ESOA
EMEA SATELLITE OPERATORS ASSOCIATION

Satellites & CYBERSECURITY

As the global reliance on information communication technologies increases, so do the cybersecurity challenges to national and global infrastructures.

The satellite industry has a proven track record in providing secure solutions well beyond those of other commercial communications technologies. Satellite operators lead in key areas essential to effective cybersecurity including encryption, subscriber management, access control, and overall system robustness.

Global Challenges | Satellite Answers

www.esoa.net

Space technology increasingly relies on digitization, which is at the heart of cyber technology. Digitization brings with it potential cyber vulnerabilities which can be exploited to cause serious harm to national and global infrastructures. As the number of satellites and their applications continues to rise, so too will our dependency upon them and in parallel the cyber threat will grow.

Satellite operators therefore employ maximum efforts to ensure:

- The highest standards of integrity, reliability and confidentiality of the data being carried over their systems
- The security of the ground segment, both physical and virtual
- The security of satellite control systems and space craft

The cybersecurity of satellite networks is ultimately the responsibility of all operators, regardless of size and regardless of whether they are legacy operators or new 'budget' entrants.

The most secure sectors in the world rely on satellite:

Governmental entities in charge of civil, public safety, peacekeeping or military sensitive operations are all users of satellite communications. Defence operations in particular have seen a huge increased dependency on secure satellite communications in recent decades. The requirements of these sectors are the most stringent in terms of data confidentiality, integrity and availability (CIA). Users of satellite networks often make life-and-death decisions based on the data transiting across these networks. Accordingly satellite operators are vetted and able to ensure their signals can be encrypted to a military grade.

Critical National Infrastructures such as energy, finance and defense systems all have space technology integrated into them. In some cases, satellites provide vital timestamps for transactions or synchronization of systems to avoid their failure, in others they enable life-saving and secure communications without which users, often in critical circumstances, would be cut-off entirely. Sometimes, satellites provide the only means of monitoring and early-warning of risks that could prove fatal to the environment or to human life. Any vulnerabilities affecting assets in space can therefore have far-reaching consequences on systems that allow for the safe and stable functioning of society as we know it.

The security of satellite systems in space goes directly to the security of multiple systems and economies on earth

How the Satellite Industry Employs Cybersecurity Practices

While no system can be assumed to be absolutely secure, each satellite network operator's commitment to security helps propel the satellite ecosystem forward. This ecosystem includes software vendors, equipment manufacturers, service providers and customers, working together to improve their collective security risk profile and safeguard networks, services and users from any attack.

There is a need for uniform cybersecurity regulation

While policymakers and CERTs[1] around the world collaborate to secure the global Internet, cybersecurity regulations remain fragmented. The nature of satellite networks is however global, covering large portions of the Earth while ground stations and users relying on the same network may be thousands of miles apart. In the case of maritime and aeronautical broadband coverage services (Earth Stations in Motion) for example, users may be in international territory or flying over a variety of countries between departure and arrival. Compliance with a patchwork of cybersecurity regulations, which may even conflict with each other, thefeore becomes an onerous task.

Regulation needs to keep pace with technology advancement

The satellite industry is bringing millions of new users online across the world, and in doing so, is transforming the lives and economic conditions of people across the globe. The acceleration of the satellite sector's ability to connect more and more people is due largely to recent innovations over recent years. The speed with which technology advances means it can be difficult for regulation to catch up and be effective.

Cybersecurity solutions are not 'one-size-fits-all'

Networks differ, risk profiles vary, attack vectors continue to change and the way potential vulnerabilities can be addressed evolves constantly. Therefore, to be effective, satellite providers, resellers, software providers and equipment manufacturers must be free to apply security strategies that fit their individual security profiles and preferences[2] .

The satellite industry is uniquely positioned to:

- Detect and respond to cyber threats to defend against adversaries' attacks
- Gather cyber threat intelligence to understand the ever-changing threats
- Engage in security-focused engineering to build and optimize secure networks
- Implement cybersecurity tools, tactics, and procedures
- Manage supply chains for network equipment and software

Each satellite network builds on industry best practices to operate and design solutions and systems for providing network security. Most satellite operators run their own Security Operations Center (SOC) in which network traffic, emerging threats and cyberattacks data can be processed, and responses can be activated.

[1] Computer Emergency Response Teams

[2] https://www.esoa.net/cms-data/news/SIA-GVF-ESOA%20Joint%20Cybersecurity%20Policy%20Statment%20May%202018.pdf

Cybersecurity and Quantum Key Distribution

Quantum Key Distribution (QKD) will be increasingly relevant to the security of future communications. With its inherent security features, hacking or eavesdropping satellite data transmission is extremely difficult, particularly in point-to-point or private circuit operation. Distributing quantum keys via satellite is therefore inherently more secure. Satellite operators are proactive in the design & adoption of innovative technology solutions. Diverse initiatives around satellite and QKD exist. SES is leading activities in the EuroQCI[3] consortium to implement the first European end-to-end Space-Based Quantum Key Distribution (QKD) in-orbit validation systems for the EU Commission, with the support of the European Space Agency and EU Member States. Hispasat aims to deploy the first QKD payload on a Geostationary satellite.

The satellite industry implements best practices for cyber security, combined with their own additional solutions to meet customers' needs

Operators lead voluntary efforts to manage risk, address cybersecurity challenges and secure supply chains at the national and international levels:

- **Embracing the risk-based model for understanding and mitigating cyber threats:**
  The ISO 27001 series provides guidance on estimating and protecting against cyber risks. Similarly, the U.S. National Institute for Standards and Technology (NIST) proposes five key functions for a Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover.[4] These frameworks are championed in many countries providing guidance to industry and other stakeholders on how each network operator can determine its risk profile and then secure its network: they allow industry actors to innovate. Given the international application of these standards, it is unnecessary and even counter-productive, for additional international bodies to set cybersecurity technical standards.

