Innovators from the private sector like Elon Musk and Jeff Bezos have come up with projects like SpaceX and Blue Origin, which gives a hint of the possibility of outer space travel during our lifetimes. In November 2021, SpaceX launched 53 Starlink highspeed internet satellites into the space. It plans to launch a total of 12,000. Amazon leadership has also anticipated to invest more than 10 billion dollars for building a network of 3,236 low earth-orbit satellites. Furthermore, Boeing also plans on launching 147 satellites. With increased coverage, high-speed broadband will be provided to users irrespective of their location.

However, with software and digital technology required to make this possible, it is important to assess these from the perspective of cybersecurity. Even now, satellites sometimes transmit data that is of sensitive nature, which makes them potential targets for cyber criminals. Moreover, only because a satellite is in its orbit does not mean that the facilities at ground station cannot be targeted by cyber criminals.

Cybersecurity experts have already warned that the world is not prepared for natural disasters or cyber threats on space infrastructure, which can damage critical systems including those used for routine communication. Space cybersecurity is now more important than ever, and space organizations like NASA are playing their part in keeping things secure. It is very important to make effort at global level to create a robust network that allows free flow of information between independent teams in different regions of the world.

To make space communications and infrastructure safe will require new partnerships and innovative thinking. Making space the next frontier for cybersecurity requires recognition of challenges, implementing regulatory frameworks that are space-oriented, and improving current cybersecurity measures.

**Challenges of Space Cybersecurity**

The threat of cyberattacks has still not proved a reality for many in-service satellites. The reason is that some of these were manufactured and made operational way before cybersecurity became a prevalent phenomenon. These satellites, however, are vulnerable with their hardcoded credentials and the companies that manufactured them itself are not able to change those.

However, [technology](http://www.cardzgroup.com/ContactSmartCard.html) and space industry depend upon the same infrastructure in many ways and undergo similar functions of our digital world. When we talk about space, the real challenge arises from distance, equipment functioning, distance, and criticality of systems. Our dependency on satellites is both a vulnerability and an asset. On one hand, we benefit from their capabilities in instances such as weather emergency or an air crash investigation. On the other hand, malicious enemy can misuse the same for spreading mass destruction. The severity of impact can also be far more disastrous than any security breach in terrestrial systems. For instance, if a hacker penetrates earth-based system and provides false information to a satellite, it can potentially result in an inter-space collision causing global communication systems to crash. Satellite collisions are also a growing concern as their number has increased in space.

Moreover, as more private organizations and governments are involving themselves in space projects, more hackers are getting potential access points. It is no longer only NASA that needs to be safeguarded from potential attackers. Hackers now have a multitude of options to target and attack, from equipment manufacturers to governments to other stakeholders in the entire supply chain.

Lastly, with advanced technology such as quantum computers that cyber criminals can use for hacking, there exists a bigger risk for space-based ecosystems to face threats from the cybersecurity perspective. With space militarization and tourism becoming potential realities, the hackers are also likely to recognize the monetary potential of ransomware and other cyber attacks. All this combined with the lack of international cooperation in cybersecurity regarding space technology, the next few decades will see excessive hurdles that need to be eventually catered for.

If cyber criminals are able to compromise satellite-based stations and spread malware through a satellite network, they can acquire the potential ability to target thousands of users or launch DDoS attacks to hamper important communications. Although it is possible that hackers find vulnerabilities to exploit in the satellites, but there is a very slight chance of that. The threat lies more in the low-lying fruit, in this case the base stations between two points. These stations have fixed transceivers that send and receive wireless signals and act as main points of communication. Essentially, these are Operational Technology (OT) environments in highly remote locations. This makes them potentially bigger targets in future.

It is already obvious that bad actors consider Operational Technology as a potential target. This is because any cyber disturbance in an OT network can have a huge impact, much more than a typical IT attack. Many ransomware cyber attackers find their targets in energy and transportation, manufacturing, and automotive industries – which are Operational Technology environments. Operational Technology vulnerabilities are also being increasingly identified by threat actors, built into exploit tools, and sold on dark web. This has made it easier for cyber criminals to search for and to exploit Operational Technology devices that are already exposed.

**How Can the Industry Make Space Safe?**

The industry now realizes these threats and is beginning to work towards protection of space software, communications, and equipment from increasing cyber threats. The most important step is to follow upfront cybersecurity accountability from the start. This does not only hold true for hardware and space equipment, but also for software and operating systems that will be used by rockets, satellites, and shuttles. It is also easier for software developers and space engineers to follow the product-functionality approach. However, it is very important to focus on security during all the process phases.

Lastly, the public and private sectors should come together and collaborate and carry out real-world cybersecurity simulation exercises and scenarios before sending the equipment into space. They need to have exhaustive drills for breach response and penetration testing. Once the equipment goes into space, it is extremely hard to control in case of an actual data breach.

**How Regulatory Bodies and Frameworks can Play a Role**

International bodies and governments should develop a global standard for technology that is hackproof throughout the supply chain of space. Moreover, current cybersecurity standards can also be enhanced for further securing the space ecosystem. One of such solutions is the zero trust architecture. This means that all equipment and devices are impenetrable, which limits users from any unauthorized access inside or outside the organization.

Because of the decentralized nature of zero trust architecture, it is next to impossible for a hacker to gain access to space equipment even after gaining access to terrestrial systems. Hence, it would not be wrong to say that zero trust lessens operational risk.

In this regard, the National Institute of Standards and Technology (NIST) can play a major role in developing and implementing standards for space cybersecurity framework. NIST has already introduced a [document](https://csrc.nist.gov/publications/detail/nistir/8270/draft) on commercial satellite operations can implement cybersecurity standards.

**Future Thoughts**

As the private sector is making more endeavors into space, it is anticipated that our future terrestrial economy will largely depend upon space technology. Though the challenge of protecting space infrastructure from cyber criminals is hard but it is not impossible. By making use of current public-private partnerships and creating globally adoptable frameworks, it is possible to secure the next frontier from cyber crimes.