When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience

Gregory Falco * † ‡
Stanford University, Stanford, CA, 94305, USA
Harvard University, Cambridge, MA, 02138, USA
Johns Hopkins University, Baltimore, MD, 21218, USA

The United States is increasingly reliant on space systems for civil and military operations. Therefore, it is no surprise that adversaries are interested in compromising these systems via cyber attack. This paper describes a new class of satellite-to-satellite cyber attacks. While such attacks were previously limited to a select group of nation-states, low-cost cubesats and ground station cloud services make these attacks increasingly feasible and accessible to adversaries. There are no publicly documented instances of satellite-to-satellite cyber attacks occurring at the time of publication, but the technical feasibility is described herein along with proposed defense and resilience techniques. Policy recommendations to help manage the risk of satellite-to-satellite attacks are also discussed.

I. Nomenclature

$NASA$	=	National Aeronautics and Space Administration
OT	=	operational technology
$SCADA$	=	supervisory control and data acquisition
RTU	=	remote terminal unit
AWS	=	Amazon Web Services
TCP/IP	=	Transmission Control Protocol and the Internet Protocol
$OBCS$	=	onboard computer system
$ADCS$	=	attitude determination and control system
$C\&DS$	=	command and data-handling
GPS	=	global positioning system
$LiDAR$	=	light detection and ranging
SAR	=	synthetic aperture radar
$TRDSS$	=	tracking and relay data satellite system
SEU	=	single event upset
$DART$	=	demonstration of autonomous rendezvous technology
$MUBLCOM$	=	multiple paths, beyond-line-of-sight communications
EMP	=	electromagnetic pulse
RF	=	radio frequency
AI	=	artificial intelligence
CPU	=	central processing unit
SPD	=	Space Policy Directive
$ISAC$	=	information sharing and analysis center

*Postdoctoral Scholar, Freeman Spogli Institute, Stanford University, Encina Hall, 616 Serra Mall Stanford, CA 94305, AIAA Member.
†Cyber Research Fellow, The Belfer Center, Harvard University, Littauer Center, 79 John F. Kennedy St, Cambridge, MA 02138, AIAA Member.
‡Assistant Research Professor, Civil & Systems Engineering and the Institute for Assured Autonomy, Johns Hopkins University, Latrobe Hall, 3400 N Charles St #205, Baltimore, MD 21218, AIAA Member

II. Introduction

SATELLITES are highly instrumented, finely tuned, complex systems. The adversary to satellite mission success had primarily been physics and the inherent complexities of space launch, propulsion and communication. Today there are new risks to mission success which revolve around cybersecurity. Cyber attacks against space systems have been demonstrated and documented in various forms [1]. Such attacks are generally completed through compromising ground control systems or by intercepting communications from satellites to terrestrial systems and vice versa[2]. Such attacks are increasingly accounted for in risk analysis and scenario planning exercises.

A. Satellite-to-Satellite Attacks

This paper describes a new class of attacks against satellites in orbit that could be launched from other satellites. As opposed to attacks popularized in the media involving physical altercations between satellites, the satellite-to-satellite attacks described herein are cyber attacks. Such attacks target the sensors and actuators that facilitate satellites mission capabilities and can result in cyber-physical consequences. Attacks against these components are complex and may require near-field or line-of-sight proximity to the targeted asset. Further, dynamic satellite manipulation of the offending satellite may be required. Such manipulation calls for robust ground station control with near real-time capabilities for signal delivery and processing. Ground station functionality historically was exclusively afforded by select nation states given the typical barriers of cost and accessibility of these ground station features. However, the relatively recent introduction of cloud-based ground stations for satellite control has provided unprecedented access to these services. Coupled with low-cost cubesats that are rife with cybersecurity issues, it is now feasible for a wide range of nation states, companies or even individuals to cause harm to other satellites in orbit [3].

