CRITICAL INFRASTRUCTURE AND OPERATIONAL TECHNOLOGY SECURITY

By Dr. Yiftah Lipkin (Israel Aerospace Industries Ltd), Amir Shlomo (Israel Aerospace Industries Ltd), Amir Paz (Israel Aerospace Industries Ltd), David Menaker (Israel Aerospace Industries Ltd), Guy Mizrahi, (Cyberia advanced cyber solutions [IAI's Cyber accessibility center]), Niv David (Tel Aviv University)

Space systems consist of three segments: the *space segment*, comprising the orbiting satellites, the *ground segment* (also referred to as the control segment), comprising the ground stations that monitor and control the satellites, and the *user segment*, comprising the equipment that uses the capabilities provided by the onboard satellite payloads (e.g., the user-terminals, in case of communication satellites). A cyber-attack, motivated by political, military, or criminal intent, may be carried out against any of the three segments. Nonetheless, the ground segment is considered more prone to cyber-attacks, owing to its greater accessibility, as well as its wide use of commercial off-the-shelf IT components (both hardware and software).

Indeed, a number of cyber-attacks on satellite systems have been reported over the years. Notably, in 1998, the German-US ROSAT space telescope was rendered useless after it inexplicably turned towards the sun, damaging a critical optical sensor by exposure. NASA investigators later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center.

A 2011 report to U.S. congress of the U.S.-China Economic and Security Review Commission documented a number of successful cyber-attacks carried out against U.S. government satellites. At least two U.S. government satellites experienced, each one individually, at least two separate instances of interference apparently consistent with cyber activities against their command and control systems. The more severe case occurred in 2008, when NASA experienced two short events of disrupted control over the earth observation satellite Terra/EOS AM-1 (lasting two minutes in June and nine minutes in October). In both cases, the attacker achieved all steps required to

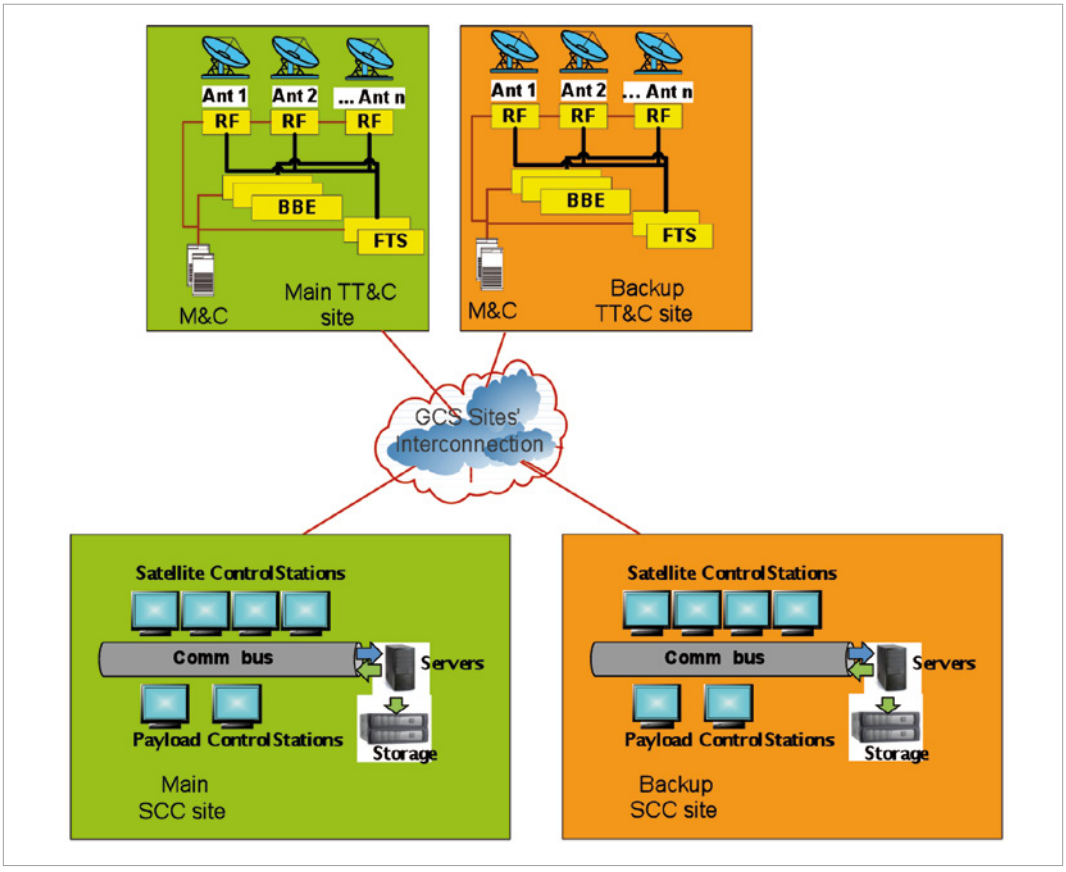

Figure 1: Typical Ground Station Architecture.

command the satellite but did not issue commands. In a similar case with Landsat-7, two events of disrupted control occurred (12 minutes each, in October 2007 and in July 2008; the first event was only discovered following the July 2008 incident), but in both events, the attacker did not achieve all steps required to command the satellite. This series of attacks is thought to have been carried out through a compromised ground station in Norway.

