Monge Solano, Luis Diego

Review of Different Geospatial Perspectives for the Identification and Mitigation of Potential Security Threats to Satellite Platforms

Ciencia y Poder Aéreo, vol. 16, no. 2, 2021, July-December, pp. 60-66
Escuela de postgrados de la Fuerza Aérea Colombiana

DOI: https://doi.org/10.18667/cienciaypoderaereo.704

Available in: https://www.redalyc.org/articulo.oa?id=673571919004

AD Astra desarrollo espacial

| Artículo de revision |

# Review of Different Geospatial Perspectives for the Identification and Mitigation of Potential Security Threats to Satellite Platforms

| Fecha de recibido: xx de xxxx del 2021 | Fecha de aprobación: xx de xxxx del 2021 |

**Luis Diego Monge Solano**

Master en Gestión e Innovación Tecnológica

Astra Codex SRL
Costa Rica
Rol del investigador: teórico y escritura
https://orcid.org/0000-0003-3979-981X
✉ Luis.monge@astracodex.com

Escuela de Postgrados **Fuerza Aérea Colombiana**

**Cómo citar este artículo:**

## Revisión de diferentes perspectivas geoespaciales para la identificación y mitigación de potenciales amenazas de seguridad a plataformas satelitales

**Resumen:** La infraestructura satelital juega un papel vital en el mundo moderno. Cada vez más sistemas dependen de esta tecnología, lo que ha generado que se convierta en un blanco de amenazas de seguridad. La existencia de estos riesgos potenciales ha sido reconocida a nivel internacional, por lo cual cada vez se destinan más recursos a estudiar y entender dichas amenazas. Ante este escenario, el estudio de las tecnologías satelitales desde una perspectiva geoespacial provee un entendimiento del tipo conciencia situacional sobre el ecosistema tecnológico y sus fortalezas, limitaciones y vulnerabilidades. Nuevas tecnologías como la inteligencia artificial, el aprendizaje automático y el blockchain deben ser estudiadas a fin de generar contramedidas de seguridad para las tecnologías satelitales.

**Palabras clave:** satélites; ciberseguridad; tecnología geoespacial; aprendizaje automático; observación terrestre.

## Review of Different Geospatial Perspectives for the Identification and Mitigation of Potential Security Threats to Satellite Platforms

**Abstract:** Satellite infrastructure plays a vital role in today's world. As more systems rely on this technology it increasingly becomes a target for security threats. The existence of such risks has been acknowledged internationally as more resources are allocated to their study and understanding. In this context, studying satellite technologies from a geospatial perspective has provided a situational awareness understanding of the technology ecosystem and its strengths, limitations, and vulnerabilities. New technologies such as artificial intelligence, machine learning, and blockchain must be studied to generate security countermeasures for satellite technologies.

**Keywords:** Satellites; cybersecurity; geospatial technology; machine learning; earth observation.

## Revisão de diferentes perspectivas geoespaciais para a identificação e mitigação depotenciais ameaças à segurança para plataformas de satélite

**Resumo:** A infraestrutura de satélite desempenha um papel vital no mundo moderno. Cada vez mais sistemas dependem dessa tecnologia, o que a tornou um alvo para ameaças à segurança. A existência desses riscos potenciais é reconhecida internacionalmente, por isso cada vez mais recursos estão sendo alocados para estudar e compreender essas ameaças. Diante desse cenário, o estudo das tecnologias de satélites de uma perspectiva geoespacial permite compreender a consciência situacional do ecossistema tecnológico e suas potencialidades, limitações e vulnerabilidades. Novas tecnologias como inteligência artificial, aprendizado de máquina e blockchain devem ser estudadas para gerar contramedidas de segurança para tecnologias de satélites.

**Palavras-chave:** satélites; cibersegurança; tecnologia geoespacial; aprendizagem automática; observação terrestre.

## A New Paradigm

EIn today's world, satellite infrastructure is vital for sustaining the global economy and society (Fritz, 2013). From telecommunications to global navigation, data collecting through earth observation, and even time signals needed for banking transactions, countries are now more dependent than ever on space-based technology. This dependence is set to be reinforced in the coming years as satellite platforms become integrated into technological ecosystems such as 5G networks or Industrial IoT (Internet of Things) (Malik, 2019).

As stated in a 2019 study from the United Nations Institute for Disarming Research, denominated "Electronic and Cyber Warfare in Outer Space," the emergence of electronic and cyber counter-space capabilities is enabling a variety of both state and non-state actors to target and disrupt space platforms from both civilian and military owners, using technology that is increasingly available.

