Cyber Security History, Trends, and Research Opportunities in Satellite Technologies

Manish Krishna (46698973)
School of Information Technology and
Electrical Engineering
The University of Queensland
Brisbane, Australia
m.krishna@uq.net.au

***Abstract*— This research paper consists of an analysis of the history, trends, and research opportunities of cyber security in satellite technologies. The paper delves into the history of satellite technologies and past events of cyber-attacks that had occurred. Emerging trends such as the evolution of cyber-enabled disruptions, cyber threats on space-link communications, and cyber-attack vectors on unpatched and outdated legacy software's deployed in satellite technologies is also investigated. Lastly, possible research opportunities such as the development of unilateral cyber-security standards, frameworks, and laws that could improve the overall governance of satellite technologies is explored. The research into the modernization of satellite legacy systems, common security architecture and the implementation of quantum communication encryption for satellite communications are investigated in a bid to improve the current cyber security posture in satellite technologies.**

Keywords—Satellite, Cyber Security, Trends, History, Research Opportunities, Aerospace

I. Introduction

As technology evolves, the reliance on satellite technology drastically increases [1]. Instances such as the use of Global Positioning Systems (GPS) satellites for navigation, satellite communications for commercial and military use and lastly space based intelligence surveillance and reconnaissance are some examples of our reliance on satellite technology [2]. However, as the reliance on satellite technology can drive a country's economic and socio-economic growth, it is important to identify the cyber security trends of satellite technologies [3]. Emerging trends such as the evolution of cyber-enabled disruptions to satellites, cyber threats on space-link communications and lastly newer cyber-attack vectors on satellite legacy software's are identified and explored in greater detail. This paper aims to also explore possible research opportunities in a bid to further accrue greater cohesiveness between nation states and a promotion for an improved governance and cyber security posture when dealing with satellite technologies.

II. The History of Satellite technologies

Moving back to the year 1950, the first satellite was launched by Russia, dubbed the Sputnik 1 [4]. The primary function of this satellite was to measure the density of the Earth's upper atmosphere and to then relay this information back to its ground station for a duration of 21 days [5]. Upon this successful launch, the benefits of implementing satellites has had a ripple effect on other countries. Many nations were then beginning to launch their own satellites such as military satellites, weather satellites, telecommunication satellites and land-watching satellites [6].

Although there were significant benefits identified during the genesis of the satellite era, success was called short when cyber threats had compromised the cyber security of satellite technology. In 1998, hackers had taken control of the US-German ROSAT X-Ray Satellite by hacking its ground control station in Maryland, USA [7]. Hackers intentionally destroyed the satellite by configuring it to aim its solar panels at the sun to overheat its batteries which then rendered itself useless [7]. The satellite then crashed back to Earth in 2011 [7].

Lastly, in 1999, hackers have also managed to take a British military's SkyNet satellite hostage and changed the orbiting positions as part of a ransom to the British government [7]. Thus, looking at the brief history of cyber-attacks on satellite technologies, it is evident that as newer trends develop, there is always a greater possibility of them becoming more dire over time.

III. Cyber Security Trends in Satellite Technologies

A. Cyber-Enabled Disruptions

A recent trend that has been on the rise is the evolution of cyber- enabled disruptions to satellite technology. Currently, these hostile disruptions are encompassed under the terminology of anti-satellite capabilities (ASAT) acts [8]. These acts cover three forms of cyber- enabled disruptions such as kinetic, virtual (cyber) and hybrid disruptions to satellites [8].

An example of kinetic disruption include intentional collisions with other satellites which can result in the creation of space debris to damage other satellites [8]. Another example of kinetic disruption includes the launch of ballistic missiles targeting specific satellites [8]. It has been evident that satellites can be easily targeted and destroyed through missile launches. China had successfully destroyed its own upper-ionosphere satellite back in January 2007 using ballistic missiles [8]. Thus, displaying that it is possible that nation states are capable of launching kinetic disruptions against other satellites belonging to other nation states.

Some intentional virtual disruptions on the other hand, comprises of signal jamming, spoofing, disruption and distortion of the satellite's computerised guidance and communications systems [8]. For example, evidence has shown that it is possible to hack satellites through the installation of specialised ground antennas [7]. Through this, malicious commands can be sent to the satellites to spoof, disrupt and distort satellite communications [7].

Lastly, ASAT hybrid attacks comprises of the combination of both virtual and kinetic disruptions. The catalyst of hybrid attacks are initiated by virtual attacks which firstly focuses on the cyber-attacks on ground control stations, cloud infrastructures used by ground stations and the exploitation of the computer network which is the enterprise IT network of the ground station [9]. Upon infiltrating ground stations, bad actors can disrupt other satellites in orbit through the use of kinetic attacks such as steering satellites into other satellites [7], emitting electromagnetic pulses through the detonation of ballistic missiles or by initiating "satellite blinding" tactics by emitting lasers from Earth by gaining current co-ordinates to further inflict physical damage on the in-orbit satellite which has been compromised [8].

Since the year 1950, it is evident that there have become more sophisticated attacks through hybrid disruptions of satellite technologies. While we are living in a highly connected world, these cyber-enabled satellite disruptions can pose as a huge threat to nation states [8].