A more recent example of a high-profile cyber event occurred late 2014, when the U.S. National Oceanic and Atmospheric Administration (NOAA) was forced to shut down critical data systems for two days, following a breach of its satellite Data and Information Service network.

The ground segment of a communication satellite typically comprises a primary ground station and one, or several secondary ones, usually located in separate geographical sites (see Fig. 1). At the heart of a ground station is the control room, wherein Satellite Telemetry is received, processed, and analysed and Satellite Command and Control (SCC) is conducted. Communication between the control room and the satellites (uplink commands, as well as downlink telemetry from the satellite) are transmitted and received through Base-Band equipment and Radio Frequency (RF) equipment. These subsystems are usually separated from the control room, and are frequently located at a considerable distance from it.

The secondary ground stations are essential for meeting the high delivery reliability (DR) and continuous operation expected from communication satellites, by serving as backup in case of failure in the primary station, and in emergency situations. All sites are usually interconnected via communication link, preferably, a reliable and secure one.

Modern ground stations are typically based on commercial, off-the-shelf IT components and standard IT infrastructure, common to most organisational and command & control (C&C) IT networks. Such networks include PC workstations and servers (usually running Windows, Linux or Unix), brand network hardware, databases, storage facilities, etc. Such architecture makes the ground stations systems vulnerable to publicly-known cyber threats, which may compromise not only the ground segment but the entire space system as well . Often, ground station networks are also connected, either directly or indirectly, to the internet, thus subjecting the station to remote penetration and other internet-related threats.

Straightforward mitigation to such vulnerabilities is the application of known IT, cyber & communication security procedures and systems hardening at all levels, using available COTS solutions, thus obtaining increased cyber-security and cyber worthiness.

In particular, disconnecting the ground station from the internet leads to reduced probability of external compromise, as well as to possible better containment of any possible damage in case of a cyber-infection. However, as some measure of internet connectivity is usually necessary for the proper operation of modern organisations, proper technological measures should be taken to minimise the station's exposure to external threats; for example, by using one-way communications, or setting a gate filter that scans all incoming files and prevents malware-infected files, files with a fake extension, or forbidden types of files from entering the station network.

A cyber-attack on the ground station may also be carried out from within, e.g., by an employee who intentionally tampers with the satellite controls or, either maliciously or innocently, attaches to the ground station network an external memory device infected by malware. Such possible internal vulnerabilities may be mitigated by addressing these issues in the ground station operation procedures (and verifying that these procedures are indeed followed). These may include any or all of the following: periodic screening of the station personnel; setting a hierarchical authorisation scheme, on a need-to-know, need-to-do basis, thus preventing access of unauthorised personnel to restricted and more sensitive areas of the station network; requiring two-factor authentication in order to access more sensitive areas of the station network and to perform special safety procedures and high-risk satellite operations (e.g. firing the satellite thrusters); setting a pre-designated, cyber-hardened computer, equipped with malware-detection tools, which will be used for installing new software, as well as for updating programs in the station network and computers; and disallowing the attachment of external devices to all but several well-monitored access points.

The ground station supply chain introduces yet another possible access point for a cyber-attack. The installation of new specialised equipment, or the upgrade of software or firmware of an existing device, often require admittance of a technician employed by a supplier into the ground station and the connection of non-authorised external devices, such as disks or USB drives, to station computers. Moreover, such specialised equipment often employs non-standard protocols and operating-systems, rendering the clearance of software updates a non-trivial task. Such occasions may allow an attacker to access the station, either with the active cooperation of the technician, or without his/her knowledge.

Special attention should be devoted to components of the ground segment that are seemingly secure but may be prone to attacks by a malicious perpetrator. One example is the C&C communication channel between the control room and the ground C&C antenna, often not only located remotely, out of the physical reach and supervision of the control station personnel, but also clearly visible, and sometimes accessible to bystanders. Another example is the communication network between the various ground-segment sites, through which continued data synchronisation

between the sites is performed, thus allowing hot backup when needed. Compromise of the network may have grave consequences on the functionality of the ground segment even though these networks are often encrypted.

It should be noted that encryption is considered a good measure for securing data: encryption protects data when transferred over insecure lines, and secures it when stored on our computer, preventing its exploitation following theft or unauthorised copying. Nonetheless, this protection becomes irrelevant when a cyber-attacker gains access to a computer and can access sent data before it is encrypted or received after it is decrypted. Similarly, since the computer cannot process encrypted data, an attacker is able to intercept the data when accessed, unencrypted, by the user.

