (OSINT) research. Once this is gathered and analyzed, the uplink jamming source must be able to acquire the proper satellite and transponder, as well as produce a signal with the correct characteristics and power necessary to overcome the signal to be jammed.

Targets of uplink jammers are the satellites’ radio receivers, including their sensors and command receivers. Uplink jamming is more difficult, since considerable jammer transmitter power is required. However, its effects may be global, since the satellite or space system could be impaired for all users.

Downlink Jamming

There are two main targets for downlink jamming: SATCOM broadcasts and navigation satellite (NAVSAT) broadcasts. In a downlink jamming scenario, the objective of the EA is to disrupt or temporarily keep the spacecraft’s transmission (communication or navigation signal) from being received by select ground users. A downlink jamming system accomplishes this by broadcasting an RF signal of approximately the same frequency as the targeted downlink signal but with more power. This jamming signal is transmitted toward a terrestrial (ground-based) or airborne satellite downlink reception antenna where it overpowers the satellite’s signal. With smart jamming (vice bruteforce jamming), the jamming signal attempts to emulate the satellite’s signal and, if successful, can provide the targeted user with false data or information. The effectiveness of downlink jamming is dependent upon the jammer being able to operate within line of sight (LOS) of the ground site and within the field of view of the ground site’s antenna; effectiveness is also dependent upon the jamming signal being processed by the SATCOM receiver. LOS restrictions can be overcome to a degree by utilizing an airborne platform; the altitude gained by the airborne platform expands the coverage and aids in overcoming ground-based obstacles. It is difficult to assess the effectiveness of downlink jamming as this normally requires monitoring the output of the targeted receiver (often not possible).

The targets of downlink jammers are ground-based satellite data receivers, ranging from large, fixed ground sites to handheld GPS user sets. Downlink jamming only requires a very low-power jammer, though its effects are local (from tens to hundreds of miles, depending on the power of both the jammer and downlink signal). Since downlink telemetry contains the mission information and health and status information, successfully attacking the downlink directly attacks information flow and, therefore, has a more immediate effect on denying or disrupting the satellite’s mission [20].

Sophisticated technologies for jamming satellite signals are emerging. For example, Russia markets a handheld GPS jamming system. A one-watt version of that system, the size of a cigarette pack, can deny access to GPS out to 50 miles; a slightly larger version can jam up to 120 miles [21].

Spoofing

Spoofing is the ability to capture, alter, and retransmit a communication stream in a way that misleads the recipient [158]. Attacking the communication segment via spoofing involves taking over the space system by appearing as an authorized user. Once established as a trusted user, false commands can be inserted into a satellite’s command receiver, causing the spacecraft to malfunction or fail its mission. Spoofing is one of the most discreet and deniable forms of attacking our space systems [21].

2.4 Satellite Network Vulnerabilities

Satellites' transmissions are subject to lengthy delays, low bandwidth, and high bit-error rates that adversely impact real-time, interactive applications such as videoconferences and lead to data corruption, performance degradation, and cyber incursions. Atmospheric and interstellar noise; cosmic radiation; interference from electronic devices; and precipitation and rain absorption in the spectral frequencies employed by satellites impede network performance and information throughput and negatively affect provision of quality of service (QoS) guarantees [22].

Satellite network applications and services are also adversely impacted by geophysical events. In 1998, for example, tremendous explosions on the sun disrupted operations onboard PanAmSat's Galaxy IV Satellite. As a consequence of these solar flares, digital paging services, bank transactions, and cable television programs across the U.S. were disabled [22].

According to the U.S. GAO (2002), satellite network functions can be compromised by ground-based antisatellite weapons, high-altitude nuclear explosions, stealth micro satellites, space mines, space-to-space missiles, and directed energy space weapons. For instance, as a consequence of intentional jamming resulting from cyber attacks on a Telestar-12 commercial satellite in 2003, U.S. governmentsupported broadcasts promoting regime changes in Iran were blocked by the Iranian Ministry of Post, Telegraph, and Telephone [22]. Satellite-based telephony services in Tehran were also disabled.

Satellite network operations are subject to denial of service (DoS) and distributed DoS (DDoS) attacks generated by automated tools that prevent authenticated users fro accessing network services; the spread of viruses to mobile satellite-enabled appliances such as cellular phones; worms that self-propagate malicious data; and spy ware that enables intruders to gain unrestricted access to classified documents [22] as well. denial of information (DoI) attacks on satellite networks such as spam or unsolicited commercial e-mail and phishing or transmission of fraudulent e-messages are typically designed to deceive legitimate users into revealing confidential information to unauthorized sources [22].

Satellite networks are also vulnerable to cyber terrorism or coordinated space-based and ground-based threats and attacks committed by unlawful and/or politically motivated terrorist groups who target critical communications systems such as satellite networks to cause data corruption, disruption of critical infrastructure services, economic damage, harm, and loss of life [22]. Satellite network attacks attributed to cyber terrorismcan result in disruptions in financial markets and disclosure of government, law enforcement, medical, and/or military classified data [22].

Intentional satellite system incursions motivated by cyber terrorismraise questions about the dependability, reliability, availability, and security of satellite network services and erode public confidence in the integrity of satellite-dependent, critical infrastructure applications [22].

Vulnerable Software

While kinetic dangers (i.e., being hit and/or damaged by stray objects such as meteorites or other satellites) remain rare, satellite systems are remarkably vulnerable to a range of cybersecurity issues and hostile attacks because they are hugely complex and expensive, take months to deploy, and the primary emphasis is on getting a working system that meets specification and the contract deliverables.

Most cyber exploit attacks take advantage of incomplete code that does not boundary check incoming data allowing for stack buffer overflow attacks. These are very prominent in embedded C and C++ systems and require an additional vulnerability assessment exercise, at great cost and time, in order to fully secure a system. In these cases an internal buffer may be overrun by an intentionally 'malformed' packet and code execution achieved by overwriting the area of memory where the return address resides. Once basic code execution is achieved, new threads and processes may be started and most, if not all, facilities within the system can be accessed [23].

Encryption
Encryption primarily ensures that the traffic through a satellite system cannot be overheard. For the most secure environments, the encryption is achieved outside of the actual satellite channels. Where encryption has been used on the satellite channels there are some examples where that encryption is so weak that it as been easily exploited.

Hard-coded Credentials And/Or Backdoors
Hard-coded credentials function as cybersecurity master keys, common back doors that allow service technicians to access multiple pieces of equipment with the same log-in credential and password.

Insecure Protocols
Weak system protocols could allow malicious actors access to satcom channels. Although, in most cases, care has been taken regarding the security of the protocol being used, there is invariable weakness that can be exploited [23].

Vendor	***Product***	***Vulnerability Class***	***Service***	***Severity***
Harris	RF-7800-VU024 RF-7800-	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical

Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

TABLE 1: Summary of Vulnerabilities.

Table 1 summarizes the types of vulnerabilities.

Vulnerability Classes

Backdoors
Mechanisms used to access undocumented features or interfaces not intended for nd users.

Hardcoded Credentials
Undocumented credentials that can be used to authenticate in documented interfaces expected to be available for user interaction.

Insecure Protocols
Documented protocols that pose a security risk.

Undocumented Protocols
Undocumented protocols, or protocols not intended for end users, that pose a security risk.

Weak Password Reset
Mechanism that allows resetting other's passwords [24;8].
Attack Scenarios Against Harris BGAN Terminals

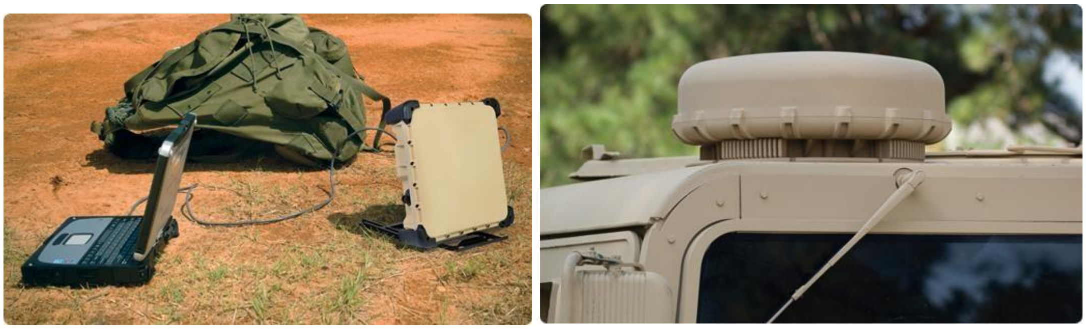


FIGURE 6: Land Portable and Land Mobile Harris BGAN Terminals.

Both land portable and land mobile Harris BGAN terminals are intended for use by the military sector. The main purpose of these terminals, such as the RF-7800B, is to provide enhanced tactical radio network capabilities. They are used in conjunction with software-defined radios (SDRs), such as the FALCON III® AN/PRC-117G SDR shown in Figure 7.

FIGURE 7: AN/PRC-117G SDR.

When the RF-7800B BGAN terminal is combined with the AN/PRC-117G SDR, the terminal operates simultaneously with the ANW2 waveform, providing beyond-line-ofsight (BLOS) communications. The system provides range extension of ANW2 networked data.

Harris' documentation contains a practical example:
For example, consider an attack on a convoy in the mountains. Such an event requires an immediate reaction from many different units. Previously, this response was pieced together through fragmented systems.

By leveraging a network of AN/PRC-117G radios, commanders would be able to launch and coordinate an immediate response using some or all of the following applications:

- Streaming video: Commanders would be able to analyze reconnaissance feeds from cameras, both on the ground and in their air, to plan their response.
- Legacy interoperability: Quick Reaction Force teams would be able to call for close-air support for a counter attack.
- Text messaging: Convoy personnel would be able to send details via text messaging, limiting confusion and removing traffic from voice networks.
- Satellite communications: The radio will support reach-back capability through satellite communications to connect warfighters to brigade headquarters."

This example matches Harris' tactical scema, shown in Figure 8 [24; 9].