B. Parallels with Remote SCADA Systems

A parallels can be drawn to attacks launched from remote Operational Technology (OT) such as Supervisory Control and Data Acquisition (SCADA) systems for electric utilities. SCADA systems have sensors and remote terminal units (RTUs) that are housed in remote locations, distant from any command center. These could be located in a field surrounded by thousands of acres of farmland or in a specially housed facility in the polar regions surrounded by glaciers. Originally, SCADA system developers thought that their remote physical location would buffer these components from attack, and equally limit their ability to be used as offensive computing units, therefore no security was built into these systems. As the communication protocols to connect these systems transitioned to variants of TCP/IP so that the assets can be accessed via the internet, remote sensors and RTUs became highly vulnerable to attack and weaponized to launch attacks on other systems. An example of this is when a variant of the infamous Mirai botnet, dubbed Echobot was discovered to overtake RTUs made by Mitsubishi [4]. After taking over these RTUs and other devices, Echobot proceeded to attack other OT devices such as RTUs [5]. This demonstrates an instance of remote systems (RTUs) that are manipulated to attack other remote systems.

Similarly, satellites were considered to be relatively unreachable by their developers, leaving the edge-based systems without security features. If space system developers secured anything, it was the communication link to/from the satellite or the ground station - not the satellite itself. Given advancements in satellite control and the increased accessibility of space systems, satellites are more vulnerable to attack.

C. The Impact of Cubesats and Ground Station Cloud Services on the Threat Landscape

Major cloud service providers such as Amazon Web Services (AWS) and Microsoft's Azure Cloud Services have recently launched their satellite cloud services[6]. Such services enable satellite operators to manage the features and functions of their satellite from the comfort of their home, equally bridging the gap for motivated adversaries to command attacks using the dynamic cloud platform. The cloud-based ground station enables a considerable degree of versatility to the capabilities of a satellite in orbit, in turn, providing the flexibility required to successfully manipulate a satellite's actuators to launch an attack from one satellite to another.

While such cloud satellite platforms enables adversaries to leverage satellites as weapons, they also could be helpful in facilitating local active cyber defense and resilience of the satellite. The ease-of-access and processing capabilities afforded by the cloud increase the opportunities for near real-time monitoring, cyber situational awareness and process execution to defend a satellite from attack.

Importantly, satellite-to-satellite attacks were feasible before cubesats and ground station cloud services. However, they were less likely to occur as the capabilities required to launch such attacks were limited to select nation-states and

military organizations given the traditionally prohibitive associated costs. The satellite-to-satellite attacks described in this paper can originate from a wide variety of satellites ranging from cubesats to sophisticated military satellites - assuming they are appropriately instrumented.

The following sections will: 1) review literature concerning the anatomy of a satellite and previous satellite component failures, 2) describe the necessary instruments required to launch an attack on another satellite and potential defense mechanisms and 3) discuss policy recommendations and future work required in satellite-to-satellite attack research.

III. Background

It is no secret that nation states are actively bolstering cyber attack and defense capabilities for their space assets. This is clear from public comments directly from the U.S. Space Force [7] to extensive studies on China's space capabilities and aspirations [8]. Before attacking a satellite, it is critical to evaluate the components of a satellite to understand its attack surface. As mentioned previously, while there are no previous reports of a satellite-to-satellite attack, instances of satellite failures, which potentially can be induced by a cyber attack.

A. Satellite Anatomy

Each satellite system is unique - especially in terms of its payload, yet there are generally five types of systems that are common for any satellite architecture. These include an onboard computer system (OBCS), actuators, sensors, a power system [9] and a communications system. A simplified description of these components are documented below.

1. Onboard Computer System

The primary responsibility of OBCS is to run the attitude determination and control system (ADCS) and facilitate ground-control or algorithm-based command and data handling (C&DH). The ADCS is responsible for first processing various sensor readings collected and then determining the orientation of the satellite. As a control system, it employs a performance, integral, derivative (PID) control loop in cooperation with actuators onboard to adjust the orientation of the satellite [10]. The orientation is generally critical for the satellite's mission objective, making this among the most important functions of the satellite. Equally important is the execution of C&DH, given the master/agent relationship of ground stations to satellites. OBCS is responsible for processing these commands and engaging the appropriate actuators to fulfill the commands where applicable.

