SPACE CYBER IMMUNITY

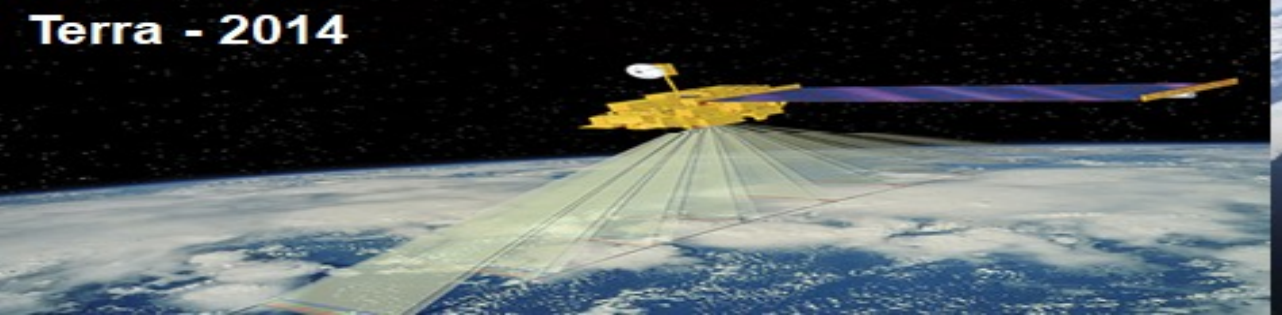
DeepSec

2024

Paul Coggin

nou Systems, Inc

Historical Satellite Attacks



Russian hacker known as Samurai (from the Russian group SecDet) claims he broke into National Institute for Space Research cybernetic systems in Brazil.

The attacker provided data and details for how the break occurred step-by-step.

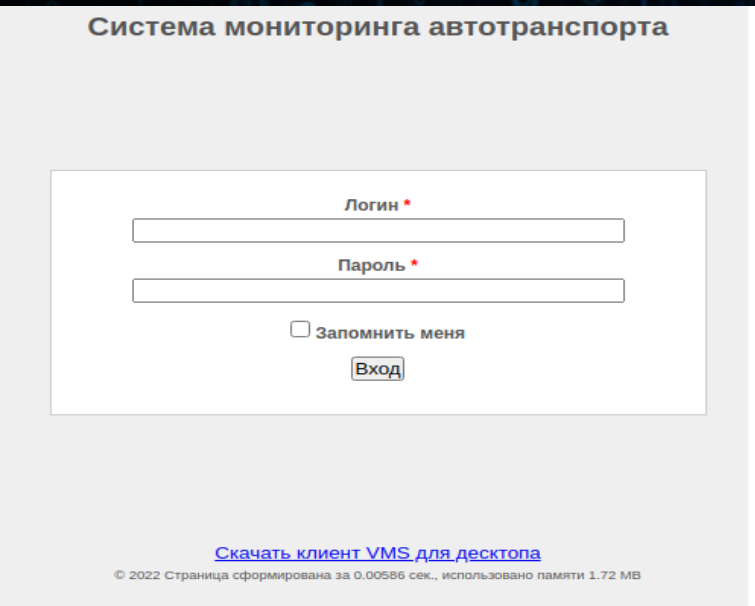
- Hack was via SQL injection (Structured Query Language), exploitation of LFI (Local File Inclusion) and reflected XSS (cross-site scripting) vulnerabilities, in addition to obtaining a reverse Shell.
- The CBERS-2/B, GLS-LANDSAT and LANDSAT-1/7 satellites were accessed.
- The following satellites are listed in the access list CBERS-2, CBERS-2B, GLS-LANDSAT, LANDSAT-1, LANDSAT-2, LANDSAT-3, LANDSAT-5, LANDSAT-7.