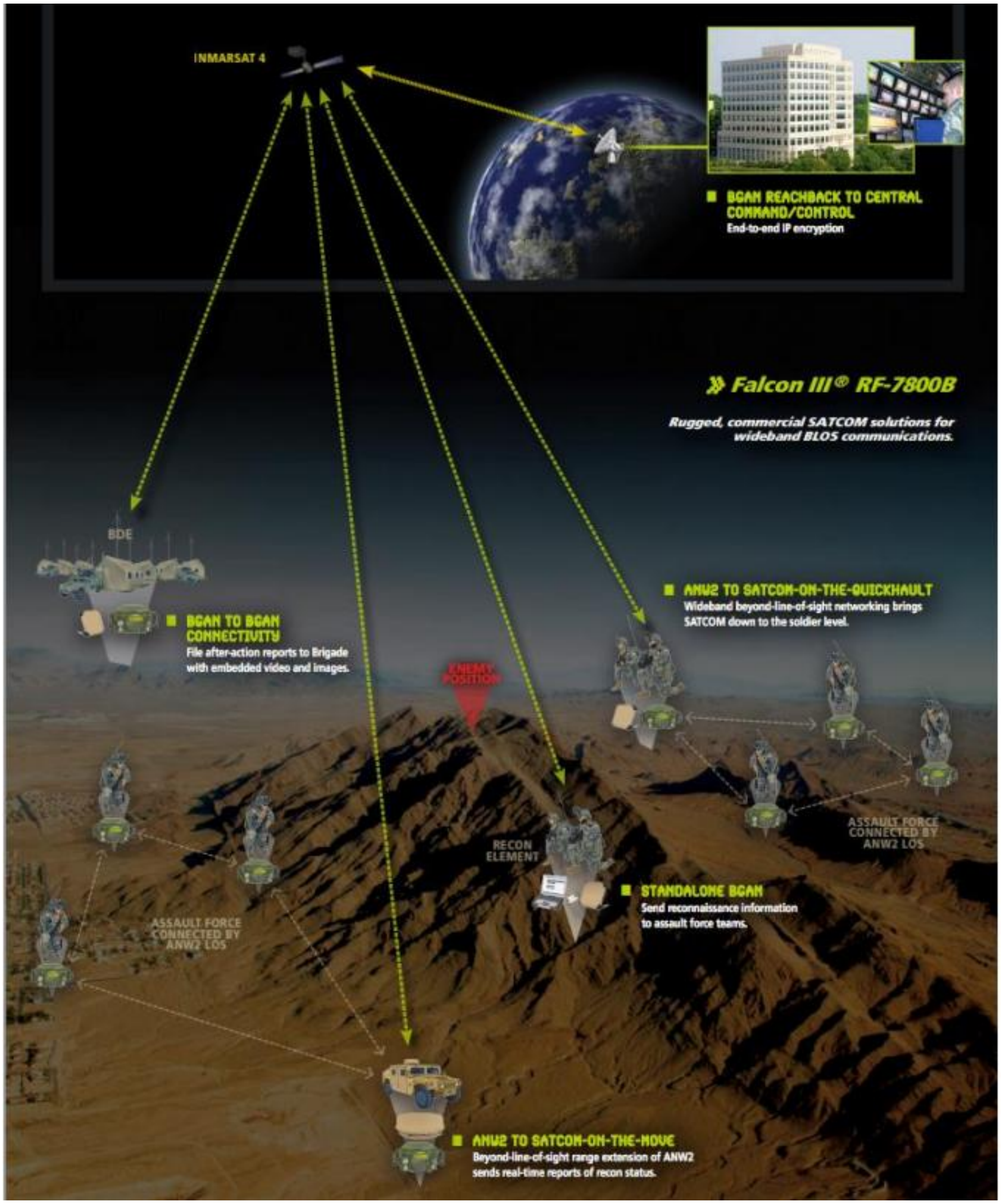

INMARSAT 4
BGAN REACHBACK TO CENTRAL COMMAND/CONTROL
End-to-end IP encryption
Falcon III® RF-7800B
Rugged, commercial SATCOM solutions for wideband BLOS communications.
BDE
BGAN TO BGAN CONNECTIVITY
File after-action reports to Brigade with embedded video and images.
ANW2 TO SATCOM-ON-THE-QUICKHAULT
Wideband beyond-line-of-sight networking brings SATCOM down to the soldier level.
ENEMY POSITION
RECON ELEMENT
STANDALONE BGAN
Send reconnaissance information to assault force teams.
ASSAULT FORCE CONNECTED BY ANW2 LOS
ASSAULT FORCE CONNECTED BY ANW2 LOS
ANW2 TO SATCOM-ON-THE-MOVE
Beyond-line-of-sight range extension of ANW2 sends real-time reports of recon status.

FIGURE 8: Harris' Tactical Schema.

The vulnerabilities IOActive found in the RF-7800B terminal allow an attacker to install malicious firmware or execute arbitrary code. A potential real-world attack could occur as follows:

1. By exploiting the vulnerabilities listed in Table 1, an attacker injects malicious code into the terminal. Malware running on an infected laptop connected to the terminal, as shown in Figure 9, could deploy this payload.
2. The malicious code uses the built-in GPS to obtain the coordinates where the system is located. This would allow the attacker to compare the system's position with a fixed area (target zone) where an attack from enemy forces is planned.
3. If a Packet Data Protocol (PDP) context is detected or the system enters the target zone, the malicious code disables communications or even damages the terminal.

4. The ability of the victims to communicate vital data or ask for support to perform a counter-attack is limited or even cut off. In the worst-case scenario, loss of lives is possible.

This kind of equipment is common within the forces of the North Atlantic Treaty Organization (NATO) [24; 11].

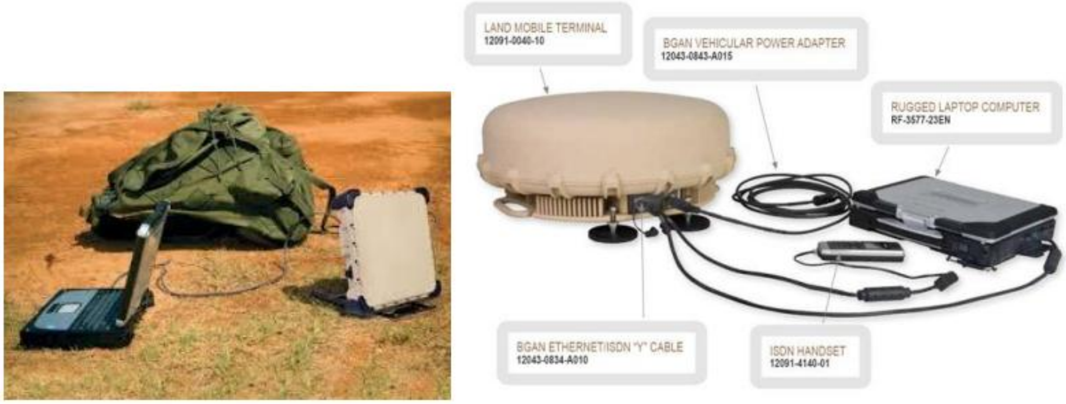


FIGURE 9: System Components, Including Laptop.

Attack Scenarios Against Hughes BGAN M2M Terminals

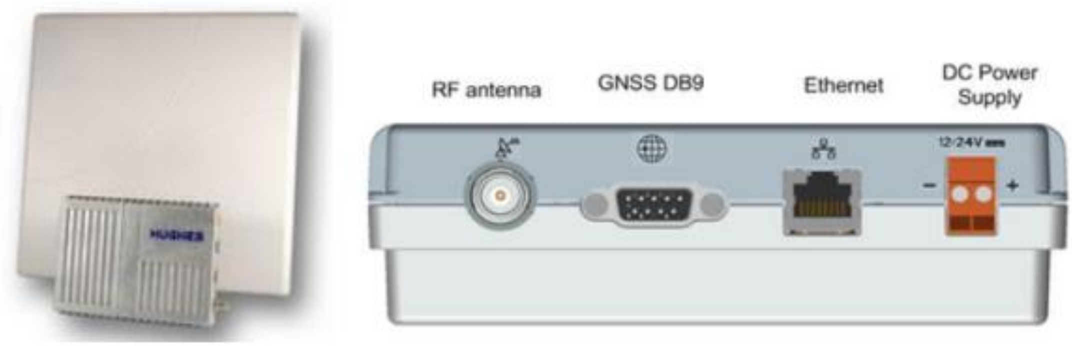


FIGURE 10: Hughes 9502 BGAN M2M Antenna and Indoor Unit.

According to Hughes' BGAN M2M Operational Scenarios document, the satellite user terminal (UT) can be controlled remotely via SMS messages or AT commands as shown in Figure 11 and Figure 12.

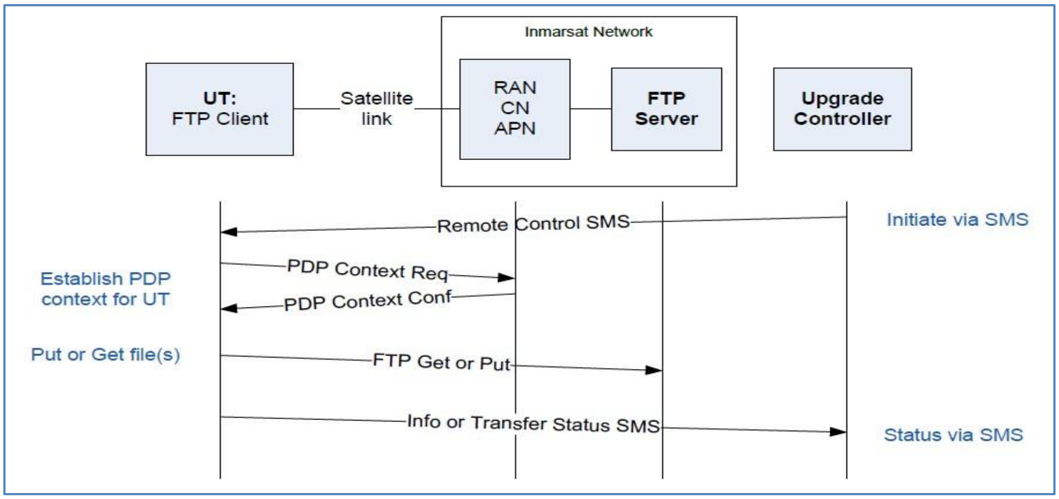


FIGURE 11: Remote Control of the Hughes BGAN M2M UT via SMS.

