UNAUTHORIZED USE OF MILITARY SATELLITES: THREATS TO MISSION SECURITY AND INTEGRITY

KITAGAWA, Alexandre Takio (PU5KTA)[1, 2], DE ALMEIDA, Pedro Henrique[2]

[1]Departament of Education of Indaial, [2]Professor Giovani Trentini Elementary and Secondary School

Abstract

The clandestine and unauthorized use of military communication satellites, colloquially known as “Bolinha” (portuguese for “Little Ball”) in certain regions, constitutes a significant and escalating threat to mission security and operational integrity within the space domain. These geostationary satellites, such as the U.S. Fleet Satellite Communications System (FLTSATCOM) and UHF Follow-On (UFO) systems, were originally designed exclusively for military communications. However, their reliance on simple, non-regenerative “bent-pipe” transponders, operating within the UHF band (approximately 260 MHz), has rendered them vulnerable to misuse and unauthorized appropriation by civilian users. This misuse has been particularly well-documented in remote areas of South America since the 1990s. This research aims to verify the current prevalence of unauthorized civilian use of these satellites and to raise an alert regarding this ongoing situation. The methodology employed involved a receiver (UV-32) paired with an antenna of ⅝ λ to capture the specific frequencies utilized by the satellites. Reception tests were conducted at random times, without a predefined pattern. A total of eleven different frequencies were analyzed between 244.125 and 258.545 MHz, which were identified from video streaming websites. The findings indicate that reception was achieved on all listed frequencies. The audio content, delivered in Portuguese, clearly contained dialogues that were outside the context of the satellite’s intended military application. Analysis confirms that these illegal transmissions, which are frequently associated with illicit operations, generate detrimental interference. This parasitic load degrades legitimate military signals, saturates transponder capacity, and, critically, accelerates the drainage of the satellites limited onboard battery resources, resulting in numerous operational disadvantages. While operational countermeasures, such as the targeted “jamming” of pirated channels, are utilized, the definitive solution lies in technological migration. Modern systems, such as the Mobile User Objective System (MUOS), which feature robust encryption, regenerative processing, and spread-spectrum techniques, are inherently more resistant to unauthorized use. In conclusion, containing this illicit practice is not merely a matter of public safety, but a critical necessity for the responsible stewardship of the space environment, the protection of national security infrastructure, and the preservation of public investment in space-based capabilities.

Introduction

Unauthorized Use of Military Communication Satellites called in Brazil “bolinha” (portuguese for “Little Ball”) as a Growing Security Threat;

Vulnerability of UHF Military “Bent-Pipe” Satellites to Civilian Misuse;

This misuse has been particularly well-documented in remote areas of South America since the 1990s;

This research aims to verify the current prevalence of unauthorized civilian use of these satellites and to raise an alert regarding this ongoing situation.

Method/Experiment

- A UV-32 receiver with a ⅝ λ antenna was used to capture satellite frequencies, ensuring adequate sensitivity within the target band;
- Procedure Tests were conducted at random times to evaluate signal availability under varying conditions;
- Eleven frequencies between 244.125 MHz and 258.545 MHz were analyzed, identified through satellite monitoring video streaming websites.

Figure 01: Moment of reception of pirate transmissions with UV-32.

Figure 02: Figure 2: Illustration depicting the possible clandestine use of the "little ball" satellite by truck drivers (Produced by Artificial Intelligence - Gemini).

FREQUENCY (MHz)
253.750
244.125
249.910
253.900
254.840
255.440
255.550
257.040
257.500
258.540
258.545

Figure 03: Table presenting the frequencies monitored during the study.

Data and Analysis

- Reception occurred on all frequencies, revealing Portuguese audio unrelated to military use and confirming illegal transmissions.
- Unauthorized transmissions cause harmful interference to legitimate signals, saturate transponder capacity, accelerate onboard battery depletion, and generate significant operational disadvantages.
- Currently, targeted jamming of pirated channels mitigates the problem, but a lasting solution relies on migrating to modern systems like MUOS, which use encryption, regenerative processing, and spread-spectrum techniques to better resist unauthorized use.

Conclusion

Clandestine use of military UHF satellites compromises national security due to their vulnerable analog architecture. This unauthorized access causes channel saturation and degrades legitimate signals, requiring a technological transition to modern systems with digital processing and robust encryption to ensure operational integrity.

SCAN ME

Figure 04: QR code for the presentation of this study.

