INL/RPT-23-73517-Revision-0

Vulnerabilities in Satellite Communications Underscore Threat to Critical Infrastructure

July 2023

Anna Christine Skelton

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/RPT-23-73517-Revision-0

Vulnerabilities in Satellite Communications Underscore Threat to Critical Infrastructure

Anna Christine Skelton

July 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Vulnerabilities in Satellite Communications Underscore Threat to Critical Infrastructure

Analytic Summary

INL analysts assess critical infrastructure sectors leveraging satellite communications (SATCOM) are likely inadvertently increasing the attack surface caused by inherent vulnerabilities in equipment and communications pathways. A lack of ownership regarding security in SATCOM ecosystems creates pervasive information security risk, and the obfuscation of patching responsibility means the mitigation of publicly and privately disclosed vulnerabilities is difficult to track. With these factors in consideration, INL analysts assess the number of attacks against SATCOM is likely to increase in the next decade as threat actors exploit these vulnerabilities.

Critical Infrastructure Increasing Dependency on SATCOM Despite Obfuscated Environment

Remote assets including offshore wind farms and pipeline monitoring systems use SATCOM to manage and monitor resources.

- SATCOM facilitates troubleshooting and distributing updates to assets that might otherwise be cost-prohibitive to maintain, according to INL subject matter experts.[1] However, the complex ecosystem of communications and equipment providers, including the addition of third parties with unknown risk and security postures, introduces risk to critical infrastructure control system environments.
- Research from Oxford University demonstrates although owners and operators may own the remote terminal unit leveraged to locally transmit and receive SATCOM, the rest of the system is unlikely to be within the asset owner's scope of control, including the communication uplink and downlink, the satellite hardware, any related software leveraged to facilitate the communication, and the receiver.[2]
- According to research presented by Cybersecurity and Infrastructure Security (CISA) analysts, decades of innovation, mergers and divestments, and consolidation within the SATCOM industry have created a persistent lack of control for asset owners and operators seeking to protect SATCOM infrastructure.[3]

Many satellite terminals are developed with multiple applications in mind; for example, in promotional material, the Wideye SABRE Ranger 5000 lists the following applications, indicating the widespread application of SATCOM in critical infrastructure:[4]

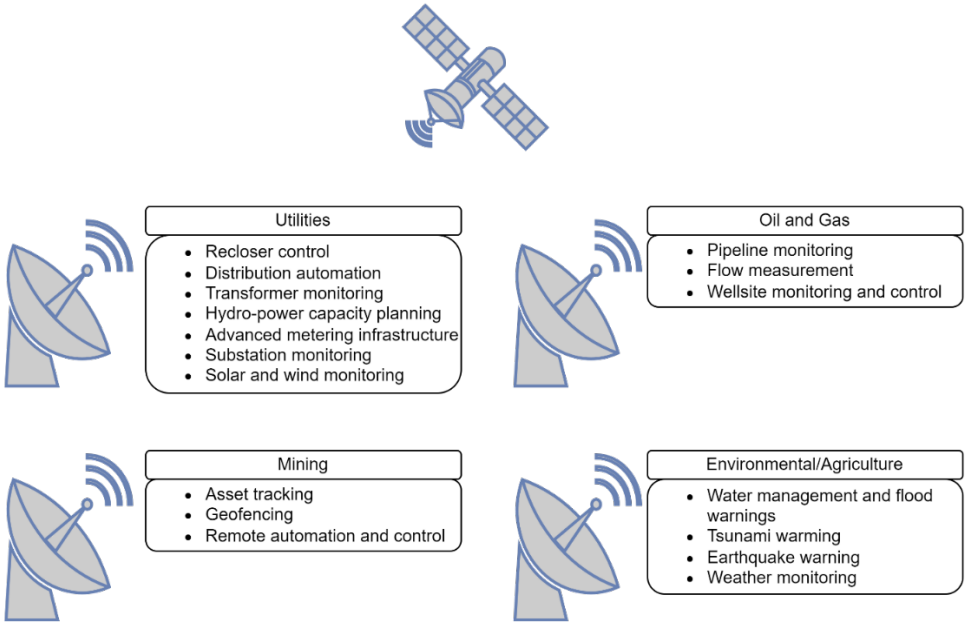

Figure 1: Uses of SATCOM in Critical Infrastructure Sectors for Wideye SABRE Ranger 5000.

Publicly Disclosed Vulnerabilities Continue to Pose Threat to SATCOM

Known and unpatched security issues render SATCOM and associated technology vulnerable to exploitation by malicious actors.

