BRIEFING NOTES

BN-71-Space and Cyberspace-Aug2021

CHALLENGES TO ENSURE SECURITY, SAFETY AND SUSTAINABILITY OF OUTER SPACE ASSETS

Authors: Parisa Yazdjerdi[1] and Kash Khorasani[2]
1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- Identification of three main challenges to ensure security, safety, and sustainability of space activities, namely (i) Governance, (ii) Information sharing, and (iii) Strategic stability.
- The space activities are mainly done by non-state actors which bring the challenge of **governance** at national and international levels.
- Accurate, timely and reliable **information** are required to be shared among spacecraft and satellites to ensure **safety** of their operations.
- **Strategic stability** of outer space should be preserved, in order for the nations to make sure that their space operations and facilities are in a safe, stable, and predictable environment.
- Need to explore reasons that could lead to a poor cybersecurity of outer space.
- Need to overview implementation of cyberattacks against outer space systems.
- Need to overview existing attack mitigation techniques in such systems and the existing mitigation techniques that are employed.

CONTEXT

Challenges

- Several academic institutions and private companies have steadily shown interest in planning and developing space related activities.
- Earth security is highly dependent on space security due to the growing reliance of our life style on space infrastructure.
- Existence of effective counter space capabilities such as kinetic anti-satellite systems, directed energy, radiofrequency, and cyber capabilities can result in spread of long-lived debris in space [1,2].
- On the other hand, defensive counter space capabilities are being developed by nations to ensure the security of their space activities and infrastructure.
- The safety and sustainability of space are not guaranteed in presence of offensive counter space capabilities. It is challenging to set clear international and national norms on development of counter space capabilities.

Poor Space Security: Reasons and Challenges

- Each component of a space system could be prone to cyber-attacks that can result in failure of the space system.

- Failure of the space system is considered as a single point of failure in engineering systems. For example, an attacker can compromise credit card service of a country by attacking the corresponding satellite that enables connectivity to the point-of-sale credit card systems [4].
- The usage of satellites is not monitored by any governing agencies and no enforcing mechanism exists to ensure their appropriate utilization.
- Since no policy, regulation, or rule exists in this regard, certain satellites may be used to launch cyber and kinetic attacks.
- Space assets are built and launched as a result of collaboration of many stakeholders and it can take a decade from the development time to the launch date. This results in unique challenges in introducing an up-to-date cybersecurity mechanism for space assets.
- Usage of open-source software (operating systems) in CubeSat class of satellites makes them vulnerable to cyber-attacks. These systems are cheap and highly demanding for any small company willing to launch a commercial CubeSat satellite. For instance, a hacker can cause a collision in the outer space by fooling a CubeSat [5].

Implemented cyber-attacks in space:

- Russian-based cyber-espionage group, Turla, has detected and stolen the IP address from the satellite Internet users and then initiated a TCP/IP connection from the stolen IP address. Attacker can then interrupt uplink or downlink in this case and inject false data [6].
- GPS Jamming and Spoofing are among the most common cyber-attacks that have occurred on GPS satellites by different countries such as Russia, USA, and Iran [7].
- GPS spoofing is the most dangerous cyber-attack as it can cause serious disasters in air, sea and ground based military services while it can remain undetectable [8].
- The U.S. government space systems which is controlled by NASA, and with their Earth observational satellites have been attacked several times and the attacker achieved full command and control of a satellite while it was remained undetectable [9].

Current mitigation techniques

- NASA enhanced the access control mechanism for its employees to reduce the chance of user's credential leak. The attack on the observational satellites was injected using the stolen credential of a NASA employee user [10].
- NASA assigned a team of experts to ensure the security of mission systems to protect their space assets. Traditionally, the security team mainly focused on the protection of servers and data rather than the actual physical space assets.

- Using encryption techniques for space assets and satellites since 2016, China has developed one of the most advanced encrypted communications by utilizing quantum key distribution [11].
- Cyber defence engineering and research (CDER) group raises cybersecurity awareness among its employees to keep their machines secure.
- CDER developed a tool known as Cyber Analysis Visualization Environment (CAVE) to visualize and model possible threats to space assets to ease the vulnerability analysis [12].
- Public and private space organizations such as NASA and SpaceX, are collaborating with the research community where their platforms are used as test bed for increasing their space assets security.