References

Brochi, A. (2011). *Satélite Bolinha* 7. Scribd. https://pt.scribd.com/document/62641953/Satelite-Bolinha7

Duncan, C., Joyce, R., Bugg, S., Marquardt, J., & Combs, M. (2024, February). Creating a Practical Education in Space Cybersecurity Through Antenna Design and Implementation. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 11, No. 1, pp. 5-5).

Lawson, H. (1990). *Operational procedures for powering up, powering down, and configuring the qualification model of the FLTSATCOM satellite* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Haverkamp, K. (2018). An analysis of the new threat environment for satellites (Master's thesis, Luleå University of Technology / Cranfield University).

Hermenau, M. (2021). *Satélites militares UHF em GEO, HEO e LEO* [Document]. Scribd. https://pt.scribd.com/document/531261396/Mundo-satelite-satelites-militares-UHF-em-GEO-HEO-e-LEO

Perkins, C. E. (1991). *A comparison of the UHF Follow-on and MILSTAR satellite communication systems* (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

Rao, G. K., & Rao, J. S. (2016, February 22–25). *New technologies to improve antijam performance of commersatcoms to bring them on par with milsatcoms* [Paper presentation]. Fourth International Conference on Electronic Warfare (EWCI 2016), Bangalore, India.

Rohret, D., & Holston, J. (2010, April). Exploitation of Blue Team SATCOM and MILSAT Assets for red Team Covert Exploitation and Back-Channel Communications. In *International Conference on Cyber Warfare and Security* (p. 288). Academic Conferences International Limited.

Acknowledgements

We are immensely grateful to the HamSCI organization for the opportunity, to the Department of Education of Indaial and to the Professor Giovani Trentini Elementary and Secondary School.

alexandrekitagawa@gmail.com

THE INFLUENCE OF SOLAR ACTIVITY ON HIGH-FREQUENCY COMMUNICATIONS: A SYSTEMIC RISK TO GLOBAL COMMUNICATION

KITAGAWA, Alexandre Takio (PU5KTA)[1, 2]; GEISLER, Rebeca Wegner[2] ; NOGUEIRA, Kathellen Thayenne Pereira[2]; ROCHA, Emillin[2]

[1]Departament of Education of Indaial, [2]Professor Úrsula Kroeger Elementary and Middle School

Abstract

Radio blackouts, phenomena resulting from the interaction between solar activity and the Earth's ionosphere, constitute an invisible and underestimated societal risk with significant potential to impact High-Frequency (HF) communications. Such communications are vital for the safety and operation of aircraft, maritime vessels, broadcasting systems, emergency services, and amateur radio networks. This study was conducted by seventh-grade elementary school students from a public school in Santa Catarina, Brazil, as a research project within the Civil Defense in Schools Program. Its objective was to record the frequency and intensity of radio blackouts, aiming to assess the viability of a low-cost approach for Disaster Risk Reduction (DRR) education by integrating space weather risks into the educational environment. The methodology employed consisted of data collection from May to December 2025 using the Space Weather application. Data were recorded whenever the application issued a notification regarding an event occurrence. These events were classified according to the official nomenclature of the National Oceanic and Atmospheric Administration's (NOAA) Space Weather Prediction Center (SWPC), which categorizes solar flares into three classes (C, M, and X) and radio blackouts on an intensity scale from R1 to R5. An average of 12 monthly occurrences were recorded, including a high-intensity X2.62-class blackout in May, which was registered and reported by various news outlets. The results confirmed the fluctuating nature of solar activity during the analyzed period. While it was not possible to directly correlate the recorded events with specific communication failures documented in amateur radio logs, NOTAMs, or NAVAREA Warnings, the study underscores the relevance of promoting research and employing low-cost tools for the educational monitoring of space weather phenomena. This approach effectively illustrates the connection between solar activity and the vulnerabilities of modern technological infrastructure. By overlaying blackout-affected areas with major air and maritime routes, the systemic nature of this risk is reinforced. For future work, it is recommended to correlate these observational records with communication failures effectively reported by critical sectors, aiming to deepen the understanding of operational impacts.

Introduction

- Radio blackouts are caused by interactions between solar activity and the Earth's ionosphere and represent an invisible, underestimated risk to society;
- They can significantly disrupt High-Frequency (HF) communications, which are essential for aviation, maritime operations, broadcasting, emergency services, and amateur radio networks;
- Conducted by 7th-grade students in Santa Catarina, Brazil, the study recorded radio blackout frequency and intensity to evaluate a low-cost approach to Disaster Risk Reduction education through space weather awareness.
- This research aims to verify the current prevalence of unauthorized civilian use of these satellites and to raise an alert regarding this ongoing situation.