## Methodology: A Situational Awareness-like Perspective

An ecosystem of privately owned and operated space assets already exists and is actively used for security and defense purposes all around the globe. Like the situational awareness approach used in aviation sciences, understanding the space "landscape" with its different technologies, limitations, and how they complement each other is vital to navigate this new technological ecosystem and understand its potential vulnerabilities. The proposed analysis methodology uses the classification of the different satellite platforms based on their application from the point of view of geospatial technologies (figure 1).

According to the Global Geospatial Industry Report, satellite technologies can be classified in global navigation satellite positioning system (GNSS), Earth observation, and Earth scanning (Geospatial Media Communications, 2017) (figure 1). By using this classification as a basis for security analysis, a more comprehensive understanding of the threats and vulnerabilities can be achieved.

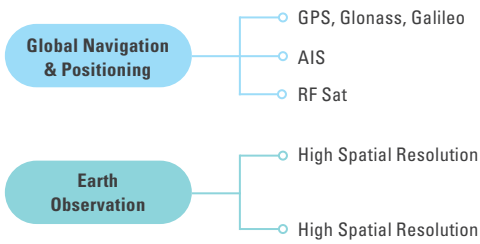


Figure 1. Geospatial technology classification of satellite platforms.
Source: Author.

In the following chapters we conducted a literature review for the different satellite technologies grouped within this category . The analysis of the threats should illustrate the relevance of this perspective.

## Global Navigation and Positioning Systems

Global navigation and positioning systems can be divided into three main levels. The most known technology is GNSS, in which satellites from known orbital positions transmit time signature signals while receivers on the ground estimate a position by triangulating the distance from at least four satellites and comparing the arrival time of each signal. Due to the use of high precision atomic clocks onboard global positioning satellites, many technologies rely on their signals for timekeeping in digital communications protocols such as day-to-day transactions. This technology is susceptible to spoofing, that is, and interference maliciously generated in its operational wavelength. Documented cases of spoofing interfering with commercial aircraft navigation have been reported (Tullis, 2019).

The other two technologies are Automatic Identification System (AIS) and radio frequency (RF) satellites. In the first case, a satellite picks up the AIS,

a TDMA-like signal emitted by ships in high seas in which they transmit their GPS coordinates, speed, and heading to other ships in a few kilometers radius in order to avoid collisions. Since ships undergoing illegal activities can willingly turn off their AIS, this technology can be limited for security application, thus explaining the development of RF satellites, which detect radio frequency signals emitted by ships at the sea and triangulate their position through several receiving satellites. This technology is promising for security applications with constellations delivering commercial data as service products, such as Kleos Space (2021).

The literature review shows that the main threat to global navigation and positioning systems —even at a civilian level— is spoofing or radio frequency interfering, which can be achieved from the ground with relatively accessible technology (Humphreys et al., 2008). The capacity of emitting carrier signals in frequencies that directly interfere with the operation of the satellite platforms is common to both technologies in the GNSS group that encompass two different technologies, such as GPS and AIS.

## Earth Observation

Earth observation technologies have been available for several decades. As the name implies, camera sensors located onboard space platforms provide image data of different parts of the world. Currently, constellations as Copernicus, from the European Space Agency, provide free access to optical data from space for all kind of geospatial analysis and applications (Copernicus, 2021). Commercial earth observation satellites provide improved spatial and temporary resolution, which refers to the amount of terrain covered by a pixel in a satellite image. Currently, submetric resolutions are commercially available with constellations such as Korean Kompsat, offering resolutions in the 70 cm per pixel range (KARI, 2021). On the other hand, constellations with multiple small satellites provide high revisit times improving the temporal resolution. The dove constellation from Planet offers data as service products through hundreds of small-satellites, which sacrifices some of the spatial resolutions but allows daily revisits of the same spot to monitor near to real-time changes in the landscape (Planet, 2021).

Earth observation data is a valuable tool for the assessment of unlawful activities such as illegal forest clearance, and is already used by international certification organizations (RSPO, 2021). Therefore, the generation of counterfeit earth observation information is an issue that must be properly addressed as part of the maturity of the technology (Iacobellis *et a*l., 2020).

Spoofing or interference of earth observation can be almost impossible due to the large number of satellites in each constellation and the large size of the files downloaded at ground stations. In the case of Earth observation, malicious corruption of data between acquisition and end-users is the main cyber threat (Iacobellis *et al*., 2020).