Satellite technology plays a crucial role in both national and global critical infrastructures which encompasses of military systems, banking systems, air traffic control and electricity grids being some examples [8]. The outer space environment has increased in militarization, hostile interference, congestion, and competition [8]. Thus, it is important to consider further research into outer space cyber-governance in a bid to create international laws to further deter and mitigate various cyber-enabled disruptions of satellite technologies [8].

B. Cyber Threats on Space-Link Communications

Another trend identified is the emerging cyber threats on space-link communications used in satellite technology. Space-link communications is a satellite's language for the uplink and downlink of data from a ground station [2]. This same language uses an open telecommunications protocol called Transaction Language 1 (TL1), and is a commonly used protocol in military satellite communications (SATCOM) [2]. As a result, data transmitted and received by satellites are vulnerable [3]. This protocol can be simply exploited by launching cyber-attacks such as data corruption, denial of service, interception of data, seizure of control, spoofing and software threats [10].

Data interception for example, is a cyber-attack which collates data that is transmitted from a ground station through to a satellite and it includes the monitoring of data transmitted to identify the activity patterns of a satellite [11]. A prime example of data interception was when Iraqi rebels had used commercial software to successfully intercept and decode a video transmission which was relayed over a satellite communication link from a US surveillance aircraft in 2009 [11].

Seizure of control occurs when bad actors gain control over a satellite and execute commands which are unrecoverable and irreversible [11]. A situation similar to this event had occurred in 2008 when NASA's Terra EOS satellite was targeted and controlled by hackers for 2 and 9 minutes respectively [11]. However, it was cited that there were no commands executed [11]. This event could have left targeted satellites disrupted or disabled to deny access to services and possibly even configured to result in hardware and software failures [11].

Lastly, data corruption has a possibility of occurring when bad actors successfully infiltrate a ground system or a satellite. The altering of data to produce false information is a possible event that can occur [11]. In 2012, security researchers found that GPS software used in satellites and ground station receivers could be exploited [2]. The function of this GPS software was to align with ground station receivers to receive the real-time location of a satellite at specific times from the satellite relay [2]. Attackers could exploit a vulnerability of the GPS software's precision timing by corrupting the timing data resulting in the receiver rejecting and jamming the data from the satellite due to the erroneous timings [2]. Thus, upon exploration on the abovementioned cyber threats on space-link communications, it is evident that threats are becoming more sophisticated and dangerous as the reliance on space technology further increases.

C. Cyber-Attack Vectors on Legacy Software

The final emerging trend that is on the rise is cyber-attack vectors on outdated and unpatched legacy software which are used in the expanding small satellites sector [12]. The developmental cost of small satellites has been significantly cheaper due to the reduced cost of Commercial Off The Shelf (COTS) hardware, open sourced software and services such as Ground-stations-as-a-Service [12]. Although the cost of developing satellites has been cost effective, the strategy has not mitigated possible cyber-attack vectors [12].

The first cyber-attack vector which still persists are cyber threats on ground based infrastructures such as ground based stations mentioned earlier [12]. As ground based infrastructures are extremely vulnerable, they can be exploited through connections to the Internet and operations by unaware operators [12], the techniques of social engineering and phishing attacks can be used to easily exploit these vulnerabilities [12].

Secondly, the other cyber-attack vector on small satellites are the use of legacy software's which might be unpatched, outdated or open sourced [13]. The implementation of these software's are known attack surfaces for bad actors [13]. The exploitation strategy to attack these software are derived from a Common Vulnerabilities and Exposures (CVE) list which is an active list that keeps track of publicly disclosed vulnerabilities [13].

As a result, unpatched versions of these deployed software's can cause software applications used in either satellites or ground based stations to be exploited and be used further to disrupt satellites both physically and virtually [13].

IV. Research opportunities into The cyber security of satellite technologies

In a bid to improve the world's current direction of cyber security in satellite technologies, a few research opportunities should be explored. Firstly, as space is a global common [14], possible research into developing unilateral cyber security standards and frameworks for satellites and space assets should be considered for all nation states worldwide [7]. This would be beneficial in cyber-defending both ground-based stations and satellites in orbit.

Secondly, there is a proposal of implementing a security architecture in satellites communication architectures with 2 layers which consist of the first layer blocking illegal communications and the second layer allowing authorised communications between ground stations and surrounding satellites in orbit [15]. Thus, research into developing a common cybersecurity architecture that could be implemented by satellite manufacturers could possibly alleviate the arduous tasks required for adequate cyber defence of satellite technologies and ground based infrastructures [7].

Thirdly, the development of non-segregated unilateral cyber-security space laws should be researched into, in a bid to promote cyber-security satellite governance between nation states [8]. The promotion of satellite governance would allow the development of sanctions for non-compliant nation states. Thus, possibly mitigating hybrid-attacks on satellites conducted by state actors.