The feasibility of a cyber-attack on an ill-secured satellite ground segment and the possible grave consequences of such an event are illustrated in the following fictional attack scenario.

Consider an operator on the ground station who receives an email, seemingly from a colleague or a friend. Opening a document attached to the message leads to the immediate infection of the computer by a RAT malware (Remote Administration Tool, which grants the attacker full remote access and control over the infected computer). Once installed, the RAT contacts the attacker's command and control server over the internet, and awaits its commands. The attacker may initially study the affected computer by examining the programs installed on it, the files that reside on it, the computers and devices in its local area network, and by monitoring its activity by examining screenshots taken regularly.

This describes a generic, social engineering-based, cyber-attack which may affect any type of IT network. However, with a bit of luck, the attacker may discover that the computer contains a satellite control command authoring program, as well as command files to be transmitted to the satellite. After studying the command protocol, the attacker may be able to modify the command files, adding a sequence of instructions that would lead to an undesirable action by the satellite.

Once the command file is uploaded to the satellite and executed, the connection with the satellite may suddenly be cut off. The operators would have no choice but to wait for the satellite to auto-recover, reboot, and re-establish connection with its home base.

It would take the ground station operators some time to understand what went wrong. Only after several failed attempts would the operators realise that the problem occurs only when commands from this computer is sent to the satellite. A forensic review of the computers and internet communication would be conducted, hopefully gathering enough clues to determine that the problems occurred originated in the C&C computer, leading to the realisation that the station is a victim of a cyber-attack.

> ... IN THE PAST FEW YEARS, CYBER-ATTACKS ON SPACE SYSTEMS HAVE TRANSFORMED FROM A FICTIONAL NIGHTMARE SCENARIO TO A CLEAR AND ACTUAL THREAT ON THE SATELLITE INDUSTRY ...

In the past few years, cyber-attacks on space systems have transformed from a fictional nightmare scenario to a clear and actual threat on the satellite industry. As space systems become more computerised and as their network connectivity increases, this threat is expected to grow in the near future, potentially affecting millions of people. Thus, cyber protection of satellite systems becomes a necessity that providers and operators cannot ignore. The *modus operandi* of the satellite market needs to adjust itself to these changing circumstances, to include cyber security controls and practices in the design of its system, its networks and its daily operation. These should include measures such as secured topology, hardened IT infrastructure, utilisation of stand-alone networks, supply-chain control and components validation. ■

ABOUT THE AUTHORS

Dr. Yiftah Lipkin is a senior analyst in the Research & Technology Dept. at Israel Aerospace Industries (IAI). He has been at IAI since 2007, involved in research and development of algorithms in cyber-security, as well as in several other defence-related fields Dr. Lipkin holds a PhD in Physics from Tel Aviv University in Israel.

Amir Shlomo is the Cyber Hardening Department Manager, Cyber Programs Directorate, Israel Aerospace Industries (IAI).

He has been with IAI since 2006, and is spearheading the business development, product management, and development efforts of IAI's Cyber Worthiness offering. Previously, Amir served for 6 years as a team leader in Motorola.

During his military service Amir served in an advanced electronic technical support unit of the Israeli Defense Force.

Amir has a B.S.C. in Electronics and Electrical Engineering, an M.B.A., and an M.S.C. in electrical and electronic engineering – with a specialisation in communication from HIT.

Amir Paz is the Director in charge of the Earth observation system at the Israeli Aircraft Industries (IAI), Space Division. As part of this role, Amir is responsible for the operation of both GEO satellite and LEO satellite Arsenal. Amir is also responsible for the development of the ground segment and systems controlling these satellites.

Prior to this role, Amir was an Executive Business Development Manager at Cisco Systems and was leading Strategic Opportunities for Cisco in Israel. Amir led several teams and was working with Cisco's executive global team to pursue multi Million dollars opportunities derived mainly from the Israeli Government. Prior to his role in Business Development, Amir led, for 3 years, Cisco's local sales for the Defense Market and was in charge of Cisco's lion sales share in Israel.

Before joining Cisco, Amir was working for an international start-up company that was developing products for the Consumer Electronic market. These products were sold globally and Amir was the Company's director for Business Development.

Amir has retired from the Israeli Defense Forces (IDF) 7 years ago, as a Lt. Col. During his career working for the IDF's Intelligence Forces, Amir led large scale R&D programs with participation and support of large Defense Contractors from the US and Canada.

Amir holds an MBA Degree from the University of Phoenix where he specialised in Technology management.

David Menaker is the IT manager in AMOS Satellites' Ground station at the Israeli Aerospace Industries (IAI), Space Division. As part of this role, David is responsible for the operation of the GEO satellites' computers infrastructure.

Prior to this role, David was in charge of Satellite Command & Control (SCC) for the AMOS communication satellites in IAI.

David holds an M.Sc. Engineering Degree from the Israeli Technion in Haifa.