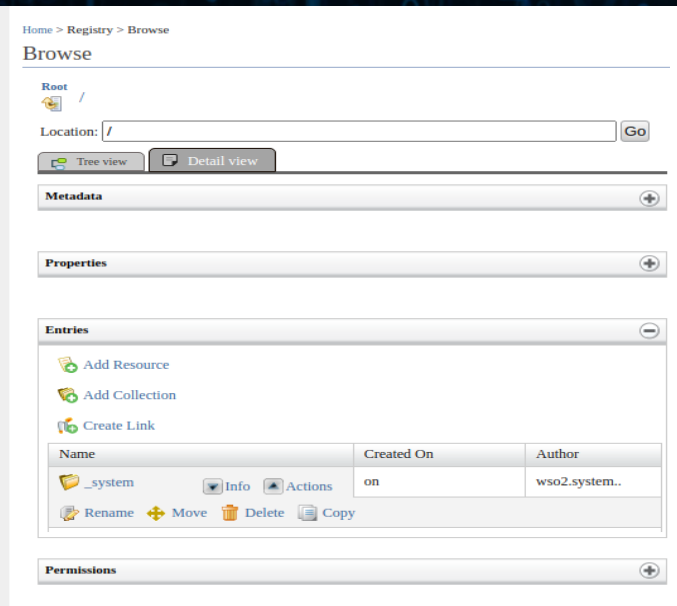
No Airgap between the Internet and Satellite Operations Networks

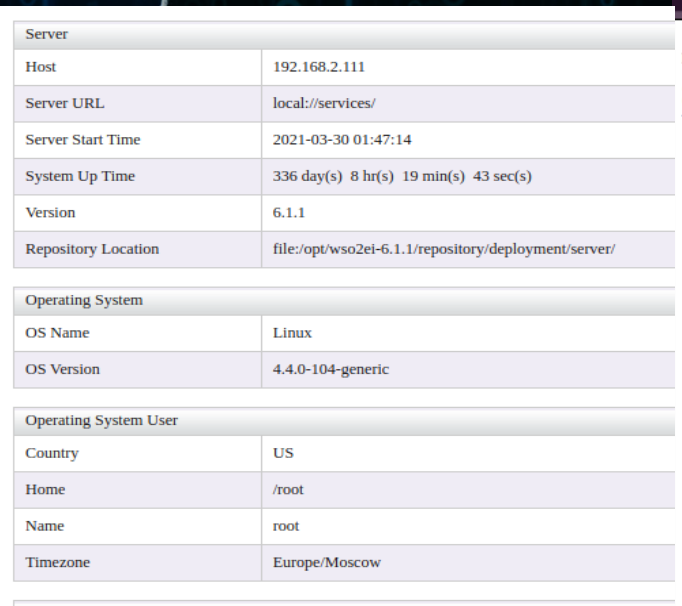
Source: (Payao, 2023)

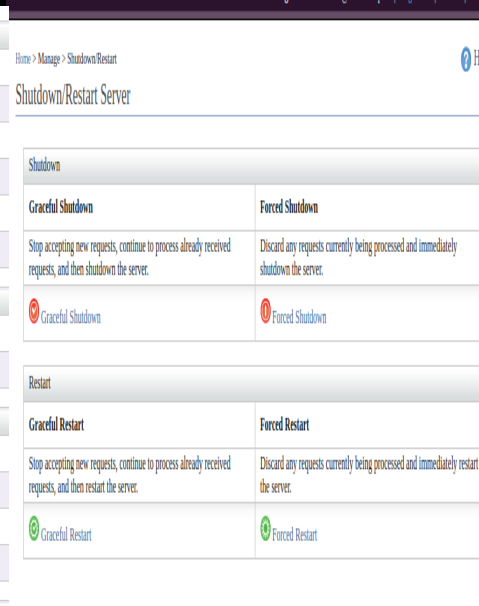
Anonymous Network Battalion 65 or ‘NB65’ claimed in 2022 to have hacked Russian Space Agency Roscosmos. The target was the Space Agencies Vehicle Monitoring System.

The group claims to have deleted the agency’s WS02 software, an open-source application program interface (API) management tool, rotated credentials, and shut down the server.









