Satellite communications

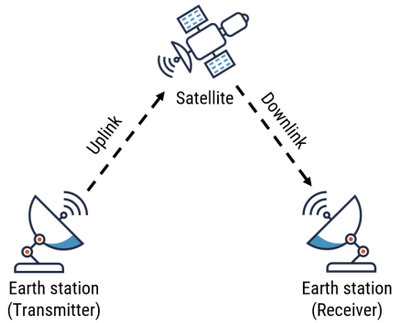
CANADIAN CENTRE FOR CYBER SECURITY

March 2023 | ITSAP.80.029

In a world where communication is key, satellite communications (SATCOM) provide connectivity for people in remote communities where cellular networks or wired connections are unavailable. SATCOM technology provides important functions, such as critical communication channels during periods of conflict or natural disasters, when traditional communications infrastructure is damaged or inaccessible. This document offers guidance on how to mitigate risks and is tailored to SATCOM network providers, operators of critical infrastructure, and organizations that rely on satellite connectivity to provide services.

What is satellite communication?

SATCOM is the use of artificial satellites to link two or more points on Earth. One of its main benefits is that it allows for communication between widely separated geographical points. A ground station on Earth transmits signals to the satellite (uplink). The satellite's onboard transponder amplifies the signals and transmits them back to Earth to a receiving ground station (downlink). The signals may contain voice, video, or data. A connection of multiple satellites, known as a satellite constellation, provides service availability such as satellite Internet and satellite phones across the entire Earth's surface.



What are the risks?

Cyber threats to satellite communications networks can have a significant impact on the ground. Threats can spillover to multiple areas and systems, resulting in collateral damage to critical infrastructure used in Internet and mobile networks or electric utilities. Threat actors can target SATCOM in the following ways:

- Jam signals to block communication between a satellite and a ground station. This can result in the deliberate disruption of critical communications.
- Intercept satellite uplink and downlink transmissions using unencrypted communications protocols.
- Attack the supply chain by creating backdoors if software or hardware from non-vetted third parties is not properly reviewed and audited before engaging in partnerships.
- Target small satellites such as "CubeSats" which are typically cheaper, lightweight, and assembled using commercial-off-the-shelf (COTS) hardware and software. Due to its low cost and resource constraints, this type of equipment may not have the capability to implement robust security measures.
- Exploit unsecured SATCOM devices, including Internet-facing transmitter and receiver stations. Sophisticated threat actors can take advantage of known or zero-day vulnerabilities in these systems to cause damage or to pivot to other parts of the network.
- Use satellite systems to geolocate ground terminals to locate specific satellites for malicious purposes. This can have privacy and operational security consequences for the general population and the military.

What is satellite communication used for?

SATCOM technology is increasingly used to help meet the growing demand for global connectivity and real-time information. Some of the most common uses of this technology are in the following areas:

Mobile communication. Satellite phones are types of mobile devices that are an indispensable tool used by many sectors including government (in emergency response and disaster recovery situations), mining (to monitor personnel and equipment), as well as in oil and gas (to connect remote exploration, production and distribution sites).

Broadcasting. Radio and television broadcasters use satellite communications to distribute a wide range of content to consumers. This includes news, sports, and entertainment as well as live broadcast feeds. Consumers can access this content at home, work or while on the move both in urban and rural settings.

Satellite Internet. A type of wireless Internet connection that allows people in remote regions and newly developed areas to access communication networks for use cases including rural classrooms and telemedicine. Like satellite phones, it enables organizations to maintain connectivity with their remote workers and operations. Some Government of Canada departments and enterprises use satellite connected routers in remote regions as a backup solution for Internet access, as part of their business continuity strategy.

Military. SATCOM technology enables the military to communicate with their personnel spread globally over land, air and sea. This includes relaying critical surveillance and reconnaissance information to support their operational missions.

Satellite direct-to-device. This emerging technology provides connectivity directly to a user's mobile phone or Internet of Things (IoT) device. Initial functionality is limited to emergency location services, messaging, and low data rate applications. Full integration with 5G networks use cases are under development.

Very small aperture terminal (VSAT)

VSAT is a technology that refers to a two-way satellite ground station that uses small dish antennas (generally less than 3 meters) to transmit and receive signals over a satellite communications network. VSAT systems are commonly used for point of sale credit card transactions in retail, to transmit banking transactions between head office and branches, to relay telemetry from OT systems, and to provide Internet access in remote regions. VSATs are easily deployable as they require little infrastructure to set up and operate.

