**Security Issues in Satellite Communication**

**Introduction**

According to the Index of Objects Launched in Outer Space by the UN Office of Outer Space Affairs, by mid-2018, there were about 792 satellites orbiting around the earth while hundreds of other satellites were being used for technology development, navigation, earth science, space science and earth observation. This increasing proliferation of satellites is bringing increased security risks and concerns, as satellite communications are not as secure as generally perceived. Though satellite systems hold critical importance for our communication bandwidth at a global level, they are also gaining attention of cyber criminals.

**Importance of Satellite Communications**

Private and government organizations depend on satellites for their important operations and services such as navigation, communications, imaging, remote sensing and weather and meteorological monitoring. Similarly, GPS technologies, mobile networks and electrical grids incessantly rely on satellite networks for their operations. IoT devices also use satellite internet services such as [HugesNet Internet](https://satelliteforinternet.com/hughesnet-gen5-internet-plans/) for them to function seamlessly. Any intentional or unintentional disruption in satellite services can create a ripple effect, creating adverse economic losses or information leakage. This is particularly alarming because even though for many organizations satellites are an integral part of their cyber ecosystem, they hardly have direct authority to regulate the satellite’s cyber security.

**Security Shortcomings in Satellite Communication**

Satellites are operated by systems based on earth, which are key targets of cyber criminals who look for security loopholes as a potential for hacking into the satellite system. The supposedly large number of system entry points including the [internet near you](http://www.planetdish.com) also make it difficult to trace and mitigate cyber-attacks. If hackers intercept satellite signals they can access downstream system that connects with the satellite. This will enable the hacker to invade into an organization’s entire network only by infiltrating a satellite’s ground station. These not only include bigger military-grade satellites but could also be small commercial-grade satellites.

Another significant vulnerability common to all satellites is their practice of using long-range telemetry to communicate with ground stations. Uplink and downlink transmission is carried out with open telecom network security protocols which can be easily intercepted by cybercriminals.

IoT devices using satellite communications also provide additional entry points for hackers.

Even knowing of all the security issues an organization could face, many startups or small enterprises consider investing in cybersecurity to be costly and of little priority. Conventionally, the satellite sector has also lagged behind in the cybersecurity domain due to the requirement of a custom solution for each satellite’s individual requirement.

**Mitigating Cyber Risk in Satellites**

Cyber risk mitigation techniques in satellite systems include robust hardware usage on satellites, logical access at base stations, physical security and signals encryption to track and control the data being transmitted to and from satellites. For commercial satellites, risk mitigation is done by federal agencies which safeguard the data links and the ground stations. Federal agencies do not, however, manage the security of control and tracking links or ground stations as the satellite service provider is responsible for them.

**Some Security Recommendations**

Here are some recommendations to keep private and public satellite system communications secure:

* Consider information security as a key priority for your organization and allocate the required budget for it
* Apply strong encryption for all data that is transmitted to and from the satellite
* Create a cyber-security policy and communicate the requirements for the organization
* Use recommended authentication methods
* Deploy the use of secure tunneling
* Protect all your IoT devices and ensure their security

**Conclusion**

Even if you implement all above mitigation and security precautions, there is always a significant chance or risk due to a plethora of device entry points connected with satellite communication systems. Satellite technology must provide seamless integration with public and private networks and flexibility to protect and connect to satellite system configuration. It’s also important to look for an easy to deploy, affordable solution to make it attractive for small satellite companies unlikely to have cyber-security practices in place. Communication satellites build an interconnected network between organizations and for mitigating infiltration risk into the ecosystem, it’s important to protect all the entry points.