Claims to have shutdown ground systems, accessed satellites and released a database of sensitive files and documentation

Source: (Petkauskas, 2023), (Papadopoulos, 2023), Twitter: @YourAnonTV , @LatestAnonNews

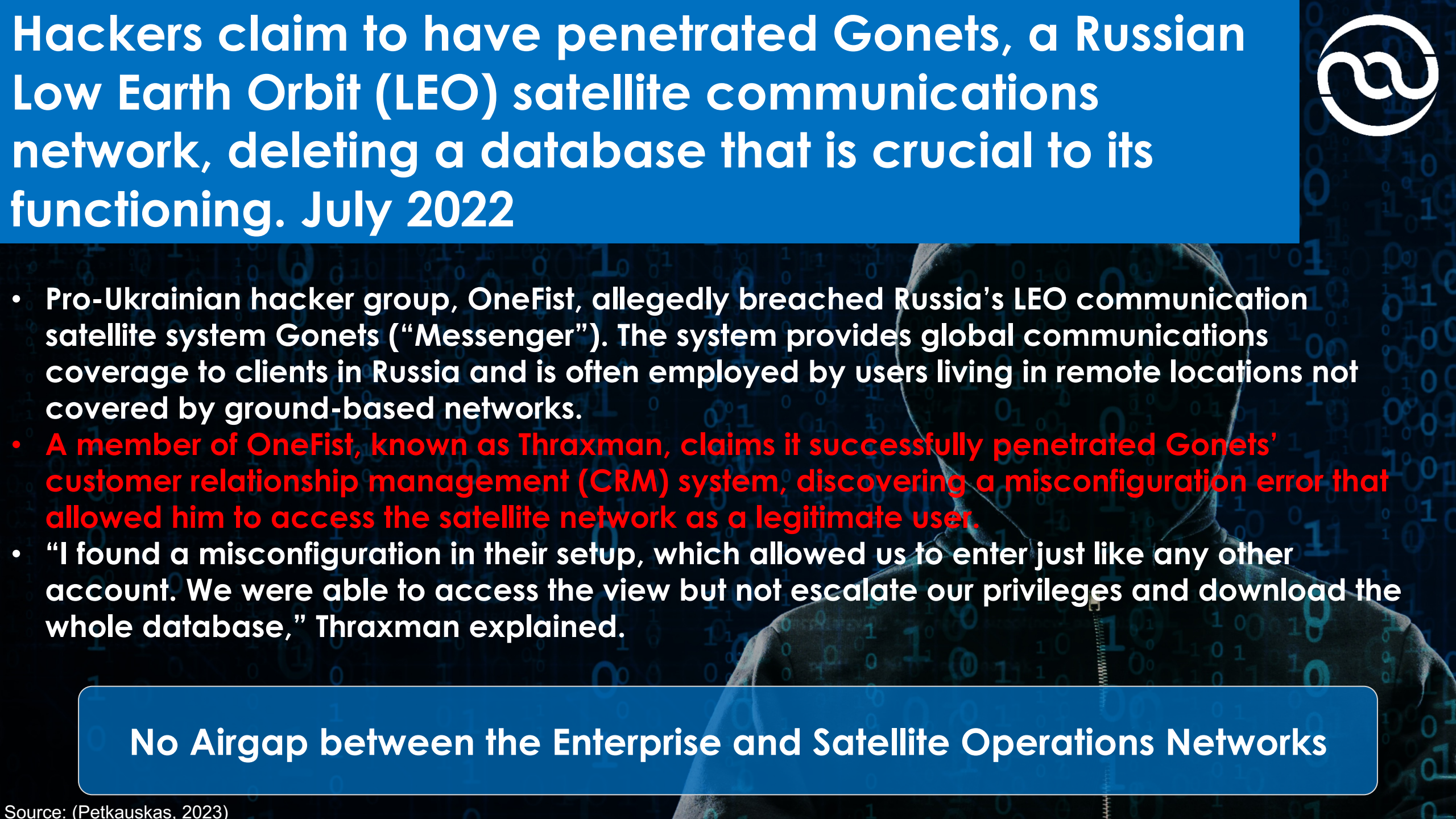
Dozor-Teleport, a Russian satellite communications provider used by the country's Ministry of Defense and security services, confirmed that hackers breached its systems in July 2023.

