ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

CYBER WARFARE IN OUTER SPACE: A CLOUD ON THE HORIZON

By
Aamna Rafiq
Research Associate
Arms Control & Disarmament Centre, ISSI

Edited by
Najam Rafique

April 3, 2020

In March 2020, the US Air Force commissioned a "digital twin" of a satellite to conduct a wide range of simulated penetration tests to detect its cyber vulnerabilities. This testing will also cover hacking of an entire satellite system - an orbiting satellite, on-ground control station and transmission links between them.[1]Taking into account the growing US dependence on space-based assets for the majority of its military operations at strategic, operational and tactical levels, this testing was authorized by the US Congress under "section 1647" of "the National Defence Authorization Act, 2016."[2] Furthermore, the satellite attack scenarios will be the focal point of the second exercise of the US "Advanced Battle Management System (ABMS)," expected to be held in June 2020.[3]Ensuring the security of space-based assets against potential cyber attacks is not only a matter of concern for the US and other 192 states, but also for the global space economy which is expected to reach US$ 1 trillion by the year 2040.[4]

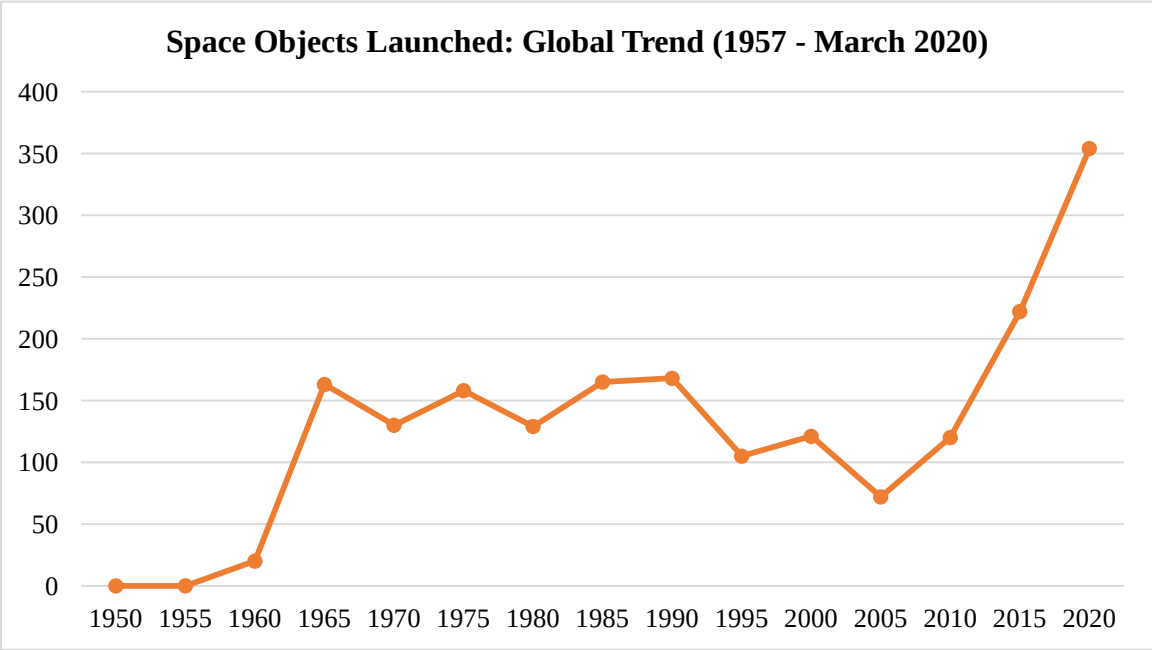
1 Shaun Waterman, "Digital Twins Proliferate as Smart Way to Test Tech," *Air Force Magazine,* last modified March 15, 2020, https://www.airforcemag.com/digital-twins-proliferate-as-smart-way-to-test-tech/

2 US Congress, *National Defense Authorization Act for Fiscal Year 2016,* Public Law 114–92, 114 Cong., November 25, 2015, https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf

3 "April All-Domain Test Postponed; AF Keeps Flying the Globe: Goldfein," *Breaking Defence*, last Modified March 18, 2020, https://breakingdefense.com/2020/03/april-all-domain-test-postponed-af-keeps-flying-the-globe-goldfein/

4 "Understanding the Space Economy," *Harvard Business Review*, last modified May 28, 2019, https://hbr.org/podcast/2019/05/understanding-the-space-economy