2. Sensors

Generally, there are several standard sensors that enable a satellite to function. These include a: antenna, global positioning system (GPS), magnetometer, sun sensor, horizontal plane sensor, star tracker, angular rate sensor, and temperature sensor [9]. The GPS helps to determine the location of the satellite, which can be shared back to ground control after being passed to the OBSC. The magnetometer, sun sensor, horizontal plane sensor, star tracker and angular rate sensors are all used to generate input to the ADCS. The temperature sensor helps to gauge the health of satellite's operations to make sure it is not overheating.

3. Payload-Specific Sensors

On any given satellite there could be tens of resident sensors particular to the satellite's payload or mission objective that are responsible for collecting data and feeding it back to the ground station. For example, a surveillance or remote sensing satellite may include some of the following sensors: digital cameras, light-detection and ranging (LiDAR) systems, synthetic aperture radar (SAR) systems, and multispectral and hyperspectral scanners [11].

4. Actuators

Naturally, more sophisticated satellites are likely to have a greater capacity for actuation and handle more actuators. It is not a given that a satellite has any actuators, but the most commonly present ones include: inertia reaction or momentum wheels, magnetic torque rods, a propulsion system [9] and a radio transmitter. The inertia reaction or momentum wheels and magnetic torque rods are employed based on commands from the ADCS to remedy their satellite's attitude. A propulsion system is employed in response to data from the GPS, commands from ADCS or

direction from C&DH to correct the satellite's orbit. While not always classified as an actuator, a radio transmitter may also be present to send data to other satellites or back to the ground station.

5. Power System

The power system is responsible for measuring and managing energy generation and storage on the satellite. Most satellites are solar-powered and have a battery for energy storage. The power system must be carefully managed or else the satellite may become useless should power levels drop too low. The power system should coordinate with the sun sensor to evaluate the sun's location and potentially manage the position of the satellite's solar array, should this actuation capability be available. Further, the power system feeds into the OBCS to facilitate steps to conserve power, as necessary.

6. Communications System

It is not a certainty that all satellites have two-way communication mechanisms. For some cubesats, communications are unidirectional from the cubesat to the ground station. Regardless of the type of communication, an antenna would be present. For two-way communication, an omnidirectional antenna would be used to both receive radio signals from the ground station's antenna or other satellite antennas and transmit radio signals to the same. The data received from the antenna would be processed by the C&DH and routed to the actuators or sensors where applicable.

While satellites may have the ability to send and receive communications via an antenna, there are relatively few satellites that are publicly known to communicate directly with other satellites. Some examples include NASA's Tracking and Relay Data Satellite (TRDS) and the Iridium constellation [12, 13]. In fact, on January 15, 2020, the United State's Space Development Agency issued a call for proposals to establish an Optical Intersatellite Link Open Standard to help facilitate satellite communications that could potentially help prevent future collisions in orbit [14]. Because of the general inability for most satellites to communicate with each other, most radio transmission is directed to and from ground stations.

B. Previous Satellite Failures

While cyber attacks specifically against satellite components are generally not discussed beyond instances of orbital satellite jamming, there are several documented cases of natural or human error-caused component failures on satellites. Some of the following examples are rather dated, but given the sparse availability of detail on such failures, they are included to showcase the spectrum of failures across the various satellite components described above.

1. Actuator Failure

Canadian telecommunications satellites Anik E1 and Anik E2 faltered in 1994, where millions of Canadians lost television service as a result of the outage. The issue was caused by an electrostatic discharge in both satellites disrupting the momentum wheel control[15]. This was likely caused by the natural environmental hazards in space - such as a solar flare.

2. OBCS Incident

NASA's Tracking and Relay Data Satellite (TRDS) 1 launched in 1983 from the Challenger spacecraft. While attempting to reach its orbit, "mission-threatening" anomalies were detected with the ADCS, which had the potential to result in the satellite tumbling [16]. This was caused by Single Event Upsets (SEUs) or "bit flipping" that yielded state changes in random access memory on the OBCS. The issue was a result of natural environmental hazards in space - such as a solar flare or other background radiation.

