# Satellite Network Security

**Marlyn Kemper Littman**
*Nova Southeastern University, USA*

## INTRODUCTION

*Satellite networks* play a vital role in enabling essential critical infrastructure services that include public safety; environmental monitoring; maritime disaster recovery and reconnaissance; electronic surveillance; and intelligence operations for law enforcement, the military, and government agencies (Jamalipour & Tung, 2001). As demonstrated by the events following the terrorist attacks in the U.S. on the Pentagon in Washington, D.C. and the World Trade Center in New York City on September 11, 2001, satellite networks also provide redundant communications services when terrestrial networks are disrupted and/or unavailable. Despite their merits, satellite networks are nonetheless vulnerable to cyber attacks that pose threats to national security and the economy.

Satellite networks transport voice, video, images, and data through the air as electromagnetic signals, thereby making these transmissions susceptible to interception. Technical advances enable the interconnectivity of satellite systems to public and private wireless and terrestrial networks including the Internet. These advances, however, amplify the risk of cyber attacks that can compromise critical infrastructure functions dependent on satellite networks in sectors that include information technology (IT) and telecommunications; defense; government; banking and finance; utilities; agriculture; emergency services; public health; and transportation (U.S. Department of Homeland Security (DHS), 2003; U.S. Government Accounting Office (GAO), 2004). As a consequence, satellite networks employ an array of security tools and mechanisms for countering costly and widespread cyber incursions and, thereby, ensuring the continuity of critical infrastructure operations. Those cyber attacks that are politically motivated and specifically designed to disrupt essential services are generally attributed to *cyber terrorism*.

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. Standards and protocols that safeguard satellite networks from unauthorized use and intentional disruptions and policies, and legislation that facilitate cyberspace asset protection are described. Capabilities of *encryption* in supporting secure satellite services and the distinctive attributes of the InterPlanetary Internet (IPN), also called the InterPlanetary Network**,** are explored.

## BACKGROUND

### Satellite Network Technical Fundamentals

Satellite networks consist of ground and space segments. The ground segment includes a ground or earth station that delivers communications services and monitors satellite operations by providing tracking, telemetry, and control (TT&C) functions. The space segment consists of the artificial satellite and its payload.

In contrast to a natural satellite or a celestial body that revolves around a larger sized planet, an artificial satellite is a wireless receiver/transmitter that orbits the earth and employs microwave technology in the super high and extremely high radio frequency (RF) bands of the electromagnetic spectrum to enable wide area interactive communications (Littman, 2002). The payload includes transceivers and antennas for RF signal reception, amplification, and retransmission.

The quality of the satellite signal reflects the quality of the uplink and downlink. An uplink describes signal transmissions from an earth station such as a gateway, teleport, hub, or very small aperture terminal (VSAT) to the satellite. A downlink refers to signal transmissions from the satellite to the designated reception site. Typically, satellite transmissions are asymmetrical with more information transported on the downlink than on the uplink (Littman, 2002). Generally classified in terms of the orbits in which they operate, satellite constellations are categorized as geosynchronous or geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO).

### 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 (Littman, 2002).

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 (U.S. GAO, 2002).

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. government-supported broadcasts promoting regime changes in Iran were blocked by the Iranian Ministry of Post, Telegraph, and Telephone (Waldrop, 2005). 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 from 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 (U.S. GAO, 2005) 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 (Conti & Ahamad, 2005; Wilson, 2005).

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 (Wilson, 2005). Satellite network attacks attributed to cyber terrorism can result in disruptions in financial markets and disclosure of government, law enforcement, medical, and/or military classified data (U.S. GAO, 2004). Intentional satellite system incursions motivated by cyber terrorism raise 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 (Bosch, 2002).

## SATELLITE NETWORK SECURITY INITIATIVES

A multifaceted approach with multiple levels of security is required to protect satellite networks against cyber attacks that can culminate in malicious data corruption; system and service disruptions; unauthorized information disclosure; and physical destruction of satellite assets. Implementation of procedures for safeguarding satellite space and ground segments, TT&C functions, and satellite uplink and downlink transmissions; strategies to optimize satellite network performance; and satellite security protocols to provide authentication and authorization services must be based on a systematic assessment of satellite network risks and a comprehensive determination of satellite network security requirements (Roy-Chowdhury, Baras, Hadjitheodosiou, & Rentz, 2005). Tools, procedures, and measures that aid in safeguarding satellite operations include the enactment of public policies and legislation; the implementation of satellite security protocols and standards; and the utilization of security mechanisms and tools such as encryption.

### Public Policies and Legislation

Presidential Decision Directives Nos. 49 (1996) and 63 (1998) define U.S. satellites' space activities as critical to national defense, economic security**,** and public health and safety and are essential in supporting critical infrastructure protection. U.S. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No.12 establishes a foundation for a nationwide information assurance policy to guide the planning, design, implementation, and operations of secure U.S. space systems (NSTISSC, n.d.). NSTISSP No. 12 measures also mandate that U.S. space systems support information confidentiality, data integrity, user authentication, the availability of information services to authorized users, and service nonrepudiation. Empowered by the U.S. Homeland Security Act of 2002, the U.S. DHS supports comprehensive vulnerability assessments and coordinates nationwide response to threats and attacks classified as cyber terrorism in conjunction with entities that include the U.S. National Infrastructure Protection Center (U.S. DHS, 2003).

International cyber security agreements and public policies such as the Council of Europe's Convention on Cybercrime endorsed in 2001 by 38 countries including the U.S. promote development of international legislation to deter cyber terrorism activities (Wilson, 2005). In 2003, a joint declaration of Cooperation to Combat Terrorism supported by the European Union and the Association of South East Asian Nations (ASEAN, 2003) called for international cooperation in detecting and responding to threats of attacks on satellite assets.