<https://github.com/Kosuke9311/Data-communication-CS320/wiki/Report>

# Cyber Security in Satellite Communication



## Abstract

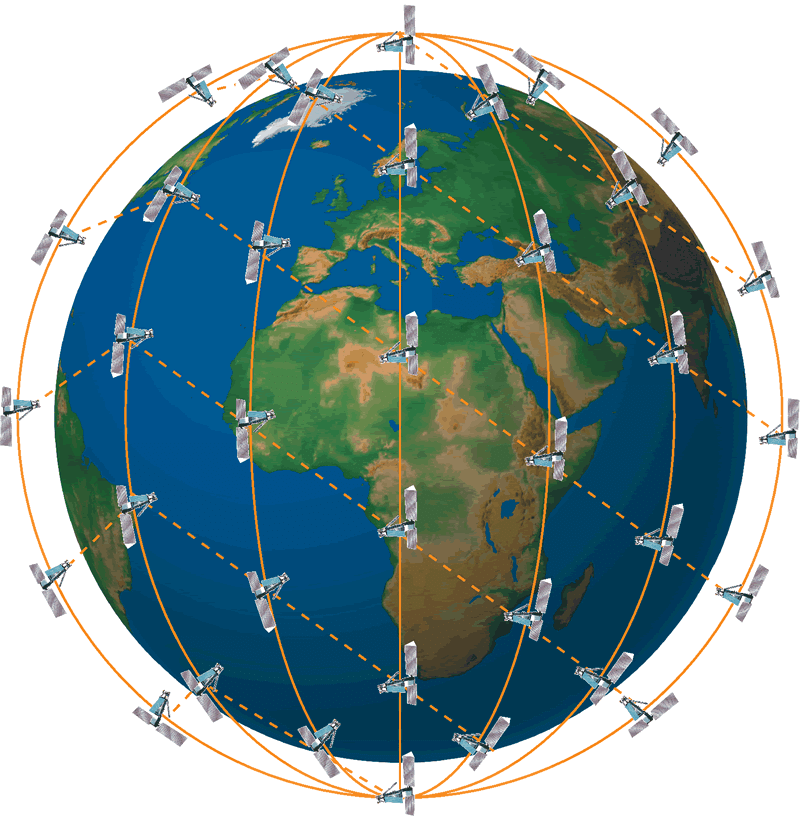
Satellite data communication has become an indispensable technology in our lives, and technology continues to develop as a revolutionary technology for long-distance communication due to its low geographical disturbance. It can help you to make a phone call with a friend in a foreign country and to watch sports games. Data communication via satellite have the ability to make our life happy and comfortable.  
However, as satellite communication becomes more developed and handles more important information, the risk of cyber-attacks will increase and be more dangerous. People need to find and improve the vulnerability of cyber security of space communication. This report explores the type of cyber-attack against satellite communication and how to protect it.

## Introduction

People need to consider cyber security of space objects seriously and to come up with a plan to deal with this. In the present day, with the miniaturization of communication satellites and increase launches by many companies all over the world, satellite communication is beginning to be expected as an important social infrastructure. I believe that this is due to the formation of a social vision that is based on communication infrastructures, such as the 5G (fifth-generation mobile communications system), the GPA (Global Positioning System), and the IoT (Internet of Things), which has been spreading around the world. While they make society more convenient and progressive, they also have the potential to have a huge negative impact on society if they are misused.