3. Sensor Failure

In 2005, the Demonstration of Autonomous Rendezvous Technology (DART) spacecraft was launched into orbit with the goal of autonomously navigating around the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite. Less than 11 hours into the mission, DART collided with MUBLCOM [17]. The collision was determined to be a result of a GPS sensor error that caused navigation calculations to be consistently off by 0.6 meters per second. This was likely caused by a human-created software error.

4. Communications System Failure

Orbital satellite jamming is a relatively inexpensive and accessible means to cause communication failures for satellite systems. As early as 2003, intentional interference with satellite communication systems has been employed to censor Persian-language television programming. Namely, the Telestar 12 satellite was jammed from Cuba using a rogue uplink station that sent contradictory frequency to the satellite, which overrode the signal - thereby effectively blocking the television programming [18]. This was a human-caused intentional attack.

5. Power System Failure

According to US Air Force Space Command, in 2015, the Defense Meteorological Satellite Program Flight 13 reached end of life [19]. A temperature spike was noticed in the power system, which was followed by an unrecoverable loss of attitude control. Shortly thereafter, the satellite exploded due to the power system failure. The cause of this failure is unknown, but can likely be attributed to natural environmental hazards in space.

IV. Satellite-to-Satellite Attack and Defense

The above incidents aim to illustrate how the failure of a given component of a satellite can lead to the failure of a mission or, in some cases, the destruction of the entire space system. Most of the failures described were conceivably attributed to the natural hazards of space or human error. However, it could be possible to induce these failures through contact-less cyber attacks originating from satellites. For purposes of this paper, the definition of a cyber attack is being used in the broadest possible sense - ranging from encompassing electromagnetic pulse (EMP) attacks [20] to radio frequency interference [21]. The cyber attack mechanisms described below are theoretical and have not been tested with the attacks originating from satellites in orbit; however, their terrestrial functionality has been demonstrated by researchers, hobbyists and government organizations. In conjunction with the attack mechanisms described, defensive techniques are also proposed for each.

A. Attack Mechanisms

To achieve any of these failures by cyber means, an offensive satellite would require special-purpose sensors and actuators that may not be typically resident on satellites. These actuators will need to be controlled via a ground station (potentially hosted in the cloud) or perhaps using decision-system algorithms resident on the satellite's OBCS.

1. Situational Awareness Sensors

While satellites generally have the ability to determine and control their orientation and attitude, these are matters of introspective situational awareness - not necessarily about surrounding objects. To wage a cyber-attack on another satellite, the offending satellite would require knowledge of the whereabouts of its victim. Generally, there are two ways that an attacker can determine the location of its victim: using local proximity sensors or by collecting information from a third-party system.

Local proximity sensors such as a high-resolution optical distance sensor can be employed to determine the distance between itself and another satellite. Challenges with using optical distance sensors is the need for line-of-sight sensing to the victim. Another possibility is to engage radio frequency (RF) proximity sensors that are increasingly being proposed for autonomous vehicle operations [22]. A consideration for either of these approaches is the power requirements of the sensors - which may be prohibitive. However, a benefit of the local proximity sensors is the real-time data collection and processing - without the need for uplink communications to the satellite.

Third-party situational awareness data could prove to be less power-intensive, but also a slower means for collecting proximity data. A variety of third-party organizations, websites and mobile applications exist that track orbital objects, whose data can be collected at the ground station and shared with the satellite [23]. The accuracy of information pertaining to a victim satellites whereabouts may vary, however it would limit the expense of adding an additional component to a satellite.

After ascertaining the location of the victim satellite, the attacker would need to use its ADCS in concert with the appropriate actuators to orient its offensive instruments towards the victim.

2. Electromagnetic Pulse Actuator

Assuming an offensive satellite can maneuver itself to deliver a line-of-sight attack to a victim, EMP actuators could be leveraged to achieve several of the satellite failures described previously. Specifically, the failures induced by natural electrostatic events or radiation as occurred with the momentum wheel control actuator, the OBCS SEU, and the power system failure are examples where an EMP could potentially cause the same failure. Instructions for building handheld EMPs are publicly available on the Internet [24] where it seems that such technology can be modular and potentially fitted to a satellite. Industrial grade EMP technology has equally been developed by university researchers and military organizations [25, 26]. Depending on the specifications of the EMP device, it is likely that there will be considerable control requirements to make sure that the EMP hits the target. To accommodate the EMP device, supplemental power would be required.

