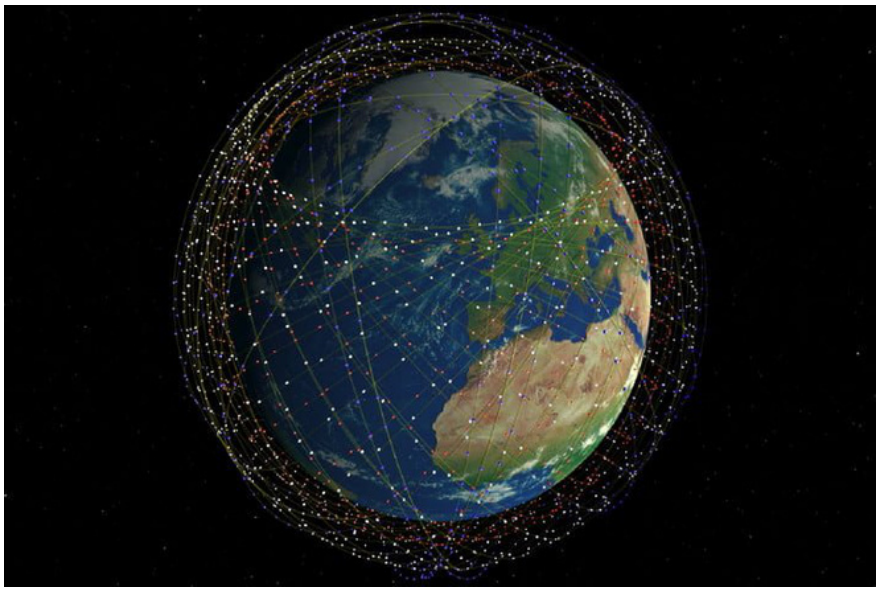
Elon Musk wary: Experts warn low-cost satellites to flood the Earth's orbit will be a 'lucrative' target for hackers

Controlled satellites can become a hacker weapon.

In the first month of 2020, SpaceX became the largest company operating the number of satellites operating in orbit. By the end of January, the company had 242 satellites orbiting Earth and also plans to launch 42,000 satellites over the next decade.

This is part of SpaceX's ambitious project to provide high-speed wireless internet around the globe.However, this race is not only SpaceX alone, but also Amazon of the United States, OneWeb of England and other companies are also trying to put thousands of satellites into orbit in the coming months.



Expected Starlink system of SpaceX

These new satellites are able to revolutionize many aspects of everyday life - from universal internet access to environmental monitoring and improved global positioning systems. But the race also presents potential dangers: most low-cost commercial satellites lack network security standards and regulations.

A scholar specializing in cyber conflict, Dr. William Akoto is acutely aware of this danger.Because satellites are made by a chain of component suppliers, it is difficult to synchronize security, so they can be completely hacked.

If hackers take control of these satellites, the consequences will be catastrophic.On a simple level, they can disable satellites and deny manufacturers access to the service.

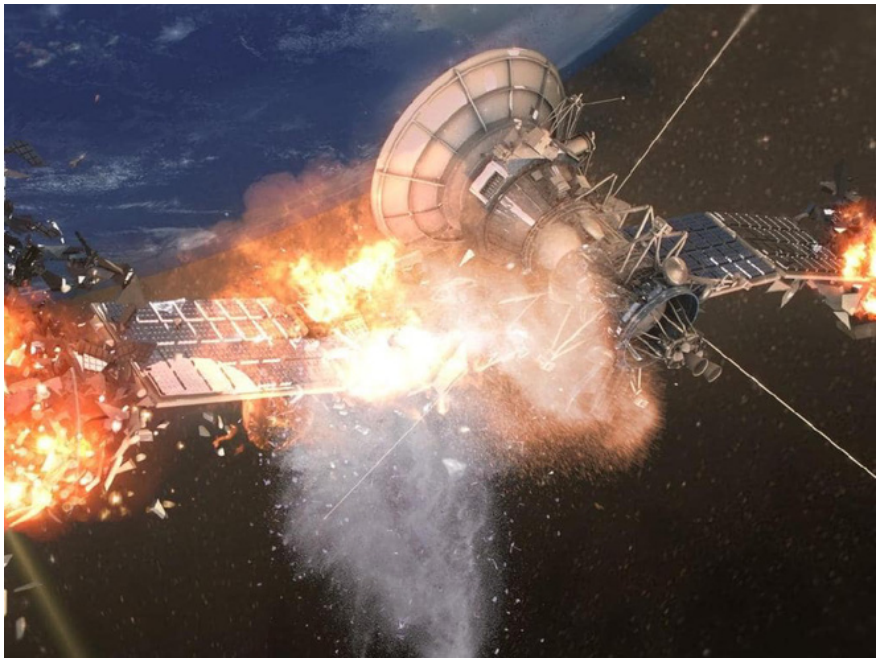
Hackers can also use satellites to jam or tamper with signals, creating devastating damage to infrastructure, including power grids, water networks and transportation systems.