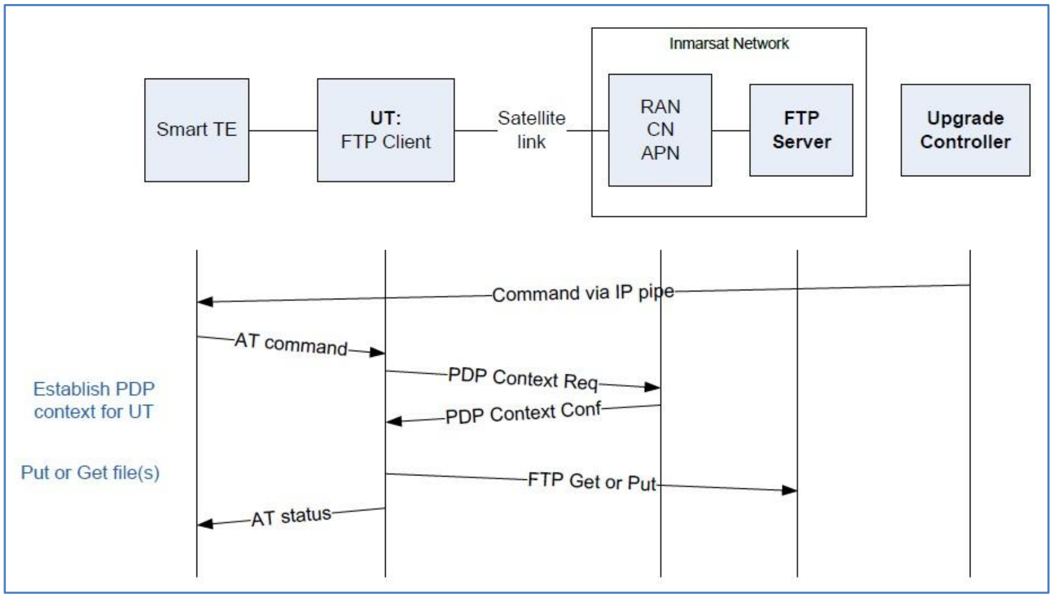


FIGURE 12: Remote Control of the HUGHES BGAN M2M UT via AT Commands.

As Figure 12 illustrates, AT commands can be sent using Smart Terminal Equipment (TE) controlled via the IP pipe over the PDP context.

The following two scenarios describe how an attacker could compromise the UT by exploiting the vulnerabilities listed in Table 1.

Scenario One

An attacker with access to the Smart TE, either directly or via malware, could exploit the ‘admin code’ backdoor when ‘Enhanced Security’ is activated. The attacker could also leverage the undocumented ‘Zing’ protocol.

Scenario Two

An attacker already knows the Mobile Subscriber Integrated Services Digital Network-Number (MSISDN) and International Mobile Station Equipment Identity (IMEI) of the UT. By generating the backdoor ‘admin code’, an attacker can send an SMS containing an encapsulated AT command to install malicious firmware.

According Inmarsat’s Channel Sales presentation, the Hughes 9502 BGAN M2M is deployed in six target markets: smart grid, SCADA, pipeline monitoring, well head/pump monitoring and control, remote ATM/POS, and environmental monitoring.

A successful attack against Hughes BGAN M2M terminals can have the following impacts:

- Fraud
- Denial of service
- Physical damage
- Data spoofing [24; 112-113]

Attack Scenarios Against Cobham BGAN Terminals

More than two-thirds of the Inmarsat satellite terminals currently in use belong to the Explorer family, manufactured by Cobham (formerly Thrane & Thrane). An attacker can take complete control of these devices by exploiting a weakness in their authentication mechanism using either direct access or scripted attacks (malware).

Cobham Explorer terminals are deployed in multiple sectors. Attacks against these communication devices would have different impacts depending on the specific application. The following images below come from the documentation that vendors and integrators provide to illustrate case studies.

FIGURE 13: Military Use.

FIGURE 14: Emergency Services and Field Operations.

FIGURE 15: Life Saving Equipment.

FIGURE 16: Personal Communications for the Military.

Scenario: Personal Communications for the Military as Attack Vector Historically, tracking the position of military units has provided the adversary with vital information about the units' objectives and tactical approach. If a member of a unit was targeted with a client-side exploit while browsing the Internet during personal communications time, an attacker would be able to install malicious firmware in the terminal. The attacker's code could then take advantage of the terminals' built-in GPS receiver to leak its position in real-time [24; 116].

There have been significant examples of this kind of exposure:

- US Army: Geotagged Facebook posts put soldiers' at risk
- The Israeli military cancelled a planned raid on a Palestinian village after one of its

soldiers posted details of the operation on Facebook

Attack Scenarios Against Marine VSAT and FB Terminals

FIGURE 17: Cobham SAILOR 900 VSAT and JRC JUE-250 FB Terminals.

The Cobham SAILOR 900 VSAT, Cobham Sailor FB and JRC JUE-250/500 FB terminals are both deployed on ships as part of a satellite communication system or an Inmarsat FB system, as shown in Figure 18.

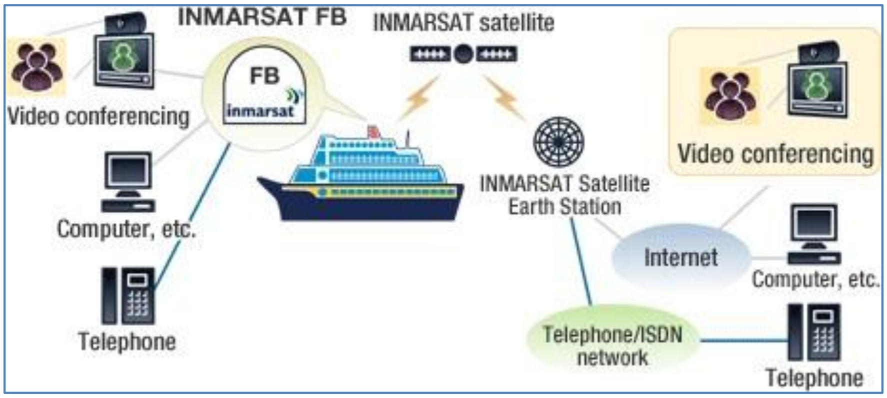


FIGURE 18: Inmarsat FB System.

- Numerous services use the satellite link:
- Telephone, ISDN, SMS, and VoIP
- Broadband Internet
- Email and file transfer
- Multi-voice
- Video conferencing
- Safety 505 and red button
- Notice to mariners
- Maritime/port regulations
- ECDIS
- Vessel routing
- Cargo management
- Planned/Predictive maintenance
- Radio over IP (RoIP) via walkie-talkie
- VHF/UHF radio integration
- Crew welfare
- Telemedicine
- Tele-training/certification

- Weather forecasts

Compromising one of these terminals would give an attacker full control over all of the communications that pass through the satellite link.

Scenario One: Navigation Charts

The vulnerabilities in these terminals make attacks that disrupt or spoof information consumed by the on-board navigations systems, such as ECDIS, technically possible, since navigation charts can be updated in real time via satellite.

Scenario Two: Operational Integrity

The ability to control the satellite link of a vessel can be used to put the operational integrity of cargo vessels at risk. SATCOM links are often used to track the status and condition of container ships while in transit. This is especially important when transporting sensitive goods such as munitions or hazardous chemical products.

The operational information enables the cargo's owner to take proper action and address any potential situation [24; 116].

Attack Scenarios Against Cobham AVIATOR

The Cobham AVIATOR family is designed to meet the satellite communications needs of aircraft, including those related to safety operations. Figure 19 illustrates a US military aircraft equipped with this product.

FIGURE 19: US Air Force C-130J Super Hercules.

Aircraft safety is highly dependent on the redundancy and accuracy of on-board systems. When it comes to aircraft, software security is not an added value but a mandatory requirement. International certification authorities provide a series of standards which represent the industry consensus opinion on the best way to ensure safe software, such as the Radio Technical Commission for Aeronautics (RTCA) specification DO-178B or the European Organization for Civil Aviation Equipment (EUROCAE) ED-12B.

These regulatory standards define five levels of failure conditions, categorized by their effects on the aircraft, crew, and passengers:

Level A–Catastrophic

Failure may cause multiple fatalities, usually with loss of the airplane.

Level B–Hazardous
Failure has a large negative impact on safety or performance, reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers.

Level C–Major
Failure significantly reduces the safety margin or significantly increases crew workload. May result in passenger discomfort (or even minor injuries).

Level D–Minor
Failure slightly reduces the safety margin or slightly increases crew workload. Examples might include causing passenger inconvenience or a routine flight plan change.

Level E–No Effect
Failure has no impact on safety, aircraft operation, or crew workload.
Software approved to levels A, B, or C requires strong certification involving formal processes for verification and traceability. Software approved to levels D or E is subject to a more ‘relaxed’ control.

Although the failure condition levels are intended to cover not only the software as a standalone entity, but also as part of a more complex system, some claim that there is room for improvement. The main concerns seem to be related to interactions between equipment at different levels.

IOActive was able to demonstrate that it is possible to compromise a system certified for level D that interacts with devices certified for level A, potentially putting the level A devices’ integrity at risk [24; 117].

The AVIATOR 700 system is available in two versions:

- AVIATOR 700 approved to RTCA specification DO-178B level E and DO- 254 level E
- AVIATOR 700D approved to RTCA specification DO-178B level D and DO- 254 level D

