BRIEFING NOTES

BN-57-Space and Cyberspace-May2021

SPACE CYBER-SECURITY VULNERABILITIES AND COUNTER SPACE ACTIVITIES

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

- It is imperative to investigate and study different components and structures of space and their vulnerable elements, the counter space activities in space and the associated challenges, and finally counter adversarial space activities of certain countries in space.
- In August 2020 SpaceX's Crew Dragon spacecraft become the first certified commercial launch vehicle for operational human space transport.
- The transformation of space flight from public/state sector to the commercial domain allows more interactions between space and Earth, which would result in more data transfer from space and more human access to outer space.
- Consequently, the range of vulnerabilities are higher as outer space becomes more reachable by governments, public and private sectors.
- Space, ground, communication links, and users are the four main segments of outer space systems to be protected against cyberattacks. However, currently the primary focus seemed to be on ground-based systems.
- Development and design of resilient intrusion detection and prevention methodologies and technologies that are being developed by using machine learning and AI techniques for detection and mitigation of cyberattack effects on spacecraft represent as one of the most strategic directions of research.

CONTEXT

Vulnerabilities of the Outer Space:

- In August 2020 SpaceX's Crew Dragon spacecraft became the first certified commercial launch vehicle for operational human space transport.
- The transformation of space flight from public sector to the commercial industry, allows more interaction between space and Earth, which results in more data transfer from and more human access to outer space [1].
- The vulnerabilities are more significant as outer space becomes more reachable by larger group of stakeholders from governments, public and individual sectors.
- According to [2], space, ground, link, and users are the four main segments of outer space systems to be protected against cyberattacks. However, the most of the emphasis and focus is on ground-based systems.
- Recent work in the literature has shown that researchers are more concerned with and are focusing on securing spacecraft.

Key Elements to Have Cyber-Resilient Spacecraft:

- Existence of resilient intrusion detection and prevention mechanisms that are developed by using machine learning techniques to detect and mitigate the effects of cyber attacks on spacecraft [3,4].

- A risk management team should continuously check the functionality of different hardware and software vendors to avoid existence of malware [5].
- Logging data and anomaly detection are necessary for both space and ground based facilities for cross validation [6].

CONSIDERATIONS

- In recent years, countries are analyzing vulnerabilities of space-based systems and are attempting to provide offensive counter space capabilities to make more reliable space-based applications. Due to these enhancements, governments are putting more aggressive polices to ensure peaceful activities in space.
- Counter space or space control is applications, developments, techniques and capabilities that support a government or country to achieve superiority in space. If a country has the capability of achieving its own goals and denies adversaries, it would stand as a leader among other countries.
- Counter space capabilities can be offensive or defensive. Offensive capabilities can destroy, disrupt, or degrade either satellites, ground stations, or the communication links. Information collected by using space capabilities has a strategic role in conventional and cold wars. This is the main encouragement for countries to enhance their offensive counter space capabilities in order to improve their military.
- Although such growth in the space environment has great military benefits, it has two main drawbacks. First obvious reason is that it can create conflicts on Earth. Second, is the long-lasting consequences in the global economy and society.
- Secure World Foundation (SWF) is a private foundation that aims to ensure security and sustainability of space for the benefits of Earth and humanity. This foundation which consists of academics, policy makers, scientists, has studied the offensive counter space capabilities. Every year they provide a report in which counter space capabilities are introduced to public. Usually space and military related policies are kept hidden from public which makes it challenging for future researches.
- Enhancement of space situational awareness capabilities and active defence against threats is the main two areas that are focused by France. This country re-assigns the control of military satellites to the military instead of the space agency. India has demonstrated direct ascent ASAT capabilities by destroying one of its own satellites. Iran has been involved in developing and launching small satellites that may lead to development of on-orbit or direct ascent anti-satellite capabilities. It has also shown Electronic Weapons (EW) capabilities that can interfere with commercial satellite signals.
- Multiple countries are showing evidences of cyber capabilities against non-space objects that can be developed and used against space objects. Moreover, the cyber vulnerabilities of space and non-space systems are undergoing research in multiple countries. Cyber capabilities have not reached the scale to be used in actual operations.

- China is committed to using counter space capabilities in peaceful ways, however, some counter arguments exist. Recently, China integrated the offensive and defensive counter space capabilities in its military where they have control over electronic warfare and cyber capabilities. It is not obvious if China would use its offensive counter space capabilities in future.
- Russia is also incorporating EW capabilities in its military in offensive and defensive manners. Both China and Russia are trying to get superiority in space. In addition, a new organization in the Russian military has been created in which space, air defense and missile defense capabilities are combined. Similar to China and Russia, US has also re-organized its military as space is becoming a war fighting domain in the future.
- Since 2014, US has prepared the public for a potential of war in space and its policy makers have been concentrating on security of space more than before. US Space Command and Space Force have been re-established and created to operate, train, and equip space forces. Their mission is similar to the previously existing military space mission, except that the new development of space-to-ground weapons has been included in their mandate.

RECOMMENDATIONS

- The following recommendations are provided for policy makers by considering the existing vulnerabilities that are indicated above.
- Transparency of activities done in the outer space by each sector is a critical element to keeping the outer space safe. Thus, having an international cooperation which follows specific and detailed rules and regulations is very important.
- Increasing the level of space security by using quantum encryption.
- It is very important for national space agencies to make sure that all active sectors in space obey the security guidelines to reduce the risk of cyber attack such as having proper risk management team, and proper intrusion detection systems.
- As private sectors are having crucial role to innovate and support the space industry, they should not be allowed to go beyond the authorities and regulations provided by state and related agencies.
- Up to now, no policy exists regarding the overreliance of infrastructure on the space-based systems. States should think of alternative and more robust systems in case of failures in space-based systems.

REFERENCES

[1] Meg, King & Sophie, Goguichvili “Cybersecurity Threats in Space: A Roadmap for Future Policy” (October 2020) Available Online: https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy.

[2]Speelman, Ryan J, Brandon Bailey, Prashant A. Doshi, Nicholas C. Cohen, Wayne A. Wheeler “Defending Spacecraft in the Cyber Domain”. (November 2020) Available online: https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

[3] Martin, Jon; Satellite Telemetry Indicators for Identifying Potential Cyber Attacks, Aerospace TOR-2019-02178, The Aerospace Corporation, El Segundo, California (August 16, 2019). Approved for Public Release; Distribution Unlimited.

[4] Scarfone, K; Mell, P; Guide to Intrusion Detection and Prevention Systems, February 2007, page 2-4, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistsp ecialpublication800-94.pdf.

[5] Holzmann, G; The Power of Ten – Rules for Developing Safety Critical Code, June 2006, http://spinroot.com/gerard/pdf/P10.pdf.

[6] Lewis, Patricia. "Space, the Final Frontier for Cybersecurity?." (2016).