## The Risk of Satellite Communication

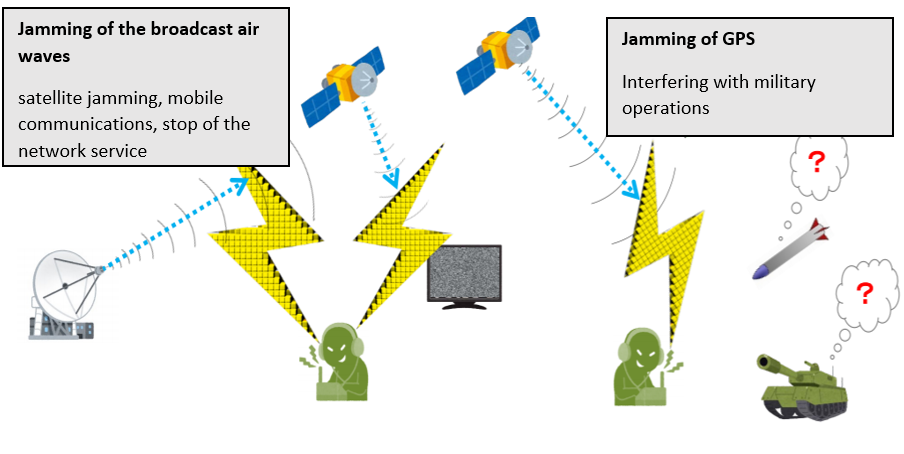
### Satellite Constellation Design

The communication service by communication satellites exists everywhere, such as the Internet service in the plane and TV program on BS. These are provided by the geosynchronous satellite, and in this way, there is a disadvantage of slow communication speed due to long distance from the ground to satellites. On the other hand, Satellite Constellation Design has the ability to communicate faster than geosynchronous satellites because its satellites stay closer to the ground. Moreover, in this design, many satellites are constructed as a group and switch them based on the location to interconnect, so each satellite is cheaper and doesn’t have to require high quality.

### Types of Risk

The satellite system could be bigger and bigger, and all of them are connected to the network. As time passes, the number of aging and less secure satellites will increase. Furthermore, many companies all over the world launch satellites, and they might produce satellites with less security or traps like a backdoor. These things cause to be an easy target to be attacked by hackers, and one vulnerable in the system can have a bad impact on the entire system. Hackers aim to not well-defended military satellites but commercial ones. They discover a point of vulnerabilities and eventually take over the entire infrastructure, including the satellite constellation and the ground network.

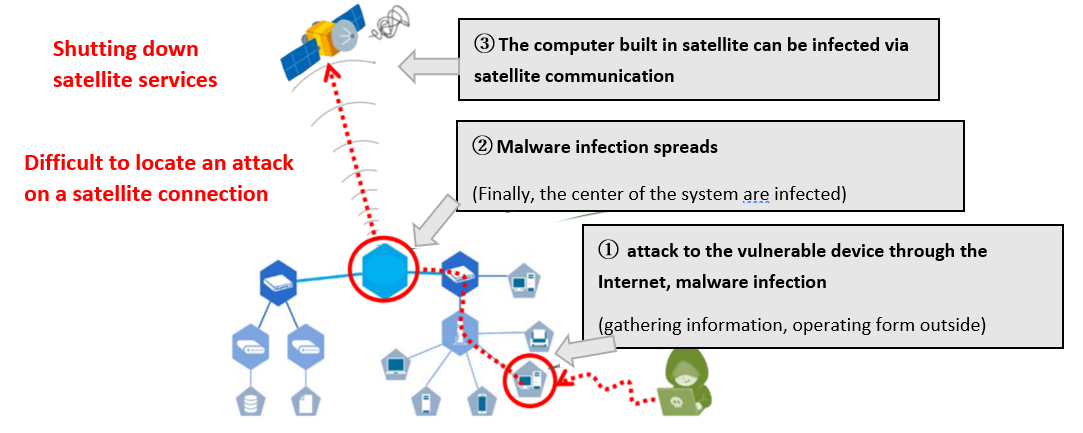
#### Jamming

Jamming is that interferes with the normal communication of the other side by humming or jamming the radio waves by the signals with the same frequency. 

##### Case

**Iran (2003)/ Jamming of broadcast airwaves**  
An Iranian company jammed the British human rights group’s satellite broadcast airwaves to Iran.  
**Iraq (2003)/ Jamming of GPS**  
The U.S. military destroyed sic GPS signal jamming devices for the Iraqi Army’s guided weapons. Numerous cases of GPS signal jamming by such devices during the 2003 Iraq war.