- "Dozor-Teleport confirmed a cyberattack on the company's systems. According to preliminary data, the infrastructure on the side of the cloud provider was compromised," head of the company Alexander Anosov said.
- Last week, attackers claiming to be aligned with the Private Military Corporation (PMC) Wagner targeted the satellite communication provider's infrastructure, damaging user terminals.

Claims to have Shutdown Ground Systems, Accessed Satellites and Released a Database of Sensitive Files and Documentation

Source: (Petkauskas, 2023), (Eswar, 2023)

Hackers claim to have penetrated Gonets, a Russian Low Earth Orbit (LEO) satellite communications network, deleting a database that is crucial to its functioning. July 2022



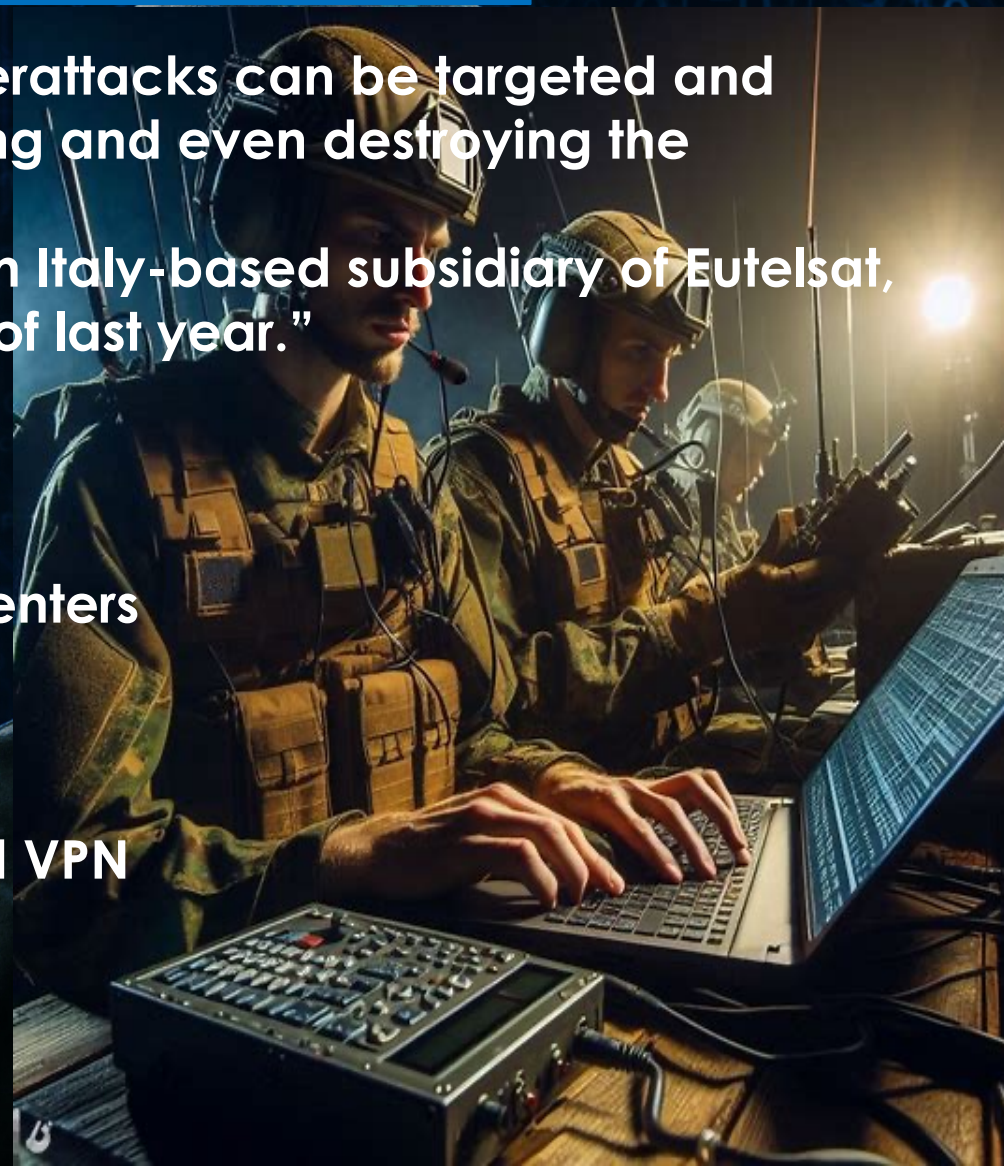
- Pro-Ukrainian hacker group, OneFist, allegedly breached Russia's LEO communication satellite system Gonets ("Messenger"). The system provides global communications coverage to clients in Russia and is often employed by users living in remote locations not covered by ground-based networks.
- A member of OneFist, known as Thraxman, claims it successfully penetrated Gonets' customer relationship management (CRM) system, discovering a misconfiguration error that allowed him to access the satellite network as a legitimate user.
- "I found a misconfiguration in their setup, which allowed us to enter just like any other account. We were able to access the view but not escalate our privileges and download the whole database," Thraxman explained.