## Earth Scanning

Earth scanning refers to the use of active sensors. Passive sensors as those used in Earth observation detect sunlight reflected from the surface of the Earth and allow modeling the surface through the characterization of the different features of the wavelengths (Chuvieco, 1990). Passive sensors, therefore, are limited by atmospheric conditions. On the other hand, active sensors emit their own radiation, usually in the radio portion of the electromagnetic spectrum, and detect the reflected signals after the radiation has interacted with Earth's surface (Richards, 2009). When a signal interacts with the surface, characteristics such as geometry and moisture content affect the polarization and amplitude of the backscattered signal, this is the principle behind earth observation through radar radio signals and technology such as synthetic aperture radar (SAR) (Chen, 2016). Due to its characteristics, Earth scanning technologies are susceptible to attacks both from RF interference and cyber-attacks down the distribution chain (figure 2).

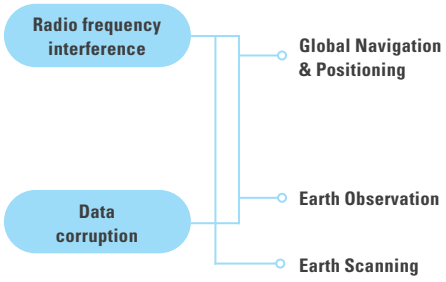


Figure 2. Security threats by geospatial technology classification platforms.
Source: Author.

## Discussion

The classification of a broad range of satellite technologies based on a geospatial application criterion yielded three main groups: GNSS, Earth observation, and Earth scanning. Each group encompasses dissimilar technologies such as GPS and AIS at the GNSS group; or small and high resolution satellites at the Earth observation group.

The literature in security threats has reported commonalities among the different technologies within the same group, with GNSS's main vulnerability being spoofing, Earth observation prone to man-in-the-middle data corruption, and Earth scanning technologies being susceptible to combinations of RF and cyber-interference.

## Conclusion: A Case for the Use of Emerging Technologies as a Countermeasure

For the threat of RF attacks and interference with space platforms, which are common to GNSS and Earth Scanning technologies, the use of artificial intelligence (AI) techniques has been proposed over decades by influential actors such as the European Space Agency (ESA). This organization states the advantages of spacecraft autonomy for space operations, as it is an environment where there is significant —and sometimes unexpected— communications delay between the operator and the spacecraft (Manning *et al*., 2018). This setting poses an opportunity for AI and machine learning technologies to give a head start in the race for space cybersecurity by allowing satellites to autonomously identify malicious signals or commands through the use of embedded software, which enable them to take actions to protect themselves (Kothari *et al*., 2020).

In the case of cyberattacks directed to corrupt data of both earth observation or earth scanning satellites, blockchain technologies such as non-fungible-token (NFT) can be used to generate certificates onboard the satellite that allow traceability of Earth observation data throughout the processing of the data and final use and presentation of the information (Iacobellis *et al*., 2020).

## Next Steps

Two main directions can be explored for further research, and they can even complement each other. The first relates to taking advantage of how easily a bench or laboratory model of a small satellite can be obtained. The CubeSat is a standard for satellite construction developed by California Polytechnic State University to facilitate access to space by university students (CubeSat, 2018). Due to this trend, models for laboratory testing purposes can be currently obtained from either renowned manufacturers (ISIS Space, 2020) or built in-house using readily available electronic components (The CubeSat Simulator Project Page, 2020).

Such a system (figure 3) can be implemented with a computer paired to a radio emitter, while different algorithms could be trained on the computer to try to hack or interfere with satellite-specific functions. Similar to the US Air Force approach, in which hackers were invited to try to hack a satellite to detect previously unidentified vulnerabilities (Hackasat, 2020), a computer could do the same in a university environment while

iterating through thousands of possibilities through algorithm training.

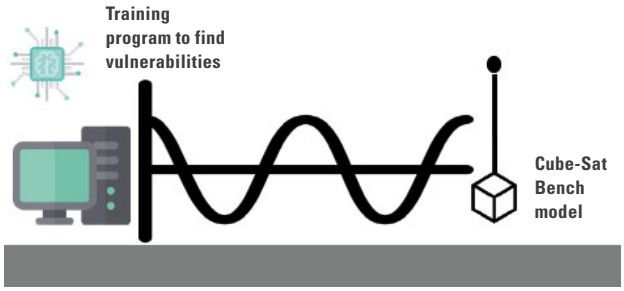


Figure 3. Training program to hack a bench model of a CubeSat in a laboratory environment.

Source: Author.