3. Radio Frequency Actuator

A potentially more potent actuator to levy damage on a victim would be a RF transmitter, which would not necessarily require line-of-sight communication to the victim system. RF attacks could be used to replicate the human-induced failures described earlier with the GPS sensor or the communications jamming incident. Devices such as HackRF One, which is a software defined radio (SDR) could be used to spoof GPS sensors[27]. A GPS spoofing attack could cause a victim satellite to not reach its desired location by tricking the victim into believing that it has already reached its orbit. Alternatively, an attacker could trick a victim satellite into using its propulsion to deorbit by falsely representing that the victim is in the wrong location. The same SDR could be used to facilitate satellite RF jamming [28]. While not as power-intensive as an EMP device, there would also be supplemental power required for SDRs.

4. Ground Station Control Requirements

While conceivable that the OBCS will one day contain enough processing power to run a variety of decision-making algorithms composed of statistical techniques or artificial intelligence (AI), current processing constraints require decision systems to be resident at the ground station. This is where cloud-based ground stations become an enabler of such attacks. Data will need to be collected from the situational awareness sensor arrays on the satellite and shared back to the ground station for processing. There, AI techniques such as planners could be employed to determine a series of steps and processes required to levy an attack given a series of goals [29]. Commands can then be sent back to the satellite for execution via the CDH and the associated actuators.

B. Defensive Techniques

The attacks proposed could be fairly devastating to a victim satellite, but there are opportunities for the victim to defend itself from such malfeasance. This would be through a combination of leveraging capabilities of a robust ground station and local actuators. Some defenses would be passive, intending to help maintain operations and ensure satellite mission resilience, whereas others will engage active cyber defense techniques.

1. Ground Station Defenses

Generally, satellites are closely monitored for their system health; however, security indicators are not always included in these assessments. Cloud-based ground stations could afford satellite operators the tools, processing capabilities and speed to detect and prevent attacks while they are occurring. For example, ground stations could closely monitor processes on the OBCS. Fluctuations in the central processing unit (CPU) cycles could indicate that a component of a satellite is not working or is working harder than necessary to achieve its mission. For example, should an EMP attack be waged against the momentum wheel control causing electrostatic discharge and the resulting failure of the actuator, this will be noticed in the CPU activity as data will no longer be collected from the momentum wheel control. The ADCS would become more reliant on other attitude actuators. Should this happen, the ground station operator could dictate commands to isolate the failure and ensure that the ADCS no longer engages with or tries to send data to the momentum wheel control system. Such passive maneuvers may help to prolong the life of the satellite despite the failed component and thereby help ensure mission resilience.

2. Satellite Defenses

Should an operator or algorithm aboard the OBCS be able to determine the cause of an attack, it is possible to deploy targeted active defenses to stop the attack, or at the least ignore the attack's effects. In some cases, this capability may require additional sensors to detect a given attack type or actuators to prevent the attack from occurring. An example of a sensor that could be useful in detecting an attack would be a future quantum accelerometer (or present day accelerometer and gyroscope) [30]. Accelerometers are not thought to be as accurate as GPS in determining location, however they could be directionally helpful to validate if the on-board GPS system is being spoofed or serve as a backup to a failed GPS sensor. Accelerometers are useful because they would not be affected by an RF spoof in the same way.

An example of an active defense that could be conducted locally on the satellite should communication system jamming occur, is to employ a series of anti-jamming techniques [21]. These range from changing the communication frequency to launching a separate jamming attack to block the attacker. Other active defenses could be tried as well including trying to spoof the offending satellite. Both of these cases would require the defensive satellite to host an SDR.

V. Discussion

While satellite-to-satellite attacks are not publicly documented today, it is a certainty that they will become more common given the reduced barriers for adversarial conduct in space given improved accessibility of satellite launch and control. Attribution is already challenging for cyber attacks, and cyber attacks launched from space-faring satellites will make attribution even more difficult. Increased policy and governance of space systems is required to help manage the risk of satellite-to-satellite attacks.