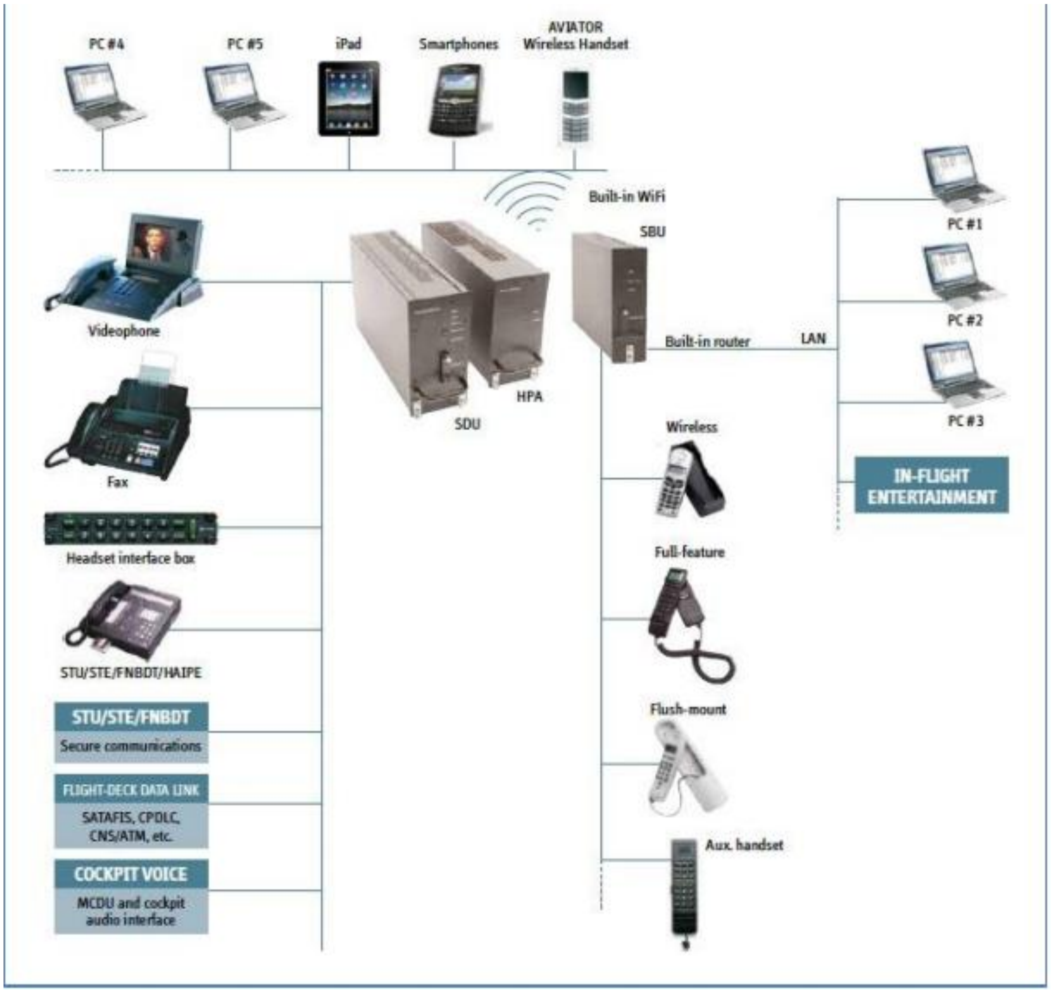
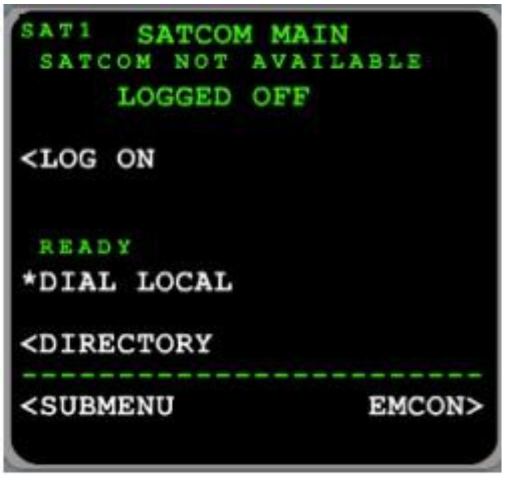


FIGURE 20: AVIATOR 700 System Interactions.

Both versions of the AVIATOR 700 operate in complex systems with multiple interfaces to other systems on board; however, only the AVIATOR 700D level D is approved for safety purposes.

The vulnerabilities listed in Table 1 could allow an attacker to take control of both the SwiftBroadband Unit (SBU) and the Satellite Data Unit (SDU), which provides Aero- H+ and Swift64 services. IOActive found vulnerabilities an attacker could use to bypass authorization mechanisms in order to access interfaces that may allow control of the SBU and SDU. Any of the systems connected to these elements, such as the Multifunction Control Display Unit (MCDU), could be impacted by a successful attack. More specifically, a successful attack could compromise control of the satellite link channel used by the Future Air Navigation System (FANS), Controller Pilot Data Link Communications (CPDLC) or Aircraft Communications Addressing and Reporting System (ACARS). A malfunction of these subsystems could pose a safety threat for the entire aircraft [24].



```
SAT1    SATCOM MAIN
 SATCOM NOT AVAILABLE
      LOGGED OFF

<LOG ON


 READY
*DIAL LOCAL

<DIRECTORY
-----------------------
<SUBMENU          EMCON>
```

FIGURE 21: The SDU (Level D) Interacts with the MCDU (Level A Component Present in the Cockpit).

Attack Scenarios Against Cobham GMDSS Terminals

GMDSS was briefly discussed in the description of Inmarsat-C services. The complete GMDSS regulation is defined in Chapter IV of the SOLAS convention. Under this international agreement, every GMDSS-equipped ship, while at sea, must be capable of:

- Transmitting ship-to-shore distress alerts by at least two separate and independent means, each using a different radio communication service
- Receiving shore-to-ship distress alerts
- Transmitting and receiving ship-to-ship distress alerts
- Transmitting and receiving search and rescue coordinating communications
- Transmitting and receiving on-scene communications
- Transmitting and, as required by regulation V/19.2.3.2, receiving signals for locating
- Transmitting and receiving maritime safety information
- Transmitting and receiving general radio communications to and from shore- based radio systems or networks subject to regulation 15.8
- Transmitting and receiving bridge-to-bridge communications

SOLAS establishes the type of radio communications systems that a ship needs, in order to be GMDSS compliant. This requirement depends on the ship's area of operation as illustrated in Figure 22 [24;3].

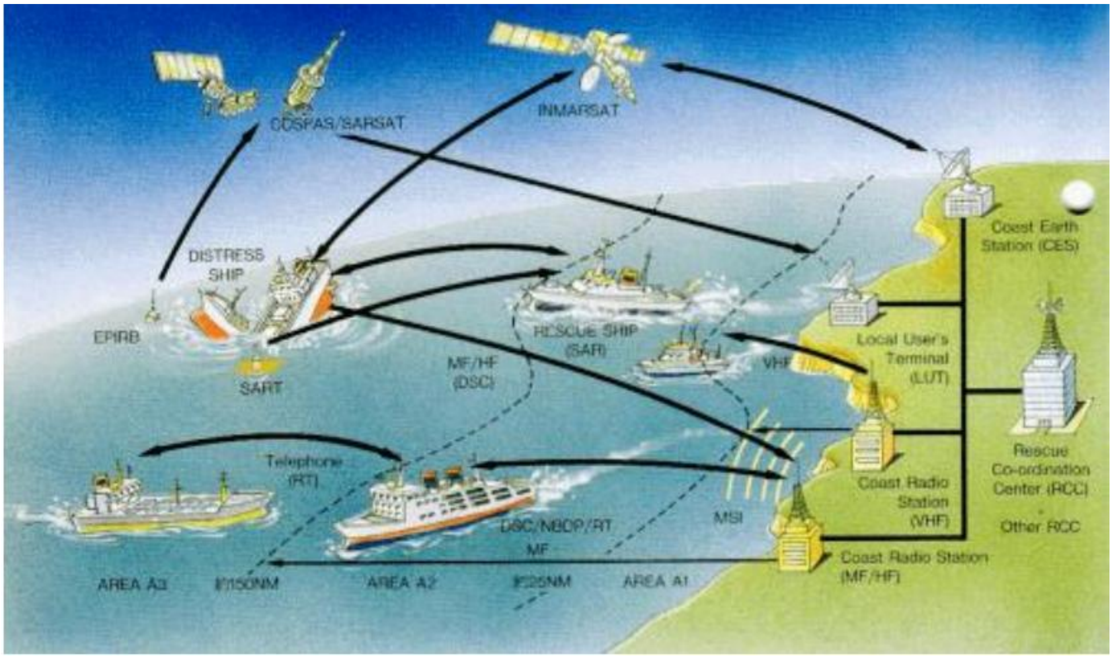


FIGURE 22: Sea Areas for GMDSS Communication Systems.

There are four sea areas:

- **A1** An area within the radio telephone coverage of at least one VHF coast station in which continuous DSC alerting is available (20–30 nautical miles)
- **A2** An area, excluding the previous one, within the radio telephone coverage of at least one MF coast station in which continuous DSC alerting is available (approximately 100/150 nautical miles).
- **A3** An area, excluding A1 and A2, within the coverage of an Inmarsat geostationary satellite in which continuous alerting is available.
- **A4** An area outside sea areas A1, A2, and A3.
- Cobham SAILOR 6000 is a GMDSS-compliant communications suite which provides the equipment specified by SOLAS.

The basic equipment includes:

- A VHF radio
- One SART if under 500 GRT, 2 SARTs if over 500 GRT
- Two portable VHF transceivers for use in survival craft if under 500 GRT, three if over 500 GRT
- A NAVTEX receiver, if the ship is engaged on voyages in any area where a NAVTEX service is provided
- An Inmarsat Enhanced Group Call (EGC) receiver, if the ship is engaged on voyages in any area of Inmarsat coverage where Marine Safety Information (MSI) services are not provided by NAVTEX or HF NBDP
- A 406 MHz Emergency Position-Indicating Radio Beacon (EPIRB) Additional equipment includes:

1SAILOR 630x MF/HF Control Unit
1 SAILOR 62xx VHF Radio

1 SAILOR 630x MF/HF Control Unit
1 SAILOR 62xx VHF Radio
1 SAILOR H1252B USB/Parallel Printer
1 SAILOR 6006 Message Terminal

1SAILOR 630x MF/HF Control Unit
1SAILOR 62xx VHF Radio
2 SAILOR H1252B USB/Parallel Printer
2 SAILOR 6006 Message Terminal

2SAILOR 630x MF/HF Control Unit
3SAILOR H1252B USB/Parallel Printer
3 SAILOR 6006 Message Terminal

IOActive found that the insecure ‘thraneLINK’ protocol could be leveraged to compromise the entire SAILOR 6000 communications suite, posing a critical threat to the ship’s safety. An attacker can install malicious firmware in order to control devices, spoof data, or disrupt communications.

The Ship Security Alert System (SSAS) is also impacted by the vulnerabilities IOActive discovered in the Inmarsat Mini-C terminal.

The SSAS is part of the International Ship and Port Facility Security (ISPS) code and contributes to the IMO's efforts to strengthen maritime security and suppress acts of terrorism and piracy. In case of attempted piracy or terrorism, the ship’s SSAS beacon can be activated and appropriate law-enforcement or military forces will be dispatched. Once a SSAS alert has been triggered, the following protocol is applied:

- Rescue Coordination Centers or SAR Points of Contact for the country code the beacon is transmitting are discreetly notified.
- National authorities dispatch appropriate forces to deal with the terrorist or pirate threat.
- As a result of the security flaws listed in Table 1, an attacker can remotely disable the SSAS by sending a series of specially crafted messages to the target ship. No user interaction is required.
- An attacker successfully exploiting any of the SSAS and GMDSS vulnerabilities may be able to:
- Provide false information to trick crew into altering routes
- Spoof or delete incoming communications such as Distress calls from other ships, weather warnings, or any other EGC message
- Render devices unusable, effectively disrupting communications and leaving a vessel without the ability to interact with the outside world
- Remotely disable safety systems before attacking a ship
- In the worst-case scenario, loss of lives is possible [24; 8].