The second approach seeks to take advantage of amateur-operated ground station data. These stations monitor satellite data and activity and are own and operated by amateur radio enthusiasts and makers from around the world (AMSAT, 2020). The project SatNOGS, by Libre Space Foundation, provides a platform in which hundreds of these stations are crowdsourced for both operation and data access (SatNOGS, 2020). As presented in figure 4, by taking advantage of these unprecedented opportunities, a large data set of telemetry information from different satellites and ground stations can be gathered. Such data sets could be processed using machine learning algorithms to identify parameters previously overlooked and that might play a key role in identifying potential vulnerabilities in space platforms.

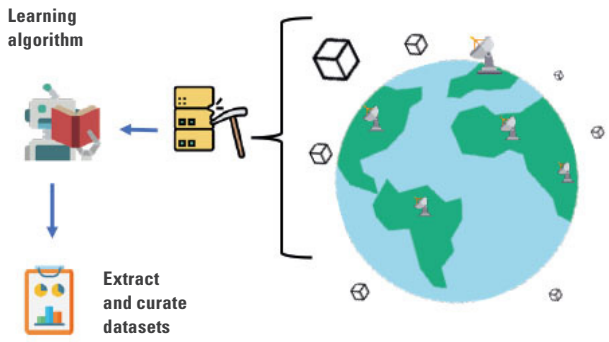


Figure 4. Training program to hack a bench model of a CubeSat in a laboratory environment.

Source: Author.

## References


Chen, K. S. (2016). *Principles of synthetic aperture radar imaging: A system simulation approach*. CRC Press.

Chuvieco, E. (1990). *Fundamentos de teledetección espacial*. Ediciones Rialp.

Copernicus.(2021).*Copernicusservices*.https://www.copernicus.eu/en

CubeSat. (2018, March 20). *CubeSat*. http://www.cubesat.org/

Fritz, J. (2013). Satellite hacking: A guide for the perplexed. *Culture Mandala, 10*(1), 5906.

Geospatial Media Communications. (2017). *Global geospatial industry report*. Geospatial Media Communications.

Hackasat. (2020). *Home*. https://www.hackasat.com

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation. Institute of Navigation*. http://www.ion.org/publications/abstract.cfm?jp=p&articleID=8132

Iacobellis, M., Amodio, A., & Drimaco, D. (2020). Cyber-security threats to space missions and countermeasures to address them. *71st International Astronautical Congress (IAC) – The CyberSpace Edition, IAC-20-E9.2.D5.4.*

ISIS Space. (2020, September 13). ISIS CubeSat development platform. ISIS Space. https://www.isispace.nl/product/isis-cubesat-development-platform/

Kleos Space. (2021). *Delivering RF reconnaissance data-as-a-service*. Kleos Space. https://kleos.space/

Korean Aerospace Research Institute [KARI]. (2021). *Korea Multi-Purpose Satellite (KOMPSAT, Arirang)*. KARI. https://www.kari.re.kr/eng/sub03_02_01.do

Kothari, V., Liberis, E., & Lane, N. D. (2020). The final frontier: Deep learning in space. *ArXiv:2001.10362*. http://arxiv.org/abs/2001.10362

Malik, W. J. (2019, July 26). *Attack vectors in orbit the need for IoT and satellite security* [Conference session]. RSA Conference 2019, San Francisco, CA, USA. http://www.rsaconference.com/industry-topics/presentation/attack-vectors-in-orbit-the-need-for-iot-and-satellite-security

Manning, J., Langerman, D., Ramesh, B., Gretok, E., Wilson, C., George, A., MacKinnon, J., & Crum, G. (2018). Machine-learning space applications on smallsat platforms

with TensorFlow. 32nd Annual AIAA/USU Conference on Small Satellites. https://digitalcommons.usu.edu/smallsat/2018/all2018/458

Planet. (2021). *Homepage*. https://www.planet.com/

Radio Amateur Satellite Corporation [AMSAT]. *Home*. (2020). AMSAT. https://www.amsat.org/

Richards, J. A. (2009). The imaging radar system. In J. A. Richards (Ed.), *Remote Sensing with Imaging Radar* (pp. 1-10). Springer. https://doi.org/10.1007/978-3-642-02020-9_1

Roundtable on Sustainable Palm Oil [RSPO]. (2021). *Home*. https://rspo.org/

SatNOGS. (2020, September). *SatNOGS*. https://satnogs.org/

The CubeSat Simulator Project Page. (2020). *Home*. http://www.cubesatsim.org/

Tullis, P. (2019, December 1). GPS is easy to hack, and the U.S. has no backup. *Scientific American*. https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/