Method/Experiment

Data was collected from May to December 2025 via the Space Weather Mobile App, recording events upon notification. Occurrences were classified using NOAA/SWPC nomenclature, categorizing solar flares (Classes C, M, X) and radio blackouts (Scales R1–R5).

Data and Analysis

- The results confirmed the fluctuating nature of solar activity during the analyzed period.
- It was not possible to directly correlate the recorded events with specific communication failures documented.
- The study highlights the importance of:
  - Promoting further research on the topic;
  - Employing low-cost tools for the educational monitoring of space weather phenomena.
- This approach effectively illustrates the connection between solar activity and the vulnerabilities of modern technological infrastructure.
- Overlaying blackout-affected areas with major air and maritime routes reinforces the systemic nature of this risk.

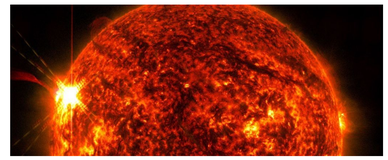

Figure 01: Image of the X2.7 solar flare of 14 May 2025, captured by the Solar Dynamics Observatory. (NASA/SDO)

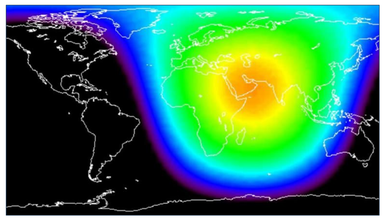

Figure 02: High-intensity X2.62-class blackout in May of 2025 (Space Weather Mobile App).

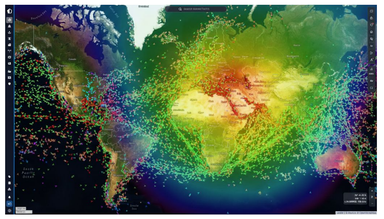

Figure 03: Simulation of a radio blackout in maritime traffic (Edited with ChatGPT).

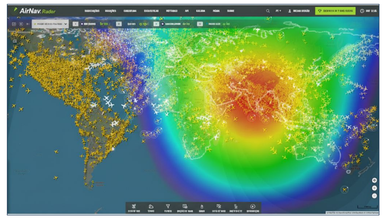

Figure 04: Simulation of a radio blackout in air traffic (Edited with ChatGPT).

Conclusion

Clandestine use of military UHF satellites compromises national security due to their vulnerable analog architecture. This unauthorized access causes channel saturation and degrades legitimate signals, requiring a technological transition to modern systems with digital processing and robust encryption to ensure operational integrity.

SCAN ME

Figure 05: QR code for the presentation of this study.

References

Brochi, A. (2011). *Satélite Bolinha* 7. Scribd. https://pt.scribd.com/document/62641953/Satelite-Bolinha7

Duncan, C., Joyce, R., Bugg, S., Marquardt, J., & Combs, M. (2024, February). Creating a Practical Education in Space Cybersecurity Through Antenna Design and Implementation. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 11, No. 1, pp. 5-5).

Lawson, H. (1990). *Operational procedures for powering up, powering down, and configuring the qualification model of the FLTSATCOM satellite* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Haverkamp, K. (2018). An analysis of the new threat environment for satellites (Master's thesis, Luleå University of Technology / Cranfield University).

Hermenau, M. (2021). *Satélites militares UHF em GEO, HEO e LEO* [Document]. Scribd. https://pt.scribd.com/document/531261396/Mundo-satelite-satelites-militares-UHF-em-GEO-HEO-e-LEO

Perkins, C. E. (1991). *A comparison of the UHF Follow-on and MILSTAR satellite communication systems* (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

Rao, G. K., & Rao, J. S. (2016, February 22–25). *New technologies to improve antijam performance of commersatcoms to bring them on par with milsatcoms* [Paper presentation]. Fourth International Conference on Electronic Warfare (EWCI 2016), Bangalore, India.

Rohret, D., & Holston, J. (2010, April). Exploitation of Blue Team SATCOM and MILSAT Assets for red Team Covert Exploitation and Back-Channel Communications. In *International Conference on Cyber Warfare and Security* (p. 288). Academic Conferences International Limited.

Acknowledgements

We are immensely grateful to the HamSCI organization for the opportunity, to the Department of Education of Indaial and to the Professor Úrsula Kroeger Elementary and Middle School.

alexandrekitagawa@gmail.com