Additional Satellite System Vulnerabilities
This section covers “additional” satellite system vulnerabilities.

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. 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 [1;40].

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. 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. 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”. A lack of training can result in existing security features being unused or improperly configured [1;41].

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”. 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”. 84% of military communications during Operation Iraqi Freedom were transmitted through commercial satellites [1;42]. 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 Stateowned 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 [1;42].

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. 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 [1;42].

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 [1;42].

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. Meanwhile the Australian government banned Chinese telecom giants from NBN contracts due to security concerns reportedly issued by ASIO [30]. 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. 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 [1;43].

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. Yet to limit information sharing and suppress technology would also be detrimental to advancement [1;43].

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. Other apps, like Orbitron, Satellite AR, Satellite Tracker, Satellite Finder, and SatFinder, encompass a greater range of satellites, like weather, and provide "frequency information". 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 [1;44].

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. 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. 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. 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". Military communications are exempt from the ITU Constitution, though they should observe measures to prevent harmful interference [1;44].

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". 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 antijamming 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. 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 [1;44].

The military doctrines of a growing number of states emphasize the use of space systems to support national security. 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”. 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". 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”. 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 [1;45]. .

2.5 Satellite Network Hacking

Further, due to their complexity, satellites and SATCOM systems are vulnerable to a range of hacks:

Denial of Service

A denial of service attack can occur in a number of ways, including ‘bricking’ the device, selective denial, denial based on position etc. These are the easiest hacks as most software vulnerabilities crash the device when exploited without too much trouble. In fact, it is the device crashing when ‘fuzzing’ a device that signals a vulnerability has been discovered.

Monitoring

Breaching a satellite’s communications channels enables hackers to access transmitted data due to the lack of sufficient encryption. In fact, a number of decryption packages that facilitate this illicit access are widely available for sale commercially, coming out of countries such as Russia, Israel and countries in the E.U.

NAT Pass-Through

Satellite modems generally are IP routers providing connectivity to various IT infrastructure on the LAN side of the terminal. With the built-in firewalls and NAT, there is protection in place to stop unauthorized access to the LAN side. However, once code execution is achieved on the terminal, these protections can be turned off and the NAT can by punched-through by outsiders, giving access to the LAN [23].

User Specific Data

All sorts of User specific data can be collected and sent back at the attackers’ convenience. This includes user logs, network credentials, connected nodes etc.

A popular IT security expert listed the following top 10 threats:

- Tracking – tracking over web data and software
- Listening – listening with the right equipment, frequencies, and locations
- Interacting – protocols and authentication used, radio transmissions need official license!
- Using – take over a bird or a TT&C [use payloads, make pictures, transmit something (DVB or radio)]

- Scanning/attacking – anonymous proof of concept in 2010 by Leonardo Nve Egea, scanning, DoS, and spoofing possible
- Breaking – old technologies used (X.25, GRE)
- Jamming – jamming well-known frequencies for satellites
- Mispositioning/Control – transponder spoofing, direct commanding, command reply, insertion after confirmation but prior to execution
- Grilling – activating all solar panels when exposed to sun, overcharging energy system
- Collisioning [34]

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 [35].

Jamming

The attacker floods or overpowers a signal, a transmitter, or a receiver, interfering with legitimate transmission.

Interference has become the primary cause of the impairment and degradation of satellite services. The hackers use a directed antenna to produce the interference, usually a specifically crafted signal having enough power to override the original transmitted signal. Satellite jamming is a hacking method often used to interfere with communication for distribution of media for censorship purpose. The two forms of satellite jamming are “orbital” and “terrestrial”.

In orbital jamming, the attacker sends a beam of contradictory signals directly toward a satellite via a rogue uplink station. The jamming signals are mixed with the legitimate signals, thus interfering with them. The jamming signals are able to override the legitimate transmission, blocking its transmission to the recipient [36].

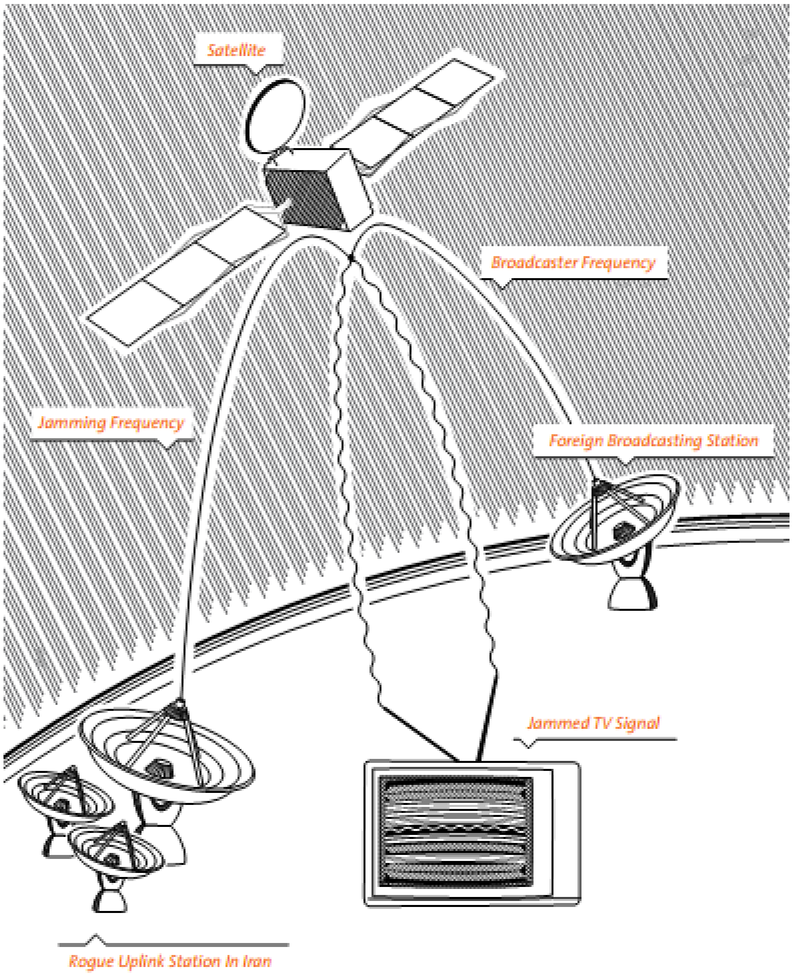


FIGURE 23: Orbital jamming.

In terrestrial jamming, the attacker transmits rogue frequencies in the direction of terrestrial targets (ground satellite dishes). Rather than targeting the satellite itself, as is the case in orbital jamming, terrestrial jamming involves transmitting rogue frequencies in the direction of local consumer-level satellite dishes. The jamming frequencies are limited to a specific area and are able to interfere only with the frequency emanating from the satellite in a specific location. Small, portable terrestrial jammers are easy to purchase and use; they typically have a range of 3-5 kilometers in urban areas, while in rural areas their range can increase to up to 20 kilometers.

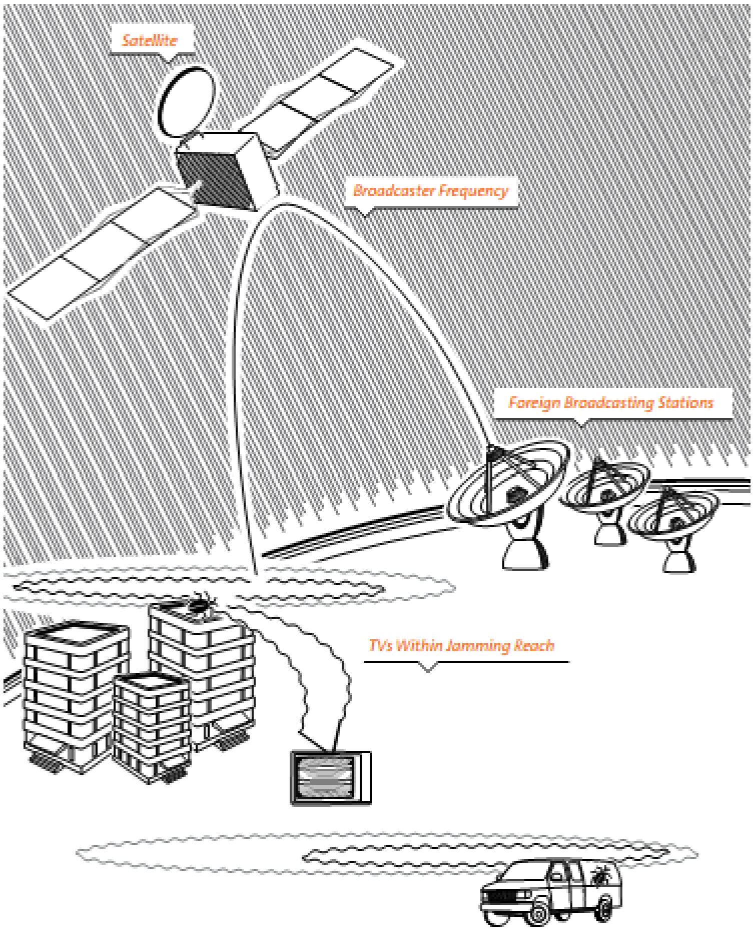


FIGURE 24: Terrestrial jamming.

The jamming attack could be directed against satellite receiving an uplink or against a ground station or user terminal receiving a downlink; the flooding of an uplink is considered the most damaging attack because it is able to saturate/destroy all possible recipients. Otherwise, jamming attacks against a terrestrial device could cause minor damages by impacting a limited portion of the satellite architecture, since downlink jamming is a reversible attack and it affects only users within line of sight of the jammer.Uplink jamming has relatively less impact because it can interfere with the transmission of a satellite over a broad area but only for a temporary period and it does not permanently harm the target system.The uplink jamming of the control link can prevent a satellite from receiving commands from the ground; it can also target user-transmitted data, thus disturbing the recipients. An uplink jammer must have at least the same power of the signal it is attempting to block and, during the attack, it must be located within the footprint of the satellite antenna it is targeting [36].