No Airgap between the Enterprise and Satellite Operations Networks

Source: (Petkauskas, 2023)

Russia Attacked US Satellite Company Viasat 1 Hour Before Invasion of Ukraine

- “It is also one of the first real-world examples of how cyberattacks can be targeted and timed to amplify military forces on the ground by disrupting and even destroying the technology used by enemy forces.”
- “The hacked ground-based network is run by Skylogic, an Italy-based subsidiary of Eutelsat, from which Viasat purchased the KA-SAT satellite in April of last year.”

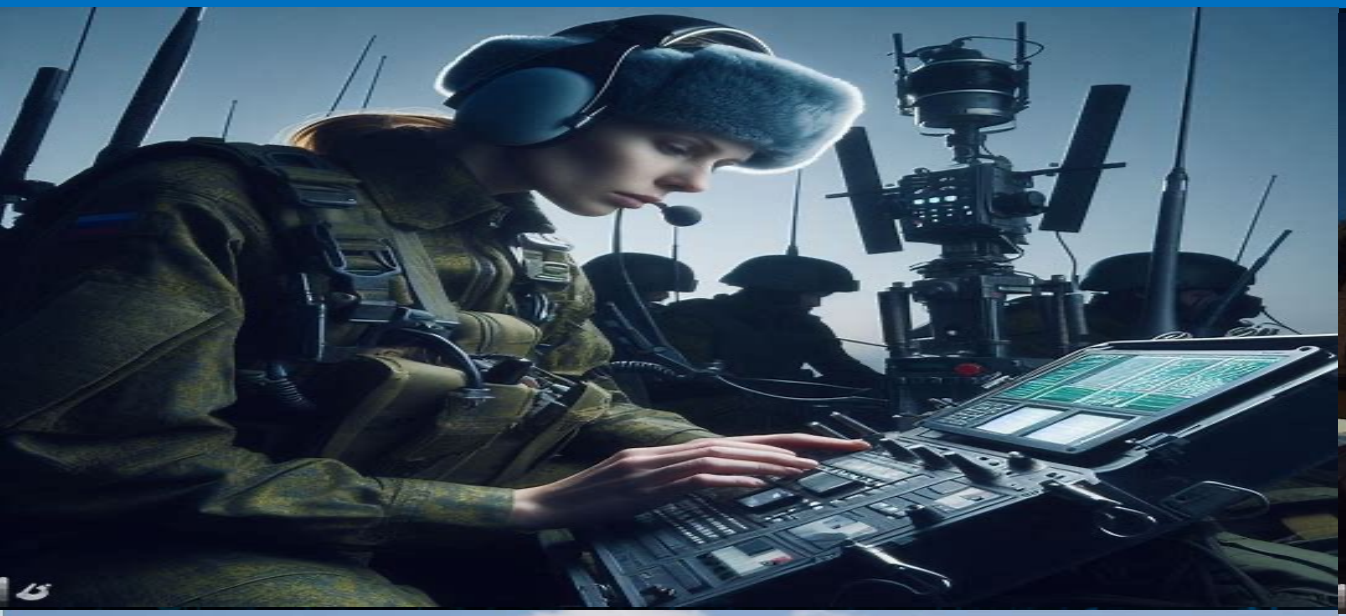