One of the new generation satellites has jetpacks, allowing them to increase or decrease speed and change direction in space.If they are taken over, the consequences may be unimaginable.Hackers can change the trajectory causing satellites to crash into each other or even the International Space Station.

Here is a series of comments as well as how to deal with future hackers, according to the article of Dr. William Akoto published in The Conversation.

Civil satellites are not concerned about security

These cheap satellites, especially CubeSats - small satellites with not too complicated technology, carry many security holes.Many of the technology components that make these satellites rely on open source, hackers can take advantage of those loopholes to create backdoors.



The high-tech nature of satellites is just about manufacturing, building different components and trying to get them to space, because these processes involve so many companies.

Once in space, the satellites are rented by third party companies for daily management.Every time a new provider is added, access will be broken down, which will increase security holes.

Hacking some of these CubeSats can be very simple, for example a hacker will wait for one of them to fly over his head and then send malicious code using a dedicated ground antenna.This is even possible for more sophisticated satellites.

Or hackers can use the most 'classic' way: Hack into the computers themselves of the earth station, which controls the satellites.

Past satellite attacks

In 1998, hackers took control of the United States-Germany's ROSAT X-Ray satellite.They did it by hacking into computers at Goddard Space Center in Maryland. Hackers have driven satellites pointing solar panels directly at the sun, causing them to 'cook' and turning high-tech satellites into useless iron lumps. The satellite fell to Earth in 2011.

Following 1999, the UK's SkyNet satellite was taken over and taken as a "hostage" for ransom.

Worse cases began in 2008, when hackers took complete control of two NASA satellites, one out of control for about two minutes and the other for nine minutes. In 2018, another group of hackers launched a sophisticated hacking campaign targeting U.S. satellite operators and defense contractors. Then came the attack of hacker groups from Iran.

Although the Department of Defense and the US National Security Agency have made some efforts to address cybersecurity, the deployment speed is still very slow.So far there is no network security standard for satellites and no regulatory authority to regulate and ensure cybersecurity for host companies.

Even if common standards can be finalized, there is no mechanism for the government to enforce them.This means that the responsibility for the cybersecurity of satellites depends entirely on the individual companies that build and operate them.

Unstable race in space

When SpaceX and its competitors compete to become dominant orbitals, they will have to cut costs to race, along with the pressure to speed up development and production.This makes fields like security less likely to be cut and less invested.

Even for companies with high security technologies, the costs associated with securing each component may not be preferred.This problem is even more serious for low-cost space missions, as the amount invested in cybersecurity can exceed the cost of the satellite itself.

If a satellite is managed by multiple companies, then the responsibility of the stakeholders will be very vague.This lack of clarity will create heartless psychology and hinder efforts in ensuring network security.

Required rules are required

A number of analysts have begun to support the government's strong involvement in the development and adjustment of network security standards for satellites and other assets in space.

Congress can pass a comprehensive legal framework for 'space trade'.For example, they could pass laws requiring satellite manufacturers to develop a common network security architecture.

Congress can also manage reports on all incidents of satellite network security breaches.And the need to give extra priority to keeping satellites in orbit.

The United States has established space forces: Space Force.

In addition, companies should be held accountable in their fight against hackers, which will be essential for them to take measures to enhance the security of their systems.

Before these problems can be solved, we can only hope that there will not be another attack on orbiting satellites, the security of cyberspace is very much dependent on the security of the network. Internet hovering in space.