A. Policy Recommendations

While space security policy such as Space Policy Directive 5 (SPD-5), which draws from a variety of academic research on space cyber security, is a good start, it must be expanded on to help prevent satellite-to-satellite attacks [31, 32]. Three recommendations that should be added in an addendum to SPD-5 include: 1) cloud service ground station providers should employ similar security requirements, terms of use and abuse monitoring for users of the ground station as are expected of users for general cloud services; 2) satellite operators should analyze satellite component failures, specifically determine if they could have been caused by cyber attack, and report incidents to the Space Information Sharing and Analysis Center (ISAC) accordingly; and 3) satellite developers should expand the functionality of existing system health monitors for satellites to determine potential security issues as well.

B. Future Work

There is considerable further research required to determine how to feasibly launch targeted attacks from a satellite to another satellite and defend a victim satellite accordingly. Future work will include developing attack trees for satellite systems, establishing likely attack patterns for satellite-to-satellite interaction, and ultimately developing a proof-of-concept for an adversarial satellite. Collaborations will be sought with government, military, industry, academic and non-profit organizations to further this new frontier of research including but not limited to the U.S. Space Force, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, Johns Hopkins University's Applied Physics Laboratory, NASA's Jet Propulsion Laboratory, the U.S. Army's Space and Missile Defense Command and the Department of Defense Cyber Crime Center.

VI. Conclusion

The burgeoning space industry fueled by the reduced barriers to entry for launch and control of satellite systems requires a renewed assessment of the future satellite threat landscape. Satellite-to-satellite cyber attacks will become increasingly prevalent in the coming decade given the increased military presence in space and the improved satellite and ground station computing and control capabilities. This paper served to describe the feasibility of satellite-to-satellite attacks and potential satellite defense and resilience mechanisms. Substantial future work is required to fully understand the cyber threats and opportunities to mitigate and manage the associated risks to satellite systems.

Acknowledgments

The author would like to thank the following individuals and institutions: Harrison Caudill of Orbital Security Alliance for brainstorming and discovering opportunities to translate research to practice; Michel Ingham and Arun Viswanathan at NASA's Jet Propulsion Laboratory for their continued feedback, partnership and research guidance; Harvard University's Belfer Center for providing a platform for this important work; and Swiss Re and Stanford University's Cyber Policy Center for financial support of this research.

References

[1] Falco, G., "Job One for Space Force: Space Asset Cybersecurity," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, Vol. 79, 2018.

[2] Falco, G., "The Vacuum of Space Cyber Security," *2018 AIAA SPACE and Astronautics Forum and Exposition*, 2018, p. 5275.

[3] Caudill, H., "Big Risks in Small Satellites - The Need for Secure Infrastructure as a Service," *ASCEND 2020*, 2020.

[4] Nigam, R., "Mirai Variant ECHOBOT Resurfaces with 13 Previously Unexploited Vulnerabilities," *Palo Alto Networks*, 2019.

[5] Kreminchuker, E., and Zavodchik, M., "Echobot Malware Now up to 71 Exploits, Targeting SCADA," *F5 Labs*, 2019.

[6] Sheetz, M., "Microsoft Wants to Take on Amazon in Connecting Satellites to the Cloud," *CNBC News*, 2020.

[7] Hitchens, T., "Cyber Attack Most Likely Space Threat: Maj. Gen. Whiting," *BreakingDefense.com*, 2020.

[8] Pollpeter, K., Ditter, T., Miller, A., and Waidelich, B., *China's Space Narrative*, China Aerospace Studies Institute, Montgomery, AL, 2020.

[9] Kim, Y. V., "Satellite Control System: Part I-Architecture and Main Components," *Satellite Systems-Design, Modeling, Simulation and Analysis*, IntechOpen, 2020.

[10] Li, J., Post, M., Wright, T., and Lee, R., "Design of attitude control systems for CubeSat-class nanosatellite," *Journal of Control Science and Engineering*, Vol. 2013, 2013.