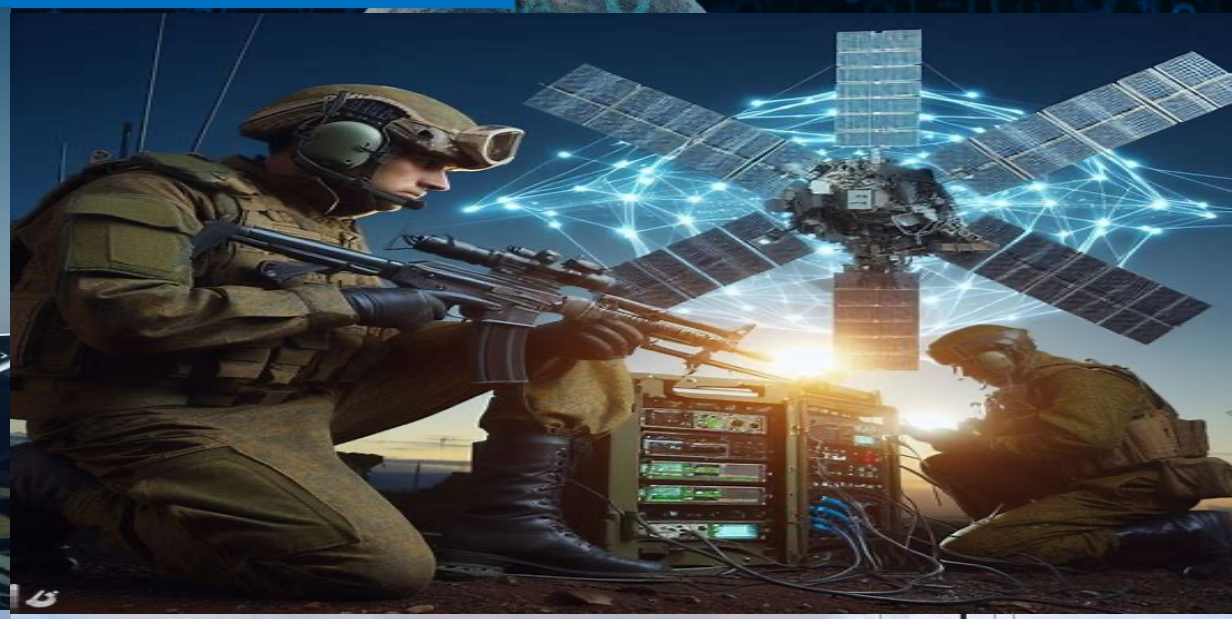
How Viasat Satellite Modems were hacked

- IP address and Credentials Reconnaissance
- Use Internet to access IP address of the Earth Gateway Centers
- Exploit VPN Vulnerability
- Select Specific Beam Spots
- Send Signal to Modems
- Access Modem Management Interface through Exploited VPN
- Upload Wiper Malware Identified as AcidRain

Sources: (Howell,2022), (Boschetti, Gordon, Falco, 2022), (Bajak, 2022)

Russia Tobol EW Space System Targeting SpaceX Starlink in Ukraine





Source: (Defense Express, 2023)