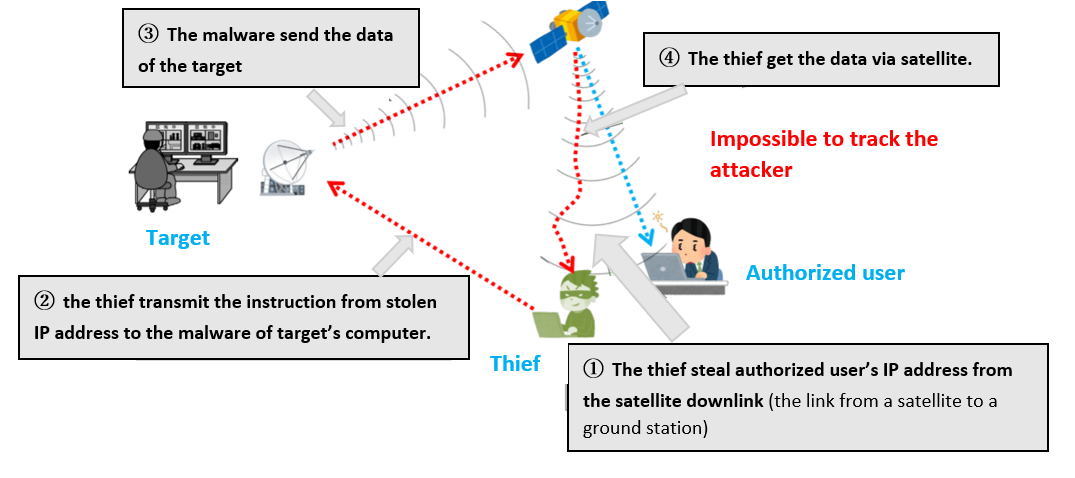
#### Cyber-attack (from The Ground)



##### Case

**America (2014)**  
The U.S. National Oceanic and Atmospheric Administration's (NOAA) weather observation network has been compromised by hackers who are suspected to be Chinese.  
The data was hacked and temporarily disabled. It is not known what data was stolen, but weather data from NOAA's satellites was hacked. This includes important information used for hurricane predictions and other purposes, as well as for distribution to other countries.

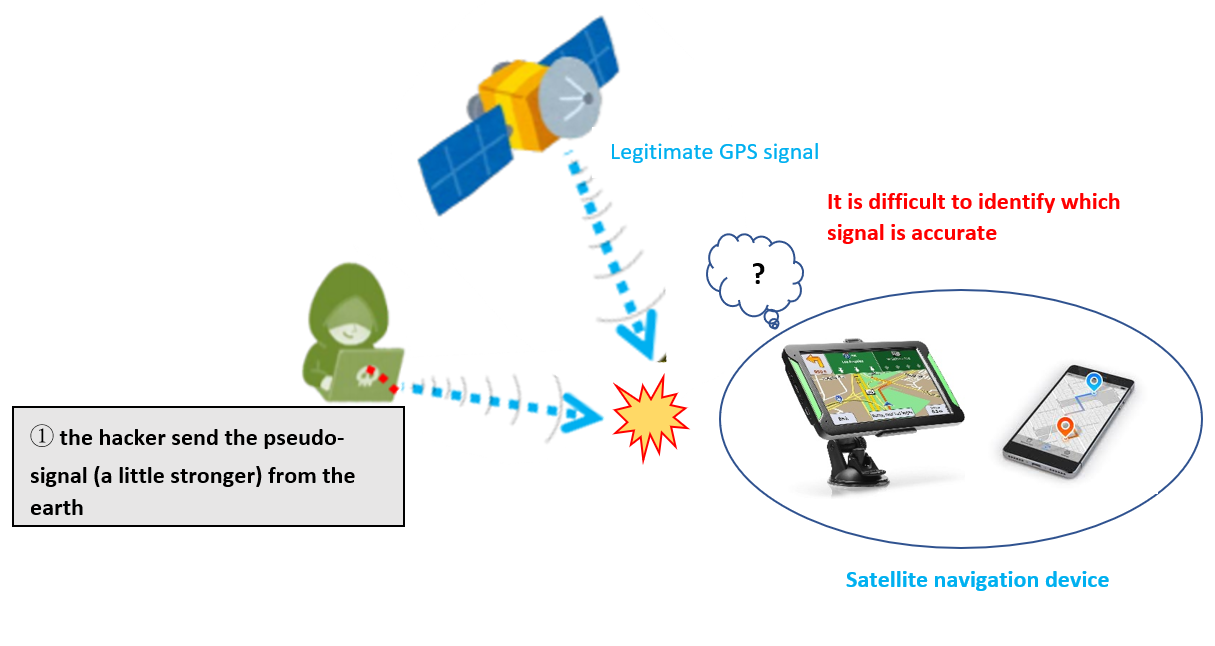
#### Cyber-attack (Misuse of Satellite Communication)