[11] Fu, W., Ma, J., Chen, P., and Chen, F., *Remote Sensing Satellites for Digital Earth*, Springer Singapore, Singapore, 2020, pp. 55–123. https://doi.org/10.1007/978-981-32-9915-3_3, URL https://doi.org/10.1007/978-981-32-9915-3_3.

[12] Teles, J., Samii, M., and Doll, C., "Overview of TDRSS," *Advances in Space Research*, Vol. 16, No. 12, 1995, pp. 67–76.

[13] Garrison, T., Ince, M., Pizzicaroli, J., and Swan, P., "Systems engineering trades for the iridium constellation," *Journal of Spacecraft and Rockets*, Vol. 34, No. 5, 1997, pp. 675–680.

[14] Agency, S. D., "Space Development Agency Optical Intersatellite Link Open Standard RFI," Tech. rep., Department of Defense, 2020.

[15] Galvan, D. A., Hemenway, B., Welser, I., Baiocchi, D., et al., "Satellite anomalies: Benefits of a centralized anomaly database and methods for securely sharing information among satellite operators," Tech. rep., Rand National Defense Research Institute, 2014.

[16] Wilkinson, D. C., Daughtridge, S. C., Stone, J. L., Sauer, H. H., and Darling, P., "TDRS-1 single event upsets and the effect of the space environment," *IEEE Transactions on Nuclear Science*, Vol. 38, No. 6, 1991, pp. 1708–1712.

[17] Croomes, S., "Overview of the DART mishap investigation results," *NASA Report*, 2006, pp. 1–10.

[18] "Satellite Jamming in Iran: A War Over Airwaves," *Small Media*, 2012.

[19] Clark, S., "Power System Failure Likely Cause of Military Satellite Explosion," *SpaceFlightNow.com*, 2015.

[20] Frankel, M., Scouras, J., and De Simone, A., "Assessing the Risk of Catastrophic Cyber Attack: Lessons from the Electromagnetic Pulse Commission," Tech. rep., Johns Hopkins University Applied Physics Lab, 2015.

[21] Grover, K., Lim, A., and Yang, Q., "Jamming and anti–jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 17, No. 4, 2014, pp. 197–215.

[22] Wu, X., Vacanti, D. C., and Van Le, Q., "Radio frequency proximity sensor and sensor system," , Mar. 19 2009. US Patent App. 12/105,980.

[23] Vaughan, C., "The Best Mobile Apps for Spotting and Identifying Orbiting Satellites and Iridium Flares," *Space.com*, 2018.

[24] Nimbalkar, K., "How to Make EMP Gun!" *Instructables.com*, 2016.

[25] Zielinski, A. E., and Werst, M., "Cannon-caliber electromagnetic launcher," *IEEE Transactions on Magnetics*, Vol. 33, No. 1, 1997, pp. 630–635.

[26] Wilson, C., "High altitude electromagnetic pulse (HEMP) and high power microwave (HPM) devices: Threat assessments," Library of Congress Washington DC Congressional Research Service, 2008.

[27] Zeng, K. C., Shu, Y., Liu, S., Dou, Y., and Yang, Y., "A practical GPS location spoofing attack in road navigation scenario," *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, 2017, pp. 85–90.

[28] Hung, P. D., and Vinh, B. T., "Vulnerabilities in IoT devices with software-defined radio," *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, IEEE, 2019, pp. 664–668.

[29] Falco, G., Viswanathan, A., Caldera, C., and Shrobe, H., "A master attack methodology for an AI-based automated attack planner for smart cities," *IEEE Access*, Vol. 6, 2018, pp. 48360–48373.

[30] Cartlidge, E., "Quantum Sensors: A Revolution in the Offing?" *Optics and Photonics News*, Vol. 30, No. 9, 2019, pp. 24–31.

[31] Trump, D., "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems," *Presidential Memoranda*, 2020.

[32] Falco, G., "Cybersecurity principles for space systems," *Journal of Aerospace Information Systems*, Vol. 16, No. 2, 2019, pp. 61–70.