



## **NOTE FOR NATIONAL DEFENCE:** **Cyber Anti–Satellite Weapons and their Impact on Outer Space**

**Authors:** P. Yazdjerdi<sup>1</sup> and K. Khorasani<sup>2</sup>

<sup>1</sup> Graduate Student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

<sup>2</sup> Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

### **SUMMARY**

- ✚ Three key stabilizing factors of space are described that could result in peace in the outer space.
- ✚ Cyber anti-satellite weapons can be designed in manners that would threaten the stabilizing factors in out space.
- ✚ A simulated Cyber Anti-Satellite (Cyber-ASAT) against space situational awareness (SSA) data has already been tested.
- ✚ It has been shown that the foundation of space peace is threatened through the introduction of Cyber-ASATs.

### **CONTEXT**

- ✚ In the current multipolar world, there exists significant potential among countries to build a similar regime and military power as U.S. in the outer space and perform activities in outer space.
- ✚ The competition between different states to achieve superiority in space activities results in rise in number of Anti-Satellite (ASAT) weapons.
- ✚ Due to increased complexity and higher reliability of states for space systems concerns about cyber-attacks to space systems are of high interest [1].
- ✚ In general, the key factors on stability in space are as follows [2]:
  - ✚ Limited accessibility,
  - ✚ Attributable norms,
  - ✚ Environmental interdependence.

- ✦ However, Cyber-ASATs can be designed in such a way that undermines the above factors.
- ✦ A practical experiment is conducted to simulate a cyber-attack on SSA data to show the feasibility of Cyber-ASATs.
- ✦ According to our understanding, there is no clear and detailed policy on the cyber security of space systems. However, the provided experimental findings in [2] can be a starting and motivating point for policy makers to consider Cyber-ASATs as real and present danger to the foundation of peace and stability in outer orbits.

## CONSIDERATIONS AND DISCUSSIONS

- ✦ Despite the existence and testing of ASAT weapons by different countries such as China, US, and Russia, the outer space has remained peaceful and stable.
- ✦ The main factors contributing to this stability are:
  - ✦ Limited Accessibility: Over 60 years of space activities, it can be said that only US has the capability to fight on space [3,4]. Also, despite the fact that launch technologies become cheaper, the limited access to orbit reduces the possibility of building ASATs weapons [5].
  - ✦ Attributable Norms: According to the existing norms centered on outer space, states recognize that they have to pay huge costs in case of breaking these norms.
  - ✦ Environmental interdependence: States with kinetic ASAT weapons are likely to harm their own satellites as a result of created debris through collision that constrains the long-term activities of attacker in space.
- ✦ Accordingly, ASATs weapons are less likely to be used in outer space as (a) they cause damage to the attacked space systems, (b) it results in significant costs for breaking norms, and (c) the attacker's limited accessibility to the orbit.
- ✦ On the other hand, Cyber-ASATs weapons can be designed regardless of the above factors.
- ✦ There exists easier accessibility and feasibility in launching cyber-attacks rather than launching rockets into orbit. Consequently, the limited accessibility to the orbit is not any more a stability factor in presence of cyber-attacks.
- ✦ Cyber-attacks can be designed in a way to be stealthy so that deterrence is a challenge and deterrence norms are no longer helpful for ensuring the stability of the space.
- ✦ Cyber-ASATs weapons can be designed such that they do not cause major environmental constraints (i.e. by fooling a satellite to take an unnecessary manoeuvre and decrease its lifetime and/or waste its fuel).
- ✦ Therefore, it is very crucial and important for policy makers to consider possible damages that Cyber-ASAT weapons could have on space systems.
- ✦ A case study is provided in [2], in which a cyber-attack is injected to the SSA data that are received by satellites.

- ✚ SSA data are shared freely on Space-track.org platform among satellites and space systems to provide information such as collision avoidance services.
- ✚ A cyber-attack on the SSA data is designed in [2], in which false information are sent to a satellite regarding a non-existing collision that causes the satellite to take an unnecessary long manoeuvre.
- ✚ This case study was just one example of a cyber-attack, while there can be more broader attacks such as injecting a malware to compromise the operation of a satellite.
- ✚ It is important to encourage the community of researchers to study and analyze the effects of such cyber-attacks and to design defence mechanisms for cyber-ASAT weapons to ensure the peace in the outer space.

## REFERENCES

- [1] Chatham House, 'Making the Connection: The future of cyber and space', London, International Security Workshop Seminar, Jan. 2013.
- [2] Pavur, J., & Martinovic, I. (2019, May). The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-18). IEEE.
- [3] N. Tannenwald, 'Law versus Power on the High Frontier: The case for a rule-based regime for outer space', Yale J. Int. Law, vol. 29, pp. 363–422, 2004.
- [4] R. Handberg, 'Is Space War Imminent? Exploring the possibility', Comp. Strategy, vol. 36, no. 5, pp. 413–425, Oct. 2017.
- [5] P. Stares, 'Space and US National Security', J. Strateg. Stud., vol. 6, no. 4, pp. 31–48, Dec. 1983.