- **Avoiding box-checking "one-size-fits-all" regulatory regimes:**
  Cybersecurity regulations must be considered carefully. Satellite networks are global and rely on both space and ground assets, in a wide variety of configurations. "One-size-fits-all" prescriptive measures will too often end up being complex, expensive, and ultimately unwieldy and ineffective at solving any problem. When prescriptive measures are adopted, entities spend too much time ensuring their compliance and are unable to invest in security innovations or are forced to leave the market altogether. Neither of these outcomes is healthy for the marketplace and may reduce the security options available to consumers.

A risk-based model is far better suited to ensuring appropriate security measures are taken by telecommunications, including satellite, network operators.

All actors in the satellite supply chain work hand-in-hand to ensure their requirements for network hygiene, encryption and network monitoring are incorporated into network design, deployment and operation.

[3] https://spacenews.com/europe-picks-euroqci-satellite-quantum-communications-consortium/
[4] https://www.nist.gov/cyberframework/online-learning/five-functions

- **Working with customers, users, suppliers and partners to ensure secure supply chains:**
  Given the reach and complexity of satellite networks, the value chain necessarily includes a variety of actors. Satellite network operators partner with customers to provide security services, train end users on cybersecurity issues, and share intelligence when appropriate. Because satellite network customers frequently have specific security requirements, operators meet and very often exceed their expectations. National policy objectives should facilitate supply chain security by ensuring that risk intelligence is shared to help industry make sound risk-management decisions, and by prioritizing secure communications supply chains in its own procurement, to foster economies of scale of robust and secure equipment.

Leveraging technology within the expertise of satellite network operators

- **Content monitoring is not part of cybersecurity:**
  Content monitoring may have policy rationales, but it is not an appropriate part of a cybersecurity regime. While network operators can identify trends and emergent threats in data streams within their networks, they are ill-suited to be the primary monitors or enforcers of content policy. One good reason for this is that increasingly network traffic is encrypted end-to-end, which means that network operators are merely providing a "pipe" and have no access nor any control whatsoever in what data is carried through it. Content monitoring is hence better suited for other actors in the Internet ecosystem, allowing network operators to focus on securing the network itself against malicious actors.

- **Building networks that are robust, scalable and secure:**
  The satellite industry continues to evolve network design, advancing in throughput, performance and resilience in doing so. High-Throughput-Satellite (HTS) networks are essential to global connectivity and are driving revolutions in satellite architecture meaning that traditional gateways (large, remote, standalone terminals that create a single point of failure on the network) are progressively a thing of the past. The satellite industry is embracing 5G network function virtualisation, cloud and other software-defined technologies so that individual country access points are increasingly unnecessary, costly and inefficient. They also provide additional points of entry for bad actors because they may lie outside of the direct management of the network operator. Newer network architectures are improving the resiliency and cybersecurity of the network, while also providing sufficient technical means for data-sharing with law enforcement and other entities, where appropriate. QKD will also bring new capabilities to considerably upgrade the resilience of satellite networks.

- **Ensuring the right regulatory balance:**
  In view of the satellite industry's role in supporting numerous critical services, it should be included in cybersecurity policy planning, rather than itself being singled out as critical infrastructure beyond other ISP networks. To create separate, more restrictive rules for satellite operators would hamper their ability to manage their risk and focus on critical elements of security.

Voluntary information sharing, capacity building and an international norms framework all support robust cybersecurity and supply chain security

- **Capacity building to prepare the ecosystem for major attacks:**
  The satellite industry fully supports building trust through capacity building, tabletop exercises and policy planning on cybersecurity issues at both the national and regional level. The International Telecommunication Union (ITU) plays an important role in capacity building on cybersecurity and should continue to do so, being mindful however not to assume a standards-setting role, or establishing regulations or other cybersecurity governance measures which should remain the domain of expert cybersecurity bodies.

- **Supporting cybersecurity and law enforcement agencies:**
  National and regional CERTs are essential in defending citizens and networks against malicious actors. ESOA members support their work where appropriate, providing information about threats and helping entities recover from attacks. The disclosure of information about threats, risks, business processes or capabilities by operators should respect commercial sensitivities. Formal and informal groups, such as the Space Information Sharing and Analysis Center (Space-ISAC[5]) or the European Network and Information Security Agency (ENISA), are helpful intermediaries to circulate intelligence without compromising individual members' positions.[6] It is essential to continue to foster such voluntary partnerships to ensure the cybersecurity of telecommunications networks.

- **Supporting the creation of international norms:**
  A norms-based ecosystem assists in reducing the risk of conflict in cyberspace and provides opportunities for de-escalation, which reduces the threats to telecommunications networks. ESOA members have long complied with information security risk management principles, such as the ISO 27001 standard or the U.S. NIST Cybersecurity Framework cited above. ESOA urges countries to adhere to norms for behavior in cyberspace, including, those of the 2015 UN Group of Governmental Experts (UN GGE).[7]

Conclusion

Each satellite network operator has a unique set of requirements for their cybersecurity practices to address the needs of their customers. A flexible regulatory environment that allows for tailored cybersecurity services can result in improved services for end users. Best practices that today guide the satellite industry's cybersecurity practices should be adopted more broadly to promote the further development of the satellite industry and thesecurity of its networks.

[5] https://s-isac.org
[6] ENISA on Information sharing: https://www.enisa.europa.eu/publications/good-practice-guide
[7] https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174