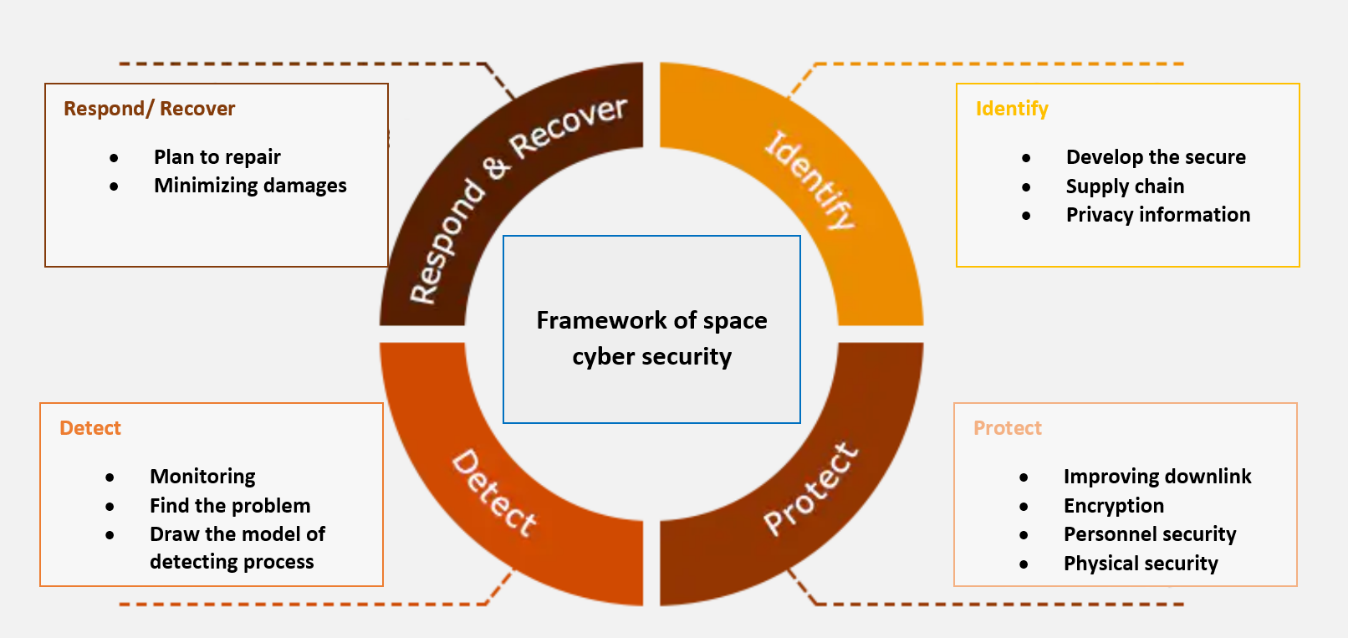
##### Case

**Russia (2015)/ Infiltrate Their Networks, Spy**  
Cyber-attacks by the Turla, cyber spy group, believed to be related to Russia. The malware was infected by government agencies, the military, educational and pharmaceutical companies in more than 45 countries.

#### GPS Spoofing



## How to Prevent Them

 Cyber-attack methods are becoming more sophisticated every day, and the entry of start-ups, the use of commercial products, and the shift of ground stations to the cloud have increased the vulnerability of cyber-attacks and made it more difficult to identify cyber risks.

### Jamming

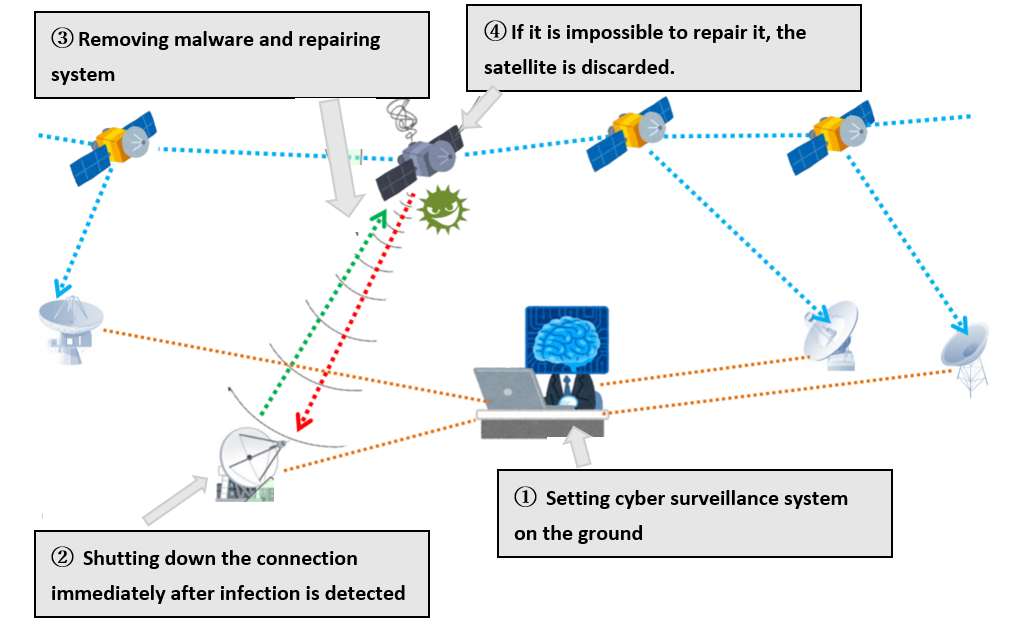
* **Preparing and switching multiple frequency channels accordingly**
* **Switching communication routers (via other satellites) and changing communication times**
* **Receive signals from multiple GPS systems**
* **Filtering**  
  CIC filter: to increase the resolution  
  FIR filter: to improve the phase accuracy

### Cyber-attack and Spoofing

#### Primary things

* **built device supply chain properly**  
  When producing satellites, you should examine the vulnerability  
  It is encouraged to use the list in order to make sure of security
* **Device’s password should be changed**  
  Default passwords are changed before launching
* **In space, activating sagely and manage equipment**  
  Periodically, send new passwords from the ground station through private connection  
  Periodically, check the devices

#### Monitoring and Removing Malware



## Conclusion:

Safety and security satellite communication systems are essential to achieve innovation for infrastructure including space. The ways of attack get more and more sophisticated as the technologies grow up, so people should keep changing and updating the security systems. Anyway, satellite data communication will be greater and more interesting, so we can’t take our eyes off its amazing development!!

## References

* Unsecured satellite communications present a gateway to hackers <https://www.securityinfowatch.com/cybersecurity/article/21144996/unsecured-satellite-communications-present-a-gateway-to-hackers>
* Protecting everyday life – How Airbus protects satellite systems against attacks <https://airbus-cyber-security.com/news/protecting-everyday-life-how-airbus-protects-satellites-against-attacks/>
* Why Satellite Cybersecurity Must Be Prioritized in the New Frontier <https://www.nextgov.com/ideas/2020/05/why-satellite-cybersecurity-must-be-prioritized-new-frontier/164977/>
* Why Satellite Security is Important <https://threatmodeler.com/why-satellite-security/>