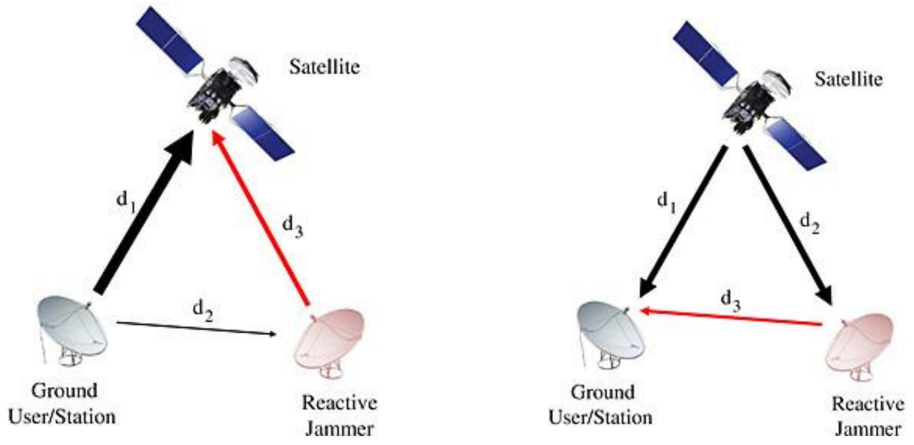


FIGURE 25: Uplink system diagram and Downlink system diagram.

The most concerning aspect of jamming attacks is that they can be undertaken using off-the-shelf technology and the detection and attribution of intermittent jamming can be difficult.

In general jamming “requires a directed antenna, knowledge of the frequency to be affected, and enough power to override its source”. 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 [2]. 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.

Timeline of Documented Jamming Incidents:
1995 Kurdish satellite channel, MED-TV, was intentionally jammed because it was believed to be promoting terrorism and violence [1;35].

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 [1;35].

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)”[1;35].

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 [1;35].

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 [1;35].

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" [1;35].

2004 The mobile, ground-based CounterCom system, designed to provide temporary and reversible disruption of a targeted satellite's communications signals, was declared operational [1;35].
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 [1;35].
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" [1;36].

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 [1;36].

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 [1;36].

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 [1;36].".

2007 Reports emerged that China had deployed advanced GPS jamming systems on vans throughout the country [1;36].

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) " [1;36].

2008 Landsat-7, a US earth observation satellite jointly managed by NASA and the US Geological Survey, "experienced 12 or more minutes of interference" [1;36].

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 [1;36].

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 [1;36].

2011 Libyan nationals jammed Thuraya satellites for more than six months in an effort to disrupt the activities of smugglers who use satellite phones [1;36].

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 [1;36].

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” [1;36].

2012 The Eritrean Ministry of Information accused the Ethiopian government of blocking transmissions from Eritrea’s state-run satellite television [1;36].

Eavesdropping

Differently from jamming, eavesdropping on a transmission allows an attacker to access transmitted data. Despite the fact that almost every satellite communication is encrypted, it is quite easy to read posts on the internet that describe how to use off-the-shelf products to intercept satellite transmissions whether they carry satellite broadcast media, satellite telephone conversations, or Internet traffic.

Quote:In early 2012 German security researchers demonstrated that satellite phones can be easily intercepted and deciphered using equipment readily available on the market, just a personal computer and an antenna were sufficient to hack the two encryption standard algorithms, known as GMR-1 and GMR-2, implemented to protect satellite phone signals of principal phone operators. These encryption standards were commonly used in the Thuraya satellite phones deployed in Africa, the Middle East, and North Asia.

GMR-1 is a variant of the A5/2 algorithm implemented by the GSM standards. It is vulnerable to cipher-text-only attacks. The GMR-2 standard introduced a new encryption algorithm, also cryptanalyzed.

Quote:One of the most popular cases of satellite eavesdropping has as a protagonist the off-shelf software SkyGrabber, produced by the Russian firm Sky Software and sold for $26. The software was used by hackers in Iraq and Afghanistan to capture unencrypted video feeds of the Predator unmanned aerial vehicles (UAVs).

The software was used to access data broadcast by satellites. The insurgents in those areas weren’t able to control or disrupt the UAVs but, using SkyGrabber, eavesdropped on the signals sent.

The news created a lot of noise in the military, for it is normal to expect the highest level of security in military equipment, including communication encryption. The fix of the flaw added cost to the military program, but the greatest menace from the eavesdropping of the videos was represented by the disclosure of locations of military areas under military surveillance and of course the patterns followed by drone used for reconnaissance activities [36].

SkyGrabber

SkyGrabber is offline satellite internet downloader
SkyGrabber allows to accept satellite internet data, assemble it in files (avi,mp3,mp4,etc.) and save files onto your hard disk. The program has user-friendly interface, diverse filter system and satellite provider manager inside.

FIGURE 26: SkyGrabber Home Page.

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 [4, 25, 26]. 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 [1;37].

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 [1;37].

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 [1;38].

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!]
[2, 44, 45].

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” [1;38].

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 [1;38].

2002 The Falun Gong illegally used an AsiaSat satellite to broadcast into China disrupting broadcasts of China Central TV (CCTV) with anti-government messages [46, 33]. 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” [1;38].

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 [1;38].

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 [1;38].

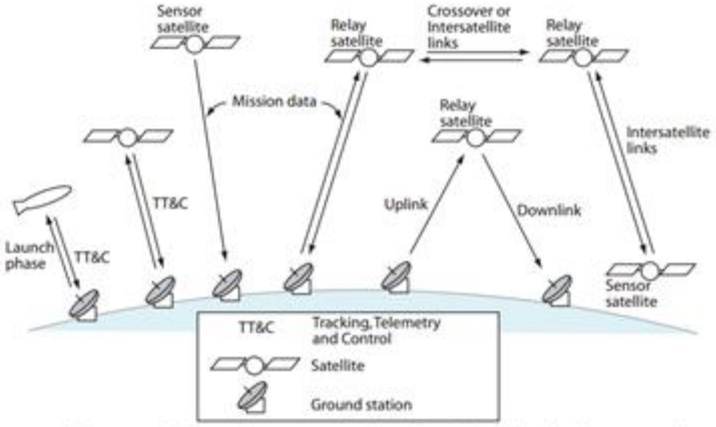
2007 The Tamil Tigers (LTTE) in Sri Lanka illegally broadcast their propaganda over Intelsat satellites [1;38].

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 [1;39].

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 [48, 51]. 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 [1;39].

Control

Controlling a satellite involves breaching the TT&C (tracking, telemetry and control) links; the wrong commands are sent to the satellite system, causing device rotation or movement that could direct solar panels and antenna in the wrong directions. Satellite control is considered very difficult to implement because security measures to protect satellites are very effective against these intentional attacks.



The communications architecture consists of satellites and ground stations interconnected with communications links. (Adapted from SMAD.)

FIGURE 27: Satellite architecture including TT&C.

In military environments, TT&C ground stations are not freely accessible; they are, in fact, usually protected within a secure area that has controlled access and physical countermeasures to avoid intrusion from external entities. Despite the high level of security the menace must be properly approached. An attacker could exploit a flaw in the command and control of commercial satellites, such as VSAT hubs, to compromise also military satellite systems.

A word on Telemetry, Tracking & Command (TT&C):
-Telemetry is an automated communications process where data is collected and then transmitted to receiving equipment for monitoring, display, and recording.
- In the case of satellites, the data from the satellite is about its operations (eg. temperature of batteries) or about its mission (eg. scientific data being collected).
- Ground control "commands" transmitted to the satellite could control a process, switch transmitters on/off, reschedule some equipment function, or adjust the satellite's altitude.
- A transducer converts the physical stimulus to be measured (eg. vibration, temperature) into an electrical signal.
- The signal is then transmitted to the ground by radio waves.
- Once the ground station receives the transmission, the data must be extracted from the received signal and displayed in a form which can later be processed by computers.
- This entire process as a whole makes up telemetry [36].

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 [1;39]. .

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" [1;39]. .

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 [1;39].

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" [1;40].

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" [1;40]. .

GPS
One of the most classic examples of satellite control attack is the exploitation of the vulnerability of GPS systems, a technology widely used today in commercial and military sectors.

The wide range of applications based on the technology in today's society requires a continuous reassessment of the risks related to the exposure of incidents. The first report in which threats to GPS systems were discussed is known as the "Volpe Report." This document describes the principal menaces for the technologies, as well as the means and the motivation behind for attacks in both the civil and military sectors.

The most insidious threat for GPS systems is known as "GPS spoofing," whereby interference with the GPS receiver is fooled into tracking counterfeit GPS signals. Unlike the case of jamming of GPS signals, in spoofing the targeted receivers are deceived. GPS "spoofers" are devices that create false GPS signals to fool receivers into thinking that they are at a different location or different times, this type of attacks can be really useful in a multitude of scenarios, such as the hijacking of drone or a vessel.

These attacks are difficult to detect and can be conducted in numerous sectors, from transportation to financial environments.

“Information on the capabilities, limitations, and operational *procedures [of*spoofers*] would help identify vulnerable areas and detection strategies,” states the report.*

During the risk assessment, numerous countermeasures that have been classified for their implementation have been evaluated. Principal countermeasures implemented in software on GPS receivers are:

- Amplitude discrimination
- Time-of-arrival discrimination
- More sophisticated techniques are:
- Consistency of navigation inertial measurement unit (IMU) cross-check
- Polarization discrimination
- Angle-of-arrival discrimination
- Cryptographic authentication [36]

Some of the above attacks are difficult to conduct because they require sophisticated and expensive hardware, such as multiple antennas or a high-grade inertial measurement unit (IMU). The most efficient countermeasure against these attacks is the adoption of signal encryption; the receiver and transmitter use mutual authentication processes to avoid interferences from external sources. Unfortunately, these techniques, while compatible with a classic GPS, require more powerful hardware and systems able to manage the overhead introduced by authentication procedures. For this reason, encryption is limited to the military sector.

In our imagination, the use of GPS systems is related to the concepts of position and route. It is documented that these systems are used in aviation, marine, and ground transportation to indicate the way forward in the absence of other references. The GPS technology is also used in other areas, from environmental control to the financial sector. A possible attack on GPS systems would impact many sectors with serious consequences. Since December 2003 the Department of Homeland Security has alerted on the risks of possible attack; it also documented that countermeasures, including monitoring the absolute and relative GPS signal strength, monitoring the satellite identification codes and the number of signals received, and checking the time intervals between the received signals can be used to guard against spoofs [36].

Extremely interesting is the impact that a GPS system can have on the financial world, where the accuracy of measuring time on a global scale and the synchronization between the various time zones, an operation made possible with the use of the GPS technology, are considered crucial. The main trading systems use GPS to synchronize each other and an attack could even cause a block to trading.

A typical attack can be addressed with the intent to sabotage the times on one of the global stock exchanges; it could cause a block of the activities once the automated trading systems notice the anomaly. It happened in during the Flash Crash of 2.45, on May 6, 2010, when the United States stock market crashed.
Imagine the effect of a misalignment of a few milliseconds between the various trading systems: Criminals could exploit this mismatch to have advance knowledge of the value of any trade, which would be a disaster for the stock exchange.