More than 9,000 objects[5] have been launched into outerspace from the time when the first satellite was launched in 1957. Currently, 5780 space objects are present in orbit, out of which 1142 are in geo-synchronized orbit (GSO). Since 2011, a gradual surge has been observed in the launching activities, but an alarming increase in the last three years is a matter of great concern. A total of 453 and 581 space objects were launched in 2018 and 2019 respectively. A total of 354 objects were launched in just first quarter of 2020.[6] This number is expected to increase with the expanding industry of cost-effective small satellites which will not only enhance the connectivity to billions of devices, but also offer various new, effortless and extremely interlinked nodes for the hackers. Keeping in view market incentives, manufacturers are paying little attention to incorporating standard security controls, leaving a great number of encryption loopholes.[7]



*Source (s):*The United Nations Office for Outer Space Affairs (UNOOSA)

The integration of emerging technologies like Artificial Intelligence (AI), quantum computing and machine learning with space communications will add fuel to the fire. Researchers are already testing an "intelligent network technology" which will make satellite operations more efficient, fast, adaptive, and above all more autonomous. It will enable the satellites to do a quick assessment of internal and external dynamics for resolving technical issues and emergency situation with minimum

[5] United Nations, United Nations Office for Outer Space Affairs (UNOOSA), *Online Index of Objects Launched into Outer Space*, accessed March 28, 2020, https://www.unoosa.org/oosa/osoindex/index.jspx?lf_id=

[6] Ibid.

[7] David Livingstone and Patricia Lewis, Space, the Final Frontier for Cybersecurity? *Chatham House* (September 2016), accessed March 25, 2020, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

ground assistance.[8] Unlike 20th century satellites, this advance generation of intelligent and digitalized satellites will be safe from inadvertent orbital accidents, but at the same time more vulnerable to cyber attacks, leading to a new kind of survivability paradox in outer space.

New methods of cyber warfare will revolutionize the entire spectrum of counter-space operations. Currently, states rely mainly on kinetic capabilities including an anti-satellite (ASAT) missile for physical destruction of space-based assets. Furthermore, they also bank on the electromagnetic/directed energies (lasers) and electronic warfare (spoofing, orbital jamming and terrestrial jamming) to destroy, disrupt, and control the satellite transmissions. The lack of attribution will make cyber warfare a desired mode of counter-space operations in the future for states as well as non-state actors.[9] However, the speed, cost and technical sophistication of these cyber attacks will depend on the level of damage an attacker want to inflict on an adversary. A cyber attack can cause complete destruction of a satellite through orbital denial and rerouting. Furthermore, a distributed denial of services (DDOS) attack can make satellites dysfunctional by damaging its sensors and electronic systems. Cyber attacks can corrupt communication through deletion and modification of important data stored in a satellite as well as ground control stations. Advancement in cyber technologies will make the interception, alteration and rerouting of satellite transmissions much easier. Cyber attacks that disrupt the crucial satellite operations like Global Positioning System (GPS) will engender far reaching impacts on the military operations at strategic, operational and tactical levels because the majority of weapon systems, maritime operations and aviation depend on it. Cyber warfare in outer space will also damage the credibility and integrity of Intelligence, Surveillance and Reconnaissance (ISR) capabilities.

States are now recognizing the magnitude of the cyber threats in outer space, many great powers like US, China and Russia are incorporating the cyber security of space-based assets in their national security policies and strategies. The recent US Cyberspace Solarium Commission Report 2020 proposed a framework of "Forward Defence" and "Layered Deterrence" in cyber space.[10] Acknowledging the significance of these emerging threats, the North Atlantic Treaty Organization

8 "AIKO: Autonomous Satellite Operations Thanks to Artificial Intelligence", *European Space Agency (ESA)*, last modified January, 2019, https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Technology_Transfer/AIKO_Autonomous_satellite_operations_thanks_to_Artificial_Intelligence

9 Rajeswari Pillai Rajagopalan, *Electronic and Cyber Warfare in Outer Space*, United Nations Institute for Disarmament Research (May, 2019), https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

10 United States of America, Cyberspace Solarium Commission Final Report (March 2020), accessed March 25, 2020, https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf?mod=article_inline

(NATO) has also included the cyber domain in the draft of its first outer space strategy.[11]All these initiatives are positive developments, but they are operating in isolation and lacking an international consensus on an integrated approach to tackle the dark clouds threatening international peace and stability.

The cyber-outer space nexus is in a formative stage today and its future will be determined by the transition of great power competition in geo-economics to astro-politics. The private sector is also a major stakeholder in the securitization of cyber threats in outer space. The existing legal regime is insufficient, even the mandate of the United Nations initiative like "Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security" does not include cyber security in outer space. This new format of threats in new strategic era requires an extensive legal arrangements like treaty, voluntary guidelines and confidence building measures (CBMs) within the broader framework of international arms control and disarmament regime..

[11] Michael Peel, "NATO prepares first outer space strategy to deal with new threats," *Financial Times*, June 21, 2019, https://www.ft.com/content/08bb833c-9439-11e9-aea1-2b1d33ac3271