Fourthly, research into the development of modernizing legacy software used in satellite technologies should be explored [16]. Issues such as the trouble of patching vulnerabilities, training of staff and complexity of software which results in the difficulty of replacing legacy software have arisen [16]. It would be beneficial for researchers to explore the opportunities of developing cost-effective and reliable legacy systems which have been modernized to suit respective satellite technologies [17]. This includes the research of implementing legacy software in a lesser time consuming manner and reducing production cost of redesigning the software [17]. As a result, this could potentially reduce and deter the potential exploitation of legacy software's deployed in satellite technologies.

Lastly, research into satellite based quantum communication encryption which promotes reliable data encryption techniques and unbreakable encryption keys [18] for the implementation into satellite communications could mitigate risk of potential cyber threats [14]. Investigating these proposed research opportunities could further improve the current state of governance and overall cyber security posture of present and future satellite technology.

V. Conclusion

In conclusion, as our reliance on satellite technology increases as technology evolves, it is imperative that efforts are made to improve the cyber security posture of satellite technologies. Critical infrastructures such as electric grids, transportation systems and water networks that rely on space technology need to be adequately safeguarded for the prevention of a catastrophe [7].

Although future research opportunities which were above-mentioned can improve the overall cyberspace security posture, nation states will still have to play their part in an effort for global co-operation, raising alternatives to reduce the reliance on space technology and to lastly adopt a risk-focused mindset to avoid future potential incidents [14].

References

[1] C. Owen-Jackson. "Securing the final frontier: Why space systems need cybersecurity too." Kaspersky. https://www.kaspersky.com/blog/secure-futures-magazine/cybersecurity-space-exploration/31581/ (accessed 12 October, 2020).

[2] S. F. Bichler, "Mitigating Cyber Security Risk in Satellite Ground Systems," Air Command And Staff College Maxwell Air Force Base United States, DTIC Technical Reports 1 Apr 2015 2015. Accessed: 10 October 2020. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/1012754.pdf

[3] C. House, "Making the Connection: The Future of Cyber and Space," Chatham House in partnership with Finmeccanica UK and Istituto Affari Internazionali, United Kingdom, 24 January 2013 2013. Accessed: 10 October 2020. [Online]. Available: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/240113summary.pdf

[4] B. Wherever. An Early History of Satellites Timeline. (2020). Accessed 13 October 2020. [Image Infographic]. Available: https://www.jpl.nasa.gov/infographics/infographic.view.php?id=11182.

[5] C. S. Centre. "Sputnik Specs." California Science Centre https://californiasciencecenter.org/exhibits/air-space/mission-to-the-planets/sputnik (accessed 13 October, 2020).

[6] E. Howell. "What is a Satellite?" Space.com. https://www.space.com/24839-satellites.html#:~:text=A%20brief%20history%20of%20artificial%20satellites&text=3%2C%201957%20the%20Soviets%20launched,31%2C%201958.&text=(Other%20stations%20followed%2C%20such%20as,and%20the%20Soviet%20Union's%20Mir.) (accessed 13 October 2020).

[7] W. Akoto. "Hackers could shut down satellites – or turn them into weapons." THE CONVERSATION. https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932 (accessed 13 October, 2020).

[8] D. Housen-Couriel, "Cybersecurity threats to satellite communications: Towards a typology of state actor responses," (in English), *Acta astronautica,* vol. 128, pp. 409-415, 8 July 2016 2016, doi: 10.1016/j.actaastro.2016.07.041.

[9] T. Dinerman. "Hybrid wars and satellite vulnerabilities." The Space Review. https://www.thespacereview.com/article/574/1 (accessed 14 October 2020).

[10] B. Unal, "Cybersecurity of NATO's Space-based Strategic Assets," Chatham House, Research Paper July 2019 2019. Accessed: 14 October 2020. [Online]. Available: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

[11] T. Way. "Counterspace Weapons 101." AEROSPACE SECURITY. https://aerospace.csis.org/aerospace101/counterspace-weapons-101/ (accessed October 14, 2020).

[12] "The Growing Risk of a Major Satellite Cyber Attack," (in English), *Satellite Today,* Trade Journals 31 December 1969 1969.

[13] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges," (in English), *International journal of information security,* p. 25, 2020, doi: 10.1007/s10207-020-00503-w.

[14] N. Al-Rodhan. "Cyber security and space security." https://www.thespacereview.com/article/3950/1 (accessed 20 October, 2020).

[15] S. Jingtao, L. Fuhong, and S. Ningning, "Novel security architecture of satellite communication network," ed. Stevenage: The Institution of Engineering & Technology, 2015, p. 4.

[16] C. S. Blogger. "The Importance of Legacy Software Modernization in 2020." Code Authority. https://www.codeauthority.com/Blog/Entry/legacy-software-modernization-2020 (accessed 22 October, 2020).

[17] P. J. Brown. "Legacy Systems: Keeping Older Satellite Systems Operating." Satellite Today. https://www.satellitetoday.com/telecom/2008/01/01/legacy-systems-keeping-older-satellite-systems-operating/ (accessed 22 October, 2020).

[18] C. S. Agency. "Quantum Encryption and Science Satellite (QEYSSat)." https://www.asc-csa.gc.ca/eng/sciences/qeyssat.asp (accessed 21 October, 2020).