Todd Humphreys, an assistant professor at the University of Texas, and his team have created the world’s most powerful GPS spoofer and have tested it on GPS-based timing devices used in mobile phone transmitters.

Fortunately, so far no serious attack has been recorded but we are seeing evidence of basic spoofing, likely carried out by rogue individuals or small groups of criminals. Evidences of these attacks have been collected in several countries monitoring jamming and spoofing activities for a long period. It is necessary to take into serious consideration this kind of threat due their sensible impact on our ordinary activities [36].

Colby Moore, a researcher at the hacker-for-hire startup Synack, has uncovered a way to crack the global positioning system (GPS) satellite network of Globalstar, a multibillion dollar satellite communications company based in Covington, La.

Globalstar GSAT -2.63% sells devices connected to its satellite network that track the locations of shipments and other goods. Since the company's technology does not, according to Moore, encrypt data transmitted between such devices and its satellite network, a "man-in-the-middle" attacker can easily spoof the system.

In other words, a hacker can intercept communications beamed over the company's Simplex data network, and then modify, fake, or jam them. The vulnerability could be exploited by intelligence agents, criminals, or enemy combatants to eavesdrop, steal cargo, or follow troop and supplies movements.

Moore described such systems as "kind of fundamentally broken from the get-go" in an interview with Reuters. Worse, the flaws are not easily addressable; they are architectural in nature, he said, and software patches would not fix them.

"We rely on these systems that were architected long ago with no security in mind, and these bugs persist for years and years," Moore told Wired. "We need to be very mindful in designing satellite systems and critical infrastructure, otherwise we're going to be stuck with these broken systems for years to come."

Moore added that he suspects similar satellite communications systems, beyond Globalstar's own, could be vulnerable, too.

Though Moore said he alerted Globalstar of the problems six months ago, the company has yet to take action in way of a solution.

Globalstar—which counts many companies in many critical industries among its customers, including oil and gas, shipping, military, and more—replied evasively to Fortune's request for comment, sidestepping questions about a possible remediation plan and not confirming whether its data in transit are unencrypted:

Globalstar monitors the technical landscape and its systems to protect our customers. Our engineers would know quickly if any person or entity was hacking our system in a material way, and this type of situation has never been an issue to date.

Fortune recently wrote about how freight thieves are turning to cybercrime. This new research represents a chilling development in that trade. The research heralds a world in which products no longer "fall off the truck," but rather entire trucks, planes, and cargo shipments can "fall off the map [53].

Scanning / Attacking

When explaining scanning and attacking concepts, it is useful to remember the content of a presentation made in 2010 by Spanish cyber security researcher Leonardo Nve at the Black Hat security conference in Arlington. The expert exposed to the audience a variety of tricks to access to satellite Internet connections and exploit them.

The expert impressed those present with following assertion:

"What's interesting about this is that it's very, very easy … Anyone can do it: phishers or Chinese hackers; it's like a very big Wi-*Fi network that's easy to access."*

At a cost of only $75 in tools he was able to intercept digital video broadcast (DVB) signals to get free high-speed Internet. Nve used a Skystar 2 PCI satellite receiver card along with open source Linux DVB software applications and the popular network sniffing tool Wireshark. NVE's techniques exploited the lack of encryption for DVB signals. The technique was already known to the hacking community but Nve also demonstrated how to use satellite signals to anonymize his Internet connection, intercept satellite Internet users' requests for Web content, and replace them to gain access to private networks. Nve exploited the satellite signal's ability to spoof any user identity on the Internet via satellite. The Spanish researcher was also able to impersonate a website operating on the user DNS requests. He was in fact able to manipulate IP addresses received in response to request of conversion from an ISP for a website name. He made a DNS entry point to another IP than the one it would be supposed to point to (DNS spoofing). The IP address was sent back by Nve faster than the ISP deceiving the user and hijacking it on a fake website. The repercussion of this attacker is easily imaginable: An attacker in this way could serve malware or steal a user's credentials.

Nve revealed that during his test he was also able to hijack signals using GRE (generic routing encapsulation) or TCP protocols that entities use to communicate between PCs and servers [36].

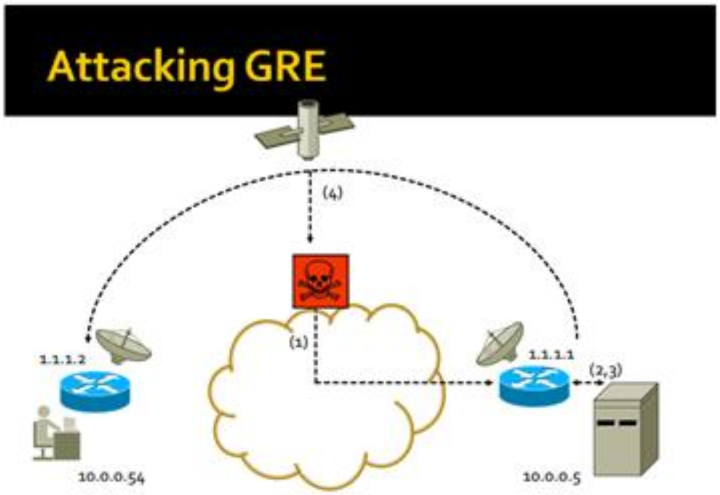


FIGURE 28: Slide of Nve presentation.

Resuming, the researcher was able to perform:

- DNS spoofing
- TCP hijacking
- Attacking GRE

Signal Encryption and Hardening

The principal countermeasures to protect satellite infrastructures are the encryption of signals and the hardening of single components, such as the ground stations.

Encryption is crucial to protect signals from spoofing attacks and it is also used to mutually authenticate communication interlocutors. It is fundamental to understand that encryption doesn't represent a definitive solution; it adds a supplementary layer of defense as occurred for the algorithms A5-GMR-1 and A5-GMR-2, which have been cracked by a team of German researchers.

The algorithms used and the level of encryption adopted is functional in the field of application. Managing signal encryption requires supplementary hardware capabilities, with repercussions on the overall cost of the systems, on the maintenance activities, and on the performance and the global security of the platform.

Another element to consider is the encryption of signals exchanged between the modules of the satellite structure. Multiple nodes can be encrypted, such as data and TT&C uplinks or access between terrestrial networks and the ground stations.

Due to the above reason, most commercial satellite systems are designed without encryption of the signals; every transmission has “open access,” and is transmitted without any protection. The information security could be improved by introducing encryption, while physical security could be increased with the adoption of hardening methods in different parts of the satellite system.

Physical protection of the terrestrial environment includes common defense devices and supplementary structures such as access control systems, cameras, fences, and security guards. In a high-security environment ground stations are located within military compounds having in place strict security measures.
The intrusion could be physical or electronic (e.g., radio signal interception and jamming). To protect signals from attackers, the satellite antennas are often obscured with barriers to prevent attacks that are dependent on line of sight.

Other techniques could be used for terrestrial equipment protection such as directional antennas that reduce interception, shielding and radio emission control measures to mitigate surveillance or jamming activities from third parties.

The satellite itself may be hardened against radiation, meteoroids, and orbital debris. To minimize disruption in case of kinetic or natural disaster, the deployment of satellite networks with redundant components having multiple satellites and ground stations is suggested.

Hardening of the 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). The main impact of the implementation of this type of countermeasures is the increase in costs in building, deployment, and maintenance [36].

Asymmetrical attacks

As recent events in Paris have shown, asymmetrical attacks are a cost-effective way for terrorists to cause immense impact. This was also the case for the cost ratio between the 9/11 attacks and the subsequent invasion of Iraq. But there are other threats coming, beyond these cowardly actions, in the future. Space is an obvious next target, as an increasing number of vital services depend on it.

Taking control of satellites, making them collide, damaging their critical sub-systems or ground stations, or spoofing and jamming their signals is no longer just science fiction. In addition, space assets are particularly vulnerable because of their long life cycles. It is not unusual forten years to pass between the design and launch of a satellite. When it's in space for the next decade, you cannot simply go and fix it, or put an armed guard in front of it.

The magnitude of the emerging threat may be beyond what had been anticipated, and hardening space equipment is expensive. Owners of military satellites have little to fear from amateur, unprofessional hackers, but civilian systems, like most European programmes, are far from being properly protected. Some online stores actually have better cybersecurity than some satellites.

Space is not just a bunch of satellites far, far away. Positioning, timing and communication satellites are vital for our economy, the safety of citizens and our modern way of life. Space assets provide a master-infrastructure which supports many other activities. As an example, dysfunctional satellites or signals can lead to power-grid black outs, severely impact STOCK EXCHANGES, or disable mobile phone networks.

The civil space community is slowly waking up to this new menace posed by cybercrime and cyberterrorism. A decade or so from now, the weaknesses will have worsened significantly, considering the certain proliferation of autonomous vehicles and the billions of devices, mostly in homes, that will be linked up by swarms of mini-satellites through the internet. Provoking a "space cataclysm" could become a reality for the fanatics as they seek to return us to their vision of the Middle Ages.

However, reaction times are much longer, and the possible damage is potentially much higher, for satellite systems, than ground infrastructures. Cyberattacks on networks hit the news every other day, but these are only in their infancy compared to what is in front of us as their progression will not be linear but exponential. We should all be concerned about this, and join forces in identifying the risks and defining common solutions [54].

One of the main challenges is to know what cybercrime or cyberterrorism will look like in 10-15 years, as the next generation of space assets need in-design hardening and current assets need better resilience based on software updates. But in the meantime, one needs to raise the awareness of the service providers, the users and the public opinion on this broad issue that should concern each and every one of us.

Cyber communities and space communities largely ignore each other, mostly because of very different cultures. Even at a military level, the US has now identified their GPS satellites as an "Achilles heel" to their aim for space supremacy. For obvious reasons it is difficult to get much information on vulnerability and countermeasures out of the defence sector. But for civilian programmes, we need to trust one another and share information more to allow vulnerability disclosure exchange from which we will all benefit.

Like all cyberattacks, attribution is difficult, but in this case it does not actually matter so much. What does matter is to identify and merge cyber-events about the actions of a common enemy. The main source of information is the space industry itself, and public and private operators as they are the main targets of disruption. We need to ensure that we are all working together, holistically.

At a time when the EU’s Galileo (European GPS) and Copernicus (European earth observation) programmes start their operational services and other programmes are in the making, resilience must become a priority. First and foremost, an awareness gap must be filled within the policy world as well as between cyber and space security experts.