CONSIDERATIONS AND DISCUSSIONS

- One of the challenges to ensure safe, secure and sustainable space, is that it is necessary to improve cooperative governance of space at national and international levels.
    - To promote international cooperative governance, an outer space treaty should be universalized. All active participants in space activities should be implemented and considered through registration and liability convention.
    - All active participants should implement the corresponding guidelines for long-term sustainability of space regarding the post-mission debris. These guidelines should be considered nationally for active sectors as part of licencing and supervision processes.
    - Private and commercial sectors are not always following the guidelines set by United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS) [3]. There should be formal and uniform set of international guidelines, standards and norms for private sectors (i.e., best practices for sustainable space activities).
    - New regulations should be considered regarding the advancement of technology. The advancement of technology reduces the entry barriers into the space industry. However, it also raises serious concerns on security, safety and sustainability of the space.
- Information sharing should be accurate, timely and reliable among spacecraft.
    - Space situational awareness (SSA) system is the main source of obtaining information. The data sharing should be an open-source and available to all active members of the space. There should be more encouragement for nations to develop such sensors.
    - Development of an open-source database which is accessible to all active sectors in space activities is also important. There should be highly cooperative sections with responsibility to assign the best information on an object and share it to the above database.

- Preserving the strategic stability in space is crucial given the
  - High dependency of the national military on space and the existence of ground and space-based weapons for preserving the national security increases the possibility of tension among nations.
  - There should be clear norms and standards developed to identify and specify responsible and irresponsible actions in space. More restricted rules and regulations on development of offensive counterspace systems and weapons should be considered.
  - Furthermore, clear norms and standards should be established to control the growth of space objects and debris.
- Space organizations world wide should focus on the following point to increase and enhance the cybersecurity of their space assets, specifically
  - Utilize the existing cybersecurity and best practices standard in developing the space assets and develop new ones when the current standards are no longer applicable.
  - Similar to NASA, all space organizations should allocate specific budget to hire a team of security experts to protect their mission critical systems.
  - Space organizations should conduct vulnerability analysis and risk assessments to identify their critical assets and take proper actions to mitigate risks based on their priorities.
  - Collaborate with research institutions and relevant security firms in order to conduct up-to-date vulnerability analyses of their critical assets.
- From the policy makers perspectives, there are quite limited number of regulations and policies to enable cybersecurity of space assets world wide.
  - Policies and regulations should be developed and assigned before a disaster occurs due to cyber-attacks on space assets.
  - Responsibility and liability of appropriate stakeholders for space assets should be determined and assigned to space organizations to encourage corresponding parties to take necessary measures to secure the space assets.
  - The governments should make sure that space organizations are following key performance parameters [13] in developing the space assets.
  - The rules of transparency between all government and space organizations are important to be established and applied. In this manner, cybersecurity incidents and any actions taken by space organizations that are crucial and essential to enhance the space security should be shared.

REFERENCES

[1] B. Weeden, V. Samson, Global counterspace capabilities: An open-source assessment, Secure World Foundation (2019) Available at https://swfound.org/counterspace/.
[2] T. Harrison, K. Johnson, T. Roberts, M. Bergethon, A. Coultrup, Space threat assessment,
[3] Center for Strategic and International Studies (2019) Available at https://aerospace.csis.org/report-space-threat-assessment-2019/.
[4] Martinez, Peter. "Challenges for ensuring the security, safety and sustainability of outer space activities." (2019): 65-68.
[5] Falco, Gregory. "Cybersecurity principles for space systems." Journal of Aerospace Information Systems 16.2 (2019): 61-70.
[6] Lewis, H. G., Schwarz, B., George, S., and Stokes, H., "An Assessment of CubeSat Collision Risk," 65th International Astronautical Congress, Sept.–Oct. 2014, https://eprints.soton.ac.uk/369583/1/IAC-1%252CA6%252C4%252C1%252Cx26805.pdf.
[7] Tanase, S., "SatelliteTurla:APTCommand andControl in theSky," KasperskyLab., 2015, https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081.
[8] Peterson, S., "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer," The Christian Science Monitor, Dec. 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.
[9] "2017-005A-GPS Interference-Black Sea," U.S. Dept. of Transportation, Maritime Administration, 2017, https://www.marad.dot.gov/msci/alert/2017/2017-005a-gps-interferenceblack-sea/ .
[10] Lecher, C., "Texas Students Hijack a U.S. Government Drone in Midair [online journal]," Popular Science, June 2012, https://www.popsci.com/technology/article/2012-06/researchers-hack-government-drone-1000-parts .
[11] Martin, P., "NASACybersecurity: An Examination of the Agency's Information Security,"NASA, Testimony Before the Subcommittee on Investigations and Oversight, U.S. House of Representatives House Committee on Science, Space, and Technology, Feb. 2012, https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf .
[12] Liao, S. K., et al., "Satellite-to-Ground Quantum Key Distribution, Nature, Vol. 549, No. 7670, 2017. pp. 43–47.
[13] Pecharich, J. L., Viswanathan, A., Stathatos, S., Wright, B., and Tan, K., "Mission-Centric Cyber Security Assessment of Critical Systems, AIAA SPACE, AIAA Paper 2106-5603, 2016.
[14] Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), U.S. Dept. of Defense, 12 Feb. 2015, p. 250, http://www.acqnotes.com/wp-content/uploads/2014/09/Manual-for-the-Operationsof-the-Joint-Capabilities-Integration-and-Development-System-JCIDS-18-Dec-2015.pdf .