- Research published by Oxford University catalogues 112 significant satellite hacking incidents, demonstrating the historic and ongoing Hmthreat to SATCOM.[5]
- The same body of research conducted ethically responsible long-range eavesdropping against SATCOM using widely available home television equipment. [6] Captured information included data flows from wind and solar electrical power generation facilities, as well as facilities associated with oil and gas pipelines. According to the study, "In the case of one specific software platform commonly used in the wind-power generation industry, over 5,000 plaintext requests were observed to various facilities and administration pages." [7] Observed data included login credentials.
- A report published in 2013 by Ruben Santamarta, at the time a Principle Security Consultant at cybersecurity company IOActive, analyzed SATCOM equipment deployed in critical infrastructure environments. The report notes, "classes of vulnerabilities uncovered by IOActive researchers included hardcoded credentials, undocumented protocols, insecure protocols, and backdoors" discovered by "reverse engineering the freely and publicly available firmware updates for popular SATCOM technologies

manufactured and marketed by Harris, Hughes, Cobham, Thuraya, JRC, and Iridium." [8] Subsequent IOActive reporting has reiterated the threat to SATCOM infrastructure.[9]

Analytic Tradecraft Summary

Confidence Statement

We have moderate confidence in our assessment that SATCOM leveraged in critical infrastructure are inherently vulnerable. Our confidence level is based on multiple corroborating and vetted open-source papers and the expertise of Idaho National Laboratory researchers. This assessment relies on the assumption threat actors are interested in causing damage to U.S. energy resources and therefore may target SATCOM as a means to achieve effects. If this assumption is proven false, it is unlikely malicious cyber adversaries would have an interest in threatening critical infrastructure SATCOM.

Source Summary

Our assessment is based on multiple corroborating open-source reports, detailed conversations with multiple Idaho National Laboratory subject matter experts, and consultation with leading SATCOM researchers. We deemed open-source reporting to be reliable due to, in many cases, extensive peer review from the academic and cybersecurity researcher community. We consider conversations with subject matter experts highly credible due to their extensive experience working directly with related systems. The convoluted nature of the SATCOM industry, as noted in this paper, makes defining the exact nature of the threat to SATCOM, as well as associated vulnerabilities, difficult. Partnership with an entity actively leveraging SATCOM in operations could dispel some of these gaps. Additionally, vetted open-source research on cyber vulnerabilities to SATCOM in critical infrastructure is limited.

Appendix A: Threat Actors Interested in SATCOM

A compilation of research correlated by Oxford researchers identified nine distinct threat actors with capabilities and resources ranging from high to low who may have an interest in compromising satellite assets. [10] The nine threat actor groups include military, intelligence, industry insider, part supplier, organized crime, terrorist/military organization, commercial competitor, individual hacker, and political activist.

[1] Interview | Bryan Hatton | Computer Security Researcher, Idaho National Laboratory | January 26, 2023
[2] Doctoral Thesis | James Pavur | University of Oxford | *Securing New Space: on Satellite Cyber-Security* |2021 | page 66| Accessed March 23, 2023
[3] Presentation | MJ Emanuel | "Demystifying Threats to Satellite Communications in Critical Infrastructure" | publicly shared November 17, 2022 | Presented at LABSCon | September 21-24, 2022 | Phoenix, USA
[4] Product Information Sheet | Inmarsat | *SABRE Ranger 5000* | https://static.mackaycomm.com/wp-content/uploads/2021/08/wideye-SABRE-Ranger5000_en-v01-2016-Mackay-241116-2.pdf |Accessed January 25, 2023
[5] Doctoral Thesis | James Pavur | University of Oxford | *Securing New Space: on Satellite Cyber-Security* |2021| page 271 | Accessed March 23, 2023
[6] Doctoral Thesis | James Pavur | University of Oxford | *Securing New Space: on Satellite Cyber-Security* |2021| page 10 | Accessed March 23, 2023
[7] Doctoral Thesis | James Pavur | University of Oxford | *Securing New Space: on Satellite Cyber-Security* |2021| page 73| Accessed March 23, 2023
[8] Paper| Ruben Santamarta| IOActive| *A Wake-Up Call for SATCOM Security*| https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf | 2014| page 3 |Accessed January 25, 2023
[9] Paper |Ruben Santamarta| IOActive| *Last Call for SATCOM Security*| https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf |August 2018||page 1| Accessed May 16, 2023
[10] Doctoral Thesis | James Pavur | University of Oxford | *Securing New Space: on Satellite Cyber-Security* |2021| page 21 | Accessed March 23, 2023