Then, to start fixing the problem effectively, member states and EU Institutions could trigger the establishment of a common cyber-events repository. This could lead to shared assessments of vulnerabilities, benchmarking, and best practice, leading to the implementation of countermeasures, from conception to actual operations of current and next-generation satellite systems.

The potential for a catastrophic event is increasing every day. We cannot wait for a wake-up call to start implementing such preventive measures. The tradeoff for the additional costs calls for a level playing field. This can be achieved by imposing common minimal standards for governmental and commercial assets, especially when the operation of critical infrastructures is at stake.

This reliability must be seen as an investment that can only be beneficial for our industry in the long run. Only an interlinked approach can make the difference as the issue is a global one: space services have world-wide reach which makes this global commons even more vulnerable. Once Europe has shown the way ahead, others will join [54].

Conclusions

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. 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 [1;45].

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 [1;45].

3. REFERENCES

1. 1. Fritz, Jason (2013) "Satellite hacking: A guide for the perplexed," Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 10: Iss. 1, Article 3.

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

3. GAO Critical Infrastructure Protection Commercial Satellite Security Should Be More Fully Addressed. Internet: http://www.gao.gov/assets/240/235485.pdf. 2002 [Feb. 12, 2013].

4. Space Security Index 2012. Internet: http://swfound.org/media/93632/SSI_FullReport_2012.pdf, 2012 [Feb.14, 2013].

5. Laurie, Adam. Satellite Hacking for Fun and Profit. Internet: http://www.securitytube.net/video/263, 2009 [Feb.14, 2013].

6. Electromagnetic Spectrum. Internet: http://en.wikipedia.org/wiki/File:Electromagnetic-Spectrum.png, 2012 [Feb.14, 2013].

7. Gordon, Steven. Talking to Martians: Communications with Mars Curiosity Rover. Internet: http://sandilands.info/sgordon/communications-with-mars-curiosity, 2012 [Feb.27, 2012].

8. Thompson, Cynthia. ABC 10 victim of hackers. Internet: http://abc10up.com/abc-10-victim-of-hackers, 2013, [Feb. 20, 2013].

9. Sri Lankan Terrorists Hack Satellite. Internet: http://it.slashdot.org/story/07/04/13/068222/sri-lankan-terrorists-hack-satellite, 2007 [Feb.14, 2013].

10. Gutteberg, Odd. Telektronikk 4.92 Satellite Communications. Internet: http://www.telenor.com/wp-content/uploads/2012/05/T92_4.pdf , 1993 [March 26, 2013].

11. Edition, The Comsys VSAT Report, VSAT Statistics. Internet: http://defensesystems.com/articles/2012/03/28/c4isr-2-military-vsat-technology-advances.aspx, [March 26, 2013].

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

13. BGAN: Global voice and broadband data. 2013, Internet: http://www.inmarsat.com/cs/groups/inmarsat/documents/document/019403.pdf, 2009 [March 28, 2013].

14. Geovedi, Jim; Iryandi, Raditya; and Zboralski, Anthony. Hacking A Bird inthe Sky 2.0. Internet: http://www.youtube.com/watch?v=dLbRuJikb1U, 2008 [Feb. 10, 2013].

15. Davies, Roger. New satellite uplink trends. Internet: http://broadcastengineering.com/mag/new-satellite-uplink-trends, 2006 [March 26, 2013].

16. Dennis, Louise , Fisher, Michael and Hindriks, Koen . A Semantic Framework for Socially Adaptive Agents: Towards strong norm compliance. Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems, 2015, pp. 423-432.

17. Messmer, Ellen. Researchers crack satellite encryption. Internet: http://www.networkworld.com/news/2012/020812-satellite-encryption-255893.html, 2003 [Feb. 26, 2013].

18. UCS Satellite Database. Database, official names only. Internet: http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucssatellite-database.html, 2012 [Feb. 26, 2013].

19. Prime: Cybersecurity Risk Management Strategies For SATCOM Networks. Internet: http://www.milsatmagazine.com/cgi-bin/display_article.cgi?number=1142237172, 2012 [Feb. 14, 2013].

20. Jonathan. Unmanned X-47B aircraft completes sea trial. Internet: http://news.cnet.com/8301-11386_3-57560226-76/unmanned-x-47b-aircraft-completes-sea-trial/, 2012 [Feb. 26, 2013].

21. Col James G. Lee, “Counterspace Operations for Information Dominance,” in Beyond the Paths of Heaven: The Emergence of Space Power Thought, ed. Col Bruce M. DeBlois, Maxwell AFB, AL: Air University Press, 1999, p. 281.

22. Wilson, “Threats to United States Space Capabilities.” Internet: https://fas.org/spp/eprint/article05.html, 2010 [Feb. 26, 2016].

23. Satellite Network Security. Internet: http://www.irma-international.org/viewtitle/14070/, 2003 [Feb. 26, 2015].

24. Hacking Satellites — The New Frontier In Security Breaches. Internet: http://satmagazine.com/story.php?number=1794004708, 2010 [Feb. 26, 2015].

25. Ruben Santamarta Principal Security Consultant. Wake-up Call for SATCOM Security Internet: http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf, 2012 [Feb. 26, 2013].

26. Greenberg, Andy. How To Hack The Sky.Internet: http://www.forbes.com/2010/02/02/hackers-cybercrime-cryptography-technology-security-satellite.html, 2010 [Feb. 16, 2013].

27. Szczys, Mike. Grab your own images from NOAA weather satellites. Internet: http://hackaday.com/2011/10/20/grab-your-own-images-from-noaa-weather-satellites/, 2011 [Feb. 16, 2013].

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

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

30. USCC. Report to Congress of the US-China Economic and Security Review Commission. Internet: http://origin.www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf, 2011 [March 24, 2013].

31. Benson, Mark. Australia angers China over broadband contract. Internet: http://www.australiaforum.com/information/general/australia-angers-china-over-broadband-contract.html, 2012 [Feb. 20, 2013].

32. Satellite Tracker. Internet: https://itunes.apple.com/us/app/satellitetracker/id306260378?mt=8, 2009 [Feb. 28, 2013].

33. GAO Unmanned Aircraft Systems. Internet: http://www.gao.gov/assets/660/652223.pdf, 2013 [Feb. 26, 2013].

34. Swann, Phillip. Washington DC TV Station 'Hijacked' By Mystery Photo. Internet: http://web.archive.org/web/20070716163040/http://www.tvpredictions.com/wjla071307.htm, 2007 [Feb. 20, 2013].

35. Hacking Satellites … Look Up to the Sky. Internet: *http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/,* 2013 [Oct. 2, 2015].

36. Jason Fritz, SATELLITE HACKING: A Guide for the Perplexed, Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, pp. 21-50, Dec. 2012 - May 2013.

37. Hacking Drones … Overview of the Main Threats Internet: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/

38. Greenberg, Andy. How To Hack The Sky. Internet: http://www.forbes.com/2010/02/02/hackers-cybercrime-cryptography-technology-security-satellite.html, 2010 [Feb. 20, 2013].

39. Waller, J. Michael. Iran, Cuba Zap US Satellites.Internet: http://www.wnd.com/2003/08/20157/, 2003 [Feb. 16, 2013].

40. Hencke, David and Gibson, Owen. Protest to Libya after satellites jammed. Internet: http://www.guardian.co.uk/uk/2005/dec/03/politics.libya, 2005 [Feb. 6, 2013].

41. Thuraya Telecom Services Affected by Intentional Jamming in Libya. Internet: from http://www.thuraya.com/about/profile/media-releases/thuraya-telecom-services-affected-byintentional-jamming-in-libya, 2011 [Feb.16, 2013].

42. Bellows, Alan. Remember, Remember the 22nd of November. Internet: http://www.damninteresting.com/remember-remember-the-22nd-of-november/, 2007 [Feb. 19, 2013].

43. British Viewers Hear Message. Ellensburg Daily Record. Internet: http://news.google.com/newspapers?id=KgkQAAAAIBAJ&sjid=YY8DAAAAIBAJ&dq=&pg=5086%2C3662230, 1977 [Feb. 20, 2013].

44. Jan Hanasz: The Polish TV Pirate. Internet: http://w.icm.edu.pl/tvS/pirat.htm, 1990 [Feb.19, 2013].

45. The Story of Captain Midnight. Internet: http://web.archive.org/web/20070128101239/http://www.signaltonoise.net/library/captmidn.htm, 2007 [Feb.17, 2013].

46. Rooker, J.W. Satellite Vulnerabilities. Internet: http://www.dtic.mil/cibin/GetTRDoc?AD=ADA507952, 2008 [Feb. 16, 2013].

47. Morrill, Dan. (2007). Hack a Satellite while it is in orbit. Internet: http://it.toolbox.com/blogs/managing-infosec/hack-a-satellite-while-it-is-in-orbit-15690, 2007 [Feb. 16, 2013].

48. Soares, Marcelo. The Great Brazilian Sat-Hack Crackdown. Internet: http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all, 2009 [Feb. 16, 2013].

49. Thompson, Cynthia. ABC 10 victim of hackers. Internet: http://abc10up.com/abc-10-victim-of-hackers/, 2013 [Feb. 20, 2013].

50. Friedman, Herbert. (2006). Psychological Operations during the Israel-Lebanon War 2006. Internet: http://www.psywar.org/israellebanon.php, 2006 [Feb. 20, 2013].

51. Wohlmuth, Radek. Umělci napadli vysílání ČT 2. Podívejte se jak. Internet: http://aktualne.centrum.cz/kultura/umeni/clanek.phtml?id=448450, 2007 [Feb. 20, 2013].

52. Zombies? Emergency Broadcast System hacked. (2013). Internet: http://www.uppermichiganssource.com/news/story.aspx?id=859352#.URnFMDvfLHR, 2013 [Feb. 20, 2013].

53. Campbell, Duncan. (1999). Cyber Sillies. Internet: http://www.guardian.co.uk/uk/1999/may/20/military.defence, 1999 [Feb. 27, 2013].

54. Here’s the scary new target hackers are going after. Internet: http://fortune.com/2015/08/04/globalstar-gps-satellite-network-hackers, 2010 [Feb. 2, 2013]

55. It's Surprisingly Simple to Hack a Satellite. Internet: http://motherboard.vice.com/read/its-surprisingly-simple-to-hack-a-satellite Space: Another frontier under threat. Internet: http://www.euractiv.com/sections/innovation-industry/space-another-frontier-under-threat-321609, 2008 [Feb. 10, 2013].