Check out the National Security Agency's (NSA) publication on Protecting VSAT Communications

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Satellite communications

CANADIAN CENTRE FOR CYBER SECURITY

March 2023 | ITSAP.80.029

How to protect the SATCOM ecosystem

SATCOM network providers must protect their deployed satellite equipment while in orbit from physical damage caused by unintentional or malicious threats. In addition, the following mitigation measures can reduce the risk of compromise to the satellite communications ecosystem:

- ☐ Monitor network activity for anomalous traffic at ingress and egress points. Unauthorized traffic and security incidents should be promptly investigated by qualified security operations centre (SOC) personnel. This enables quick response to contain the spread of compromise to the rest of the network.
- ☐ Ensure that all management, control, and user planes communications are physically or logically separated. They should also be isolated, encrypted, and authenticated within the network and when transmitted over satellite links.
- ☐ Implement physical security measures to protect the satellite core infrastructure and ground stations from malicious attacks, equipment failures, or natural disasters. Some examples include the use of surveillance cameras, physical locks, access controls, and fire or flood protection. This can prevent unauthorized access, loss of management access to critical core network equipment, or diminished capacity of the network operations centre (NOC).
- ☐ Avoid unnecessary connectivity to the Internet or public networks for SATCOM devices. But if required, implement network protections such as firewalls and virtual private networks (VPN) to limit access to only trusted communications.
- ☐ Use spot beams and frequency hopping methods to reduce signal interference and avoid interception. Spot beams concentrate satellite signals to cover limited geographic areas on Earth. Frequency-hopping is the rapid switching of the carrier frequency during transmission.
- ☐ Ensure the satellite core network infrastructure is designed and built with robustness and redundancy. For example, implement hot, warm, or cold back-up sites, disk mirroring, or storage replication. Use appropriate protocols and policies to minimize instability in the core Internet routing table. These measures can keep data flowing in the event of a failure or prevent complete loss of subscriber authentication platform.

Operators of critical infrastructure, enterprises and organizations can help protect the SATCOM ecosystem by implementing the following measures:

- ☐ Leverage the use of tools with transmission security protections to conceal traffic volumes, mask traffic sources and destinations, as well as validate that remote terminal access sessions are authorized.
- ☐ Install filtering devices on antennas to mitigate localized interference from non-malicious (unintentional) ground jamming from other wireless devices.
- ☐ Work with satellite operators or network providers to understand possible data leakage scenarios and mitigate risk of exposed geolocation information.
- ☐ Configure Internet exposed SATCOM and mobile communications devices with non-descriptive naming conventions and identifiers. This can make it harder for threat actors to identify the devices on the network and which ones may have existing vulnerabilities that can be exploited.
- ☐ Ensure SATCOM equipment and software developers use secure software development practices (e.g. avoid the use of hardcoded backdoors or of weak encryption and authentication mechanisms).

As a general best practice, both SATCOM network providers and their customers should implement the following mitigations to protect their networks and the whole SATCOM ecosystem:

- ☐ Enforce the principle of least privilege, where users are given only the set of privileges they need to perform authorized tasks.
- ☐ Enable automatic updates of IT equipment and patch known exploited vulnerabilities as soon as possible.
- ☐ Use intrusion detection systems to monitor and identify unwanted traffic (e.g. port scans) on the network. Vulnerability assessment services or tools should be used to scan the network for vulnerabilities.
- ☐ Segment the corporate IT network from operational technology (OT) and Internet of Things (IoT) networks to minimize compromise of sensitive information in the event of a security breach.
- ☐ Secure satellite connected communications devices by changing vendor-supplied default credentials, using multi-factor authentication, and encrypting data generated from them.
- ☐ Develop an IT recovery plan as part of an overall business continuity strategy in the event that satellite communications services become unavailable.
- ☐ Establish a robust supply chain risk management strategy to reduce the chance of acquiring and deploying potentially vulnerable products into the satellite communications ecosystem. This should include applying security clauses in procurement contracts and purchasing telecommunications equipment and services from trusted vendors.

Learn more

- Cyber security hygiene best practices for your organization (ITSAP.10.102)
- Isolating web-facing applications (ITSAP.10.099)
- Security considerations for critical infrastructure (ITSAP.10.100)
- Developing your IT recovery plan (ITSAP.40.004)
- Contracting clauses for telecommunications equipment and services (TSCG-01L)

Check out the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) publication on Strengthening cybersecurity of SATCOM network providers and customers.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada