Forum: Economic and Social Council (ECOSOC)

Issue: Creating Standards for the Protection of Satellite Networks

Student Officer: Klára Blaškovanová

Position: Chair of the ECOSOC

Table of Contents

I. Introduction

In the modern era of relentless technological advancement, satellite networks have evolved to serve a crucial role in communication, navigation, or observation systems. These intricate systems are the very backbone of our interconnected world, playing a role in GPS navigation, banking transactions, or climate change observations. This; however, gives rise to intentional attacks on such systems and their functionality.

The use of artificial intelligence and machine learning keeps increasing the complexity of cyber attacks and current defense mechanisms are becoming insufficient for mitigating the danger. Disturbances to satellite systems can negatively influence the world economy and diplomatic relations between countries.[1]

Additionally, a different possible threat is the use of nuclear weapons in space. Although the Outer Space Treaty was ratified in 1967, prohibiting nuclear weapons or other weapons of mass destruction in space, there are speculations about the development of such weapons that could destroy targeted satellites. The extent of a nuclear detonation is enormous; satellites on the other side of Earth might suffer damage to their electronics due to the released radiation.

It is for these reasons extremely important to focus on this issue and find long term solutions for satellite protection.

[1] Kaczmarek, S. (no date) Cybersecurity for satellites is a growing challenge, as threats to space-based infrastructure grow. https://theconversation.com/cybersecurity-for-satellites-is-a-growing-challenge-as-threats-to-space-based-infrastructure-grow-223877.

II. Definition of Key Terms

A. Satellites

Satellites are objects created by humans that are sent up to space for various purposes such as the collection and transmission of information. There are Low Earth Orbit satellites (LEO) situated 600-1500 km above ground, which usually create mesh networks. Medium Earth Orbit satellites (MEO) orbit around 10 000-20 000 km above ground, and Geostationary satellites are 37 500 km above ground. Unlike LEOs and MEOs, Geostationary satellites travel at a speed that matches the Earth's rotation and therefore stay in a fixed location relative to the Earth.[2]

B. Internet broadband

High-speed internet connections that are "always on." They can be provided through cable, DSL, fiber and satellite.

C. Cyber security standards

A set of guidelines for companies on how to implement and manage security controls to protect the cyber environment of a product and its user. There are four types of security: application security, network security, cloud security and cryptography (encryption). The two key standards to meet are ISO 27001 and ISO 27002, both issued by the International Organisation for Standardisation. However, considering the rapid advancements of hacking technologies, these standards are in need of improvement.[11]

A. Physical security

Satellite networks are not only exposed to cyber attacks. The danger of vandalism, sabotage or collision with space debris is very real and more light needs to be brought upon it when discussing the security of satellites, especially considering that no physical repairs can be done to the unreachable satellite.

B. Encryption

Encryption is a process of encoding information to increase safety. The original piece of information (plaintext) is converted to ciphertext before it travels to its

[2] Bagci, T. (2023) What is a Satellite Network? https://www.sysnettechsolutions.com/en/what-is-satellite-network/; Lesics (2019) How does Satellite Television work? | ICT #11. https://www.youtube.com/watch?v=OpkatIqkLO8.

destination. The goal is for the recipient to be the only party that can decipher the information back to its original form. The purpose of it is not to prevent interference, but to compromise the interceptor by making the information unintelligible.

C. Space weather

Space weather includes phenomena such as solar flares, geomagnetic storms, or radiation hazards. It is necessary to take these into account as they can also cause damage to satellites in orbit. One benefit is that it occurs naturally and has been occurring since the beginning of satellite development, therefore teams of developers already have some strategies to deal with such issues.

D. Jamming and spoofing

Both jamming and spoofing are techniques used by hackers to compromise satellite networks. Jamming is the intentional transmission of radio frequency signals to cause interference with the intended signals. The attacker emits signals of similar frequency and overpowers the original signal the satellite was receiving. This can lead to service outages, communication blackouts or compromised mission objectives.

Spoofing works on a similar basis. However, instead of transmitting nonsense signals to cause interference, the attacker generates counterfeit signals to confuse the satellite about time, its location, or authentication information. This can lead to a change in trajectory of spacecraft, or even allow unauthorized access to secure networks.

E. Ransomware

A type of malware that restricts access to personal information of a victim unless a ransom is paid. Sometimes the data is simply blocked, while in other cases the virus can cause a deletion of the data.

III. General Overview

A. History of Satellites

a. Space Race

The first ever objects sent to space were as a result of the Space race between the USA and Soviet Union. Sputnik 1 and 2 were Russian satellites

launched from Earth a month apart. The first one, launched on October 4th of 1957 was the first object put into orbit by humans and the second one, launched November 3rd successfully carried Laika, a Russian dog, into space. The sole purpose was to leave Earth's atmosphere, so there wasn't a return plan for either of them. The first American satellite Explorer 1 was launched on January 31st of the following year.[3]

b. Evolution of Satellite Networks

Not long after the first successful satellites, the goal was to enable communication of these satellites with Earth. Americans were the first to achieve this in 1958 with satellite SCORE. It managed to send a pre-recorded Christmas message from the president back to Earth. A lot of new technology was then tested in the year 1960. The USA developed satellites for observation of Earth, radio communication and telecommunication. In 1964, the first geostationary satellite was installed into space and provided live television coverage of the 1964 Olympic Games in Tokyo. By 1970, more countries, such as Japan, Italy, Germany, Canada or Australia launched their first communication satellites.

Fast forward to the early 2000s, e-BIRD became the first successful satellite to provide internet broadband. From the year 2014 onwards, in-orbit spacecraft have been increasing rapidly as a result of satellite constellations; companies such as SpaceX, Amazon, or Telesat have started launching their own satellites into space and creating satellite constellations. Technology keeps advancing and the current trend in the world of satellite networks is developing nano satellites and ways to efficiently place them in orbit.[4]

B. Attacks on Satellite networks

Initially, the main vulnerability of satellites was physical tampering and espionage. As much as this remains a valid issue to this day, cyber attacks have become the main safety threat of these networks. The hacking of a US-German satellite in 1998 is famous for being one of the first successful cyber attacks. Allegedly, a Russian hacker managed to gain access to NASA's computer network and intervened with the altitude

[3] https://www.jpl.nasa.gov/ (no date) An early history of satellites timeline. https://www.jpl.nasa.gov/infographics/an-early-history-of-satellites-timeline.
[4] Ground Control (2024) A brief history of satellite communications | Ground Control. https://www.groundcontrol.com/knowledge/guides/a-brief-history-of-satellite-communications/.

control system, changing the alignment of one satellite which caused permanent damage. Such crime fueled research into better cybersecurity, but protecting satellites continues to be a race to outsmart the hacking technology that gets better and more accessible by the minute.[9]

The frequency of cyber attacks also rises. Smaller scale ransomware attacks such as jamming and spoofing of satellites can happen on a daily basis. Usually, the hacker manages to gain access to confidential information and only returns it after a financial compensation. Still, that doesn't mean that large compromising missions aren't happening. In February of 2022, right at the beginning of the war between Russia and Ukraine, the Viasat service used by the Ukrainian military was hacked, being marked as one of the most successful cyberattacks of the war. Since then, the military has been using SpaceX's Starlink as an alternative that has proven itself valid as it has withstood multiple attacks already.[5] Political use of cyberattacks is common and countries invest money into the development of better, more efficient anti-satellite weapons as it allows them to interfere with foreign threats.

Additionally, according to US intelligence, Russia is developing a nuclear powered weapon against satellites. If such concern was true, such weapons could cause damage on a much larger scale, possibly destroying many satellites at once.[6]

IV. Major Parties Involved

A. United States of America (USA)

The United States has a long history of satellite programs, starting with the Space race in the 1950s and '60s. These programs are led primarily by NASA for civilian space activities and by the Department of Defense for military purposes. The US is considered a global leader in satellite technology. As a part of cybersecurity laws and regulation, they have the Federal Information Security Management Act (FISMA) for the protection of government and critical infrastructure systems, which is much

[5] https://www.jpl.nasa.gov/ (no date) An early history of satellites timeline. https://www.jpl.nasa.gov/infographics/an-early-history-of-satellites-timeline.
[6] Davenport, C. et al. (2024) 'With a dire warning, concerns rise about conflict in space with Russia,' Washington Post, 20 February. https://www.washingtonpost.com/technology/2024/02/15/space-weapons-russia-china-starlink/.

needed as they have experienced attacks by state-sponsored actors or even hostile foreign governments (for instance the SolarWinds Breach in 2020).

B. Russian Federation

The Russian Federation also has space related missions dating back to the Soviet era of 1950s, being the first ever nation to launch a satellite into space. Roscosmos is the national agency responsible for the vast majority of satellite networks. Russia has a robust satellite infrastructure that is also protected by laws and regulations. However, the country has been accused multiple times of engaging in cyberattacks and conducting espionage to sabotage other nations' satellites.

C. China

China has emerged as a major player in space exploration and satellite technology, with the China National Space Administration (CNSA) overseeing the country's space program. They have enacted laws and regulations governing space activities, including the National Space Law, but similarly to Russia, China has been accused of engaging in cyber espionage and cyberattacks targeting satellite networks and space infrastructure, including attempts to infiltrate government and military satellite systems, disrupt satellite communication links, and steal sensitive information related to space technology and satellite operations. Although China is considered the dominant Asian country in terms of space programs, countries like India, Japan or South Korea are also strong players.

C. Satellite Companies

a. SpaceX

SpaceX, an American aerospace manufacturer and space transportation company founded by Elon Musk, has played a significant role in revolutionizing satellite networks. Known for its innovative approach and reusable rocket technology, SpaceX has rapidly expanded its Starlink satellite constellation, aiming to provide global broadband internet coverage. While SpaceX adheres to national and international regulations governing satellite operations, it faces scrutiny over potential cybersecurity vulnerabilities due to its extensive network infrastructure.

b. Telesat

Telesat is a Canadian satellite communications company that has been a key player in providing satellite solutions for communication, broadcasting, and broadband services. With a focus on delivering reliable and secure connectivity, Telesat operates a constellation of satellites to serve diverse market needs. Despite stringent regulations governing satellite operations in Canada, Telesat faces ongoing challenges in safeguarding its satellite infrastructure from cyber threats and espionage activities.

c. Satellite telecommunications company (SES)

Headquartered in Luxembourg, SES is a global satellite operator renowned for its extensive fleet of geostationary and medium Earth orbit satellites. Catering to various sectors including broadcasting, telecommunications, and government services, SES prioritizes security measures to protect its satellite networks. However, operating in a highly interconnected digital landscape, SES remains vigilant against cyber threats and espionage attempts targeting its satellite assets, despite adherence to national and international regulatory frameworks.

V. Timeline of Events

Date	Event
1957	Sputnik 1
1958	SCORE sends Christmas message from space
1964	First geostationary satellite
Early 2000s	e-BIRD becomes the first successful satellite to provide internet broadband.
Since 2014	Private companies begin to send increasingly more satellites.

VI. Previous and Possible Solutions

A. End to End Encryption

Proper end to end encryption (E2EE) provides protection of data while being transferred. Steps should be made so that it is accessible to all internet users and therefore the whole network becomes safer.

B. Hacking Contest

In a hacking contest, individuals try to find vulnerabilities in a system. They then give that information to the system operator. When the US Air Force organized a hacking contest in which competitors tried to hack into a real satellite in orbit. Three teams were announced as winners and received cash prizes. This way the US Air Force acknowledged the weaknesses of their satellites and adjusted their program to eliminate them.[7]

C. Detection of Suspicious Activity

A technique that could enable satellites to identify and mitigate an attack before it causes any damage is detection of suspicious activity. Monitoring tools, algorithms and analytics can be developed to be more effective in detecting such activities.

D. Authentication Protocols

Authentication protocols are mechanisms used to identify users or devices. In some cases, username and passwords are not sufficient for protection anymore and have to be paired with authentication through biometric data or digital certificates. Authentication also helps eliminate automated viruses trying to break into secured networks.

E. Immediate Response Plans

For larger scale cyberattacks, an immediate response plan is absolutely crucial to help minimize the detrimental impact. As of right now they are designed by individual companies and tailored to their specific needs related to the type of data they work with.

F. Legal Restrictions

[7] Wall, M. (2021) 'SolarWinds hack ‘a big wakeup call,’ NASA’s human spaceflight chief says,' Space.com, 26 May. https://www.space.com/solarwinds-hack-nasa-human-spaceflight-cybersecurity.

Legal restrictions encompass a wide range of mandates, including data protection laws (e.g., GDPR, CCPA), industry-specific regulations (e.g., HIPAA for healthcare, PCI DSS for payment card industry), and international treaties (e.g., Wassenaar Arrangement for export controls on dual-use technologies). These restrictions define the rights and responsibilities of organizations regarding data privacy, security, disclosure, breach notification, and cross-border data transfers. However, as technology evolves, laws also have to be updated to match the current trends and needs.

G. Limit Number of Satellites

Another possible threat to satellites is collision with other objects in orbit. Limiting the amount of satellites sent to space could decrease the chances of such an accident happening, while also decreasing the number of potential victims of a cyberattack.

H. Prevent the Deployment of Nuclear Weapons in Space

By imposing sanctions and punishments on countries that violate already set guidelines such as the Outer Space Treaty, the risk of countries like Russia or China using a nuclear weapon in space would decrease. More work could also be done to close possible loopholes in such treaties. This includes clarifying which specific military space activities are prohibited to avoid countries hiding military use behind dual-use technology. Another issue is that the Outer Space Treaty is outdated and may not take into account current technology connected to mini satellites or satellite constellations. Such work alongside negotiations could be done through an already existing UN Committee on the Peaceful Uses of Outer Space (COPUOS).

VII. Conclusion

Satellite networks have become an integral part of our world and their protection is essential. As these systems grow in size and complexity, safeguarding methods have to evolve along them to ensure reliability. The key to adapting to the ever-changing nature of satellite threats is to establish debates between main parties, governments and security experts. By not ignoring the protection of satellites, we can ensure the continued reliability,

integrity, and accessibility of satellite-based services for the benefit of humanity and the advancement of our exploration of the cosmos.

VIII. Questions to Consider

- What types of attacks or dangers are there to satellite networks?
- How do cyberattacks on satellite networks impact global communications, navigation, and space-based services?
- How do satellite operators and government agencies collaborate to mitigate cyber threats and safeguard satellite infrastructure?
- How do commercial satellite operators balance the need for innovation and competitiveness with the imperative of maintaining security and resilience?

IX. Sources for Further Research

- **Secure World Foundation**
  swfound.org
- **Space Policy Online**
  spacepolicyonline.com
- **NATO Review**
  www.nato.int/docu/review/articles/2023/10/24/protecting-our-critical-satellite-infrastructure-the-importance-of-space-based-infrastructure-to-humanity-and-its-status-within-nato/index.html

X. Works Cited / Bibliography

Bagci, T. (2023) What is a Satellite Network? https://www.sysnettechsolutions.com/en/what-is-satellite-network/.

Brumfield, C. (2022) 5 years after NotPetya: Lessons learned. https://www.csoonline.com/article/573049/5-years-after-notpetya-lessons-learned.html.

Davenport, C. et al. (2024) 'With a dire warning, concerns rise about conflict in space with Russia,' Washington Post, 20 February. https://www.washingtonpost.com/technology/2024/02/15/space-weapons-russia-china-starlink/.

Ground Control (2024) A brief history of satellite communications | Ground Control. https://www.groundcontrol.com/knowledge/guides/a-brief-history-of-satellite-communications.

https://www.jpl.nasa.gov/ (no date) An early history of satellites timeline. https://www.jpl.nasa.gov/infographics/an-early-history-of-satellites-timeline.

Kaczmarek, S. (no date) Cybersecurity for satellites is a growing challenge, as threats to space-based infrastructure grow. https://theconversation.com/cybersecurity-for-satellites-is-a-growing-challenge-as-threats-to-space-based-infrastructure-grow-223877.

KA-SAT Network cyber attack overview (2022). https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

Lesics (2019) How does Satellite Television work? | ICT #11. https://www.youtube.com/watch?v=OpkatIqkLO8.

London School of Economics and Political Science (no date) Cyberattacks on satellites. https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites.

Wall, M. (2021) 'SolarWinds hack 'a big wakeup call,' NASA's human spaceflight chief says,' Space.com, 26 May. https://www.space.com/solarwinds-hack-nasa-human-spaceflight-cybersecurity.

'What are information security standards? | RiskXchange' (2023) riskxchange.co, 15 February. https://riskxchange.co/1006780/information-security-standards/.

Menn, J. (2023) 'Cyberattack knocks out satellite communications for Russian military,' Washington Post, 30 June. https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/.

Tingley, B. (2023) 'These 3 teams just hacked a US Air Force satellite in space ... and won big cash prizes,' Space.com, 16 August. https://www.space.com/satellite-hacking-hack-a-sat-competition-winners.