Astronomy Sites

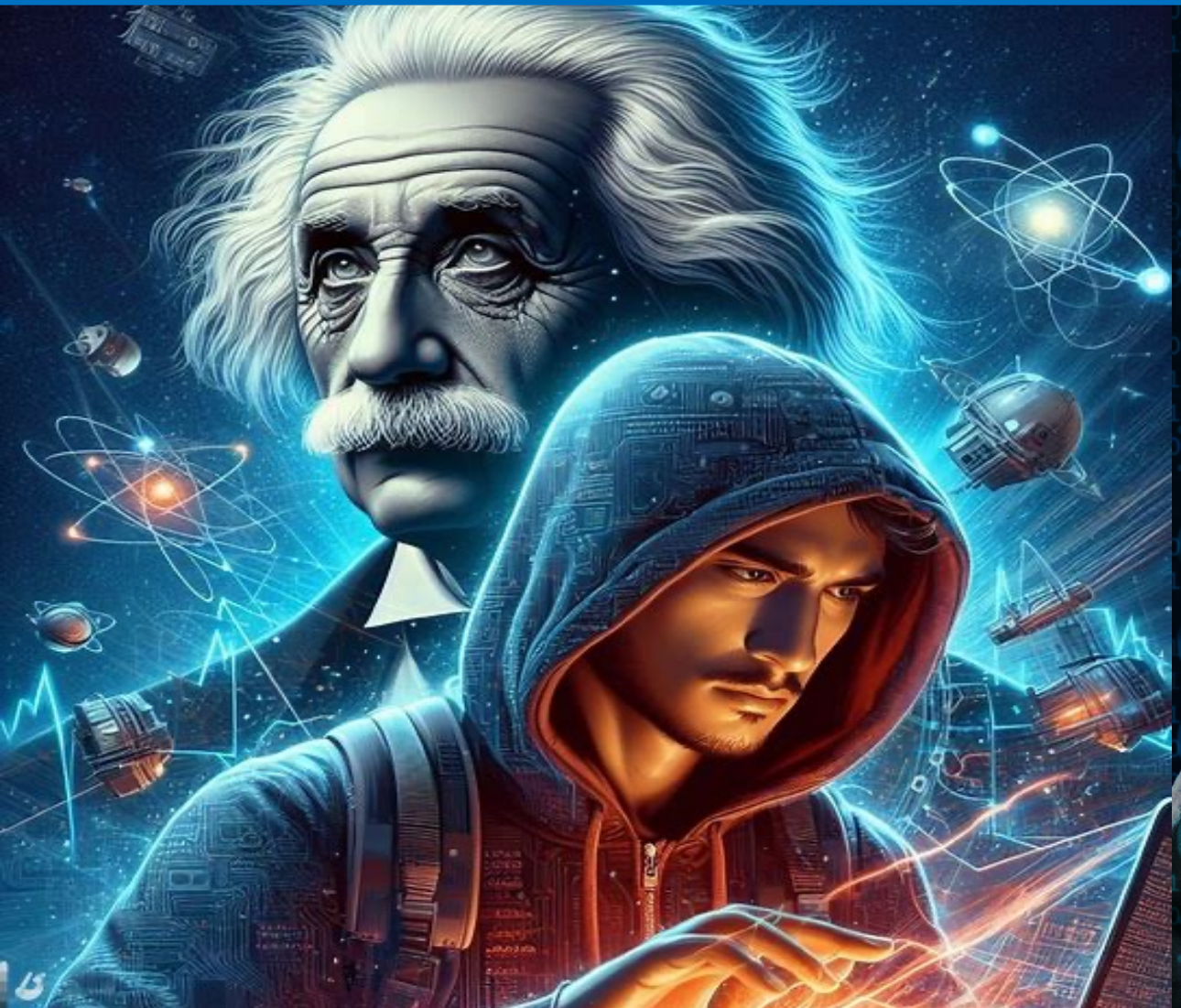
- August 2023
- 10 International Astronomy Sites in Hawaii and Chile Shutdown Due to Cyber Attacks
- Equipment in Hawaii Shutdown in Time to Prevent Physical Damage
- Loss of Remote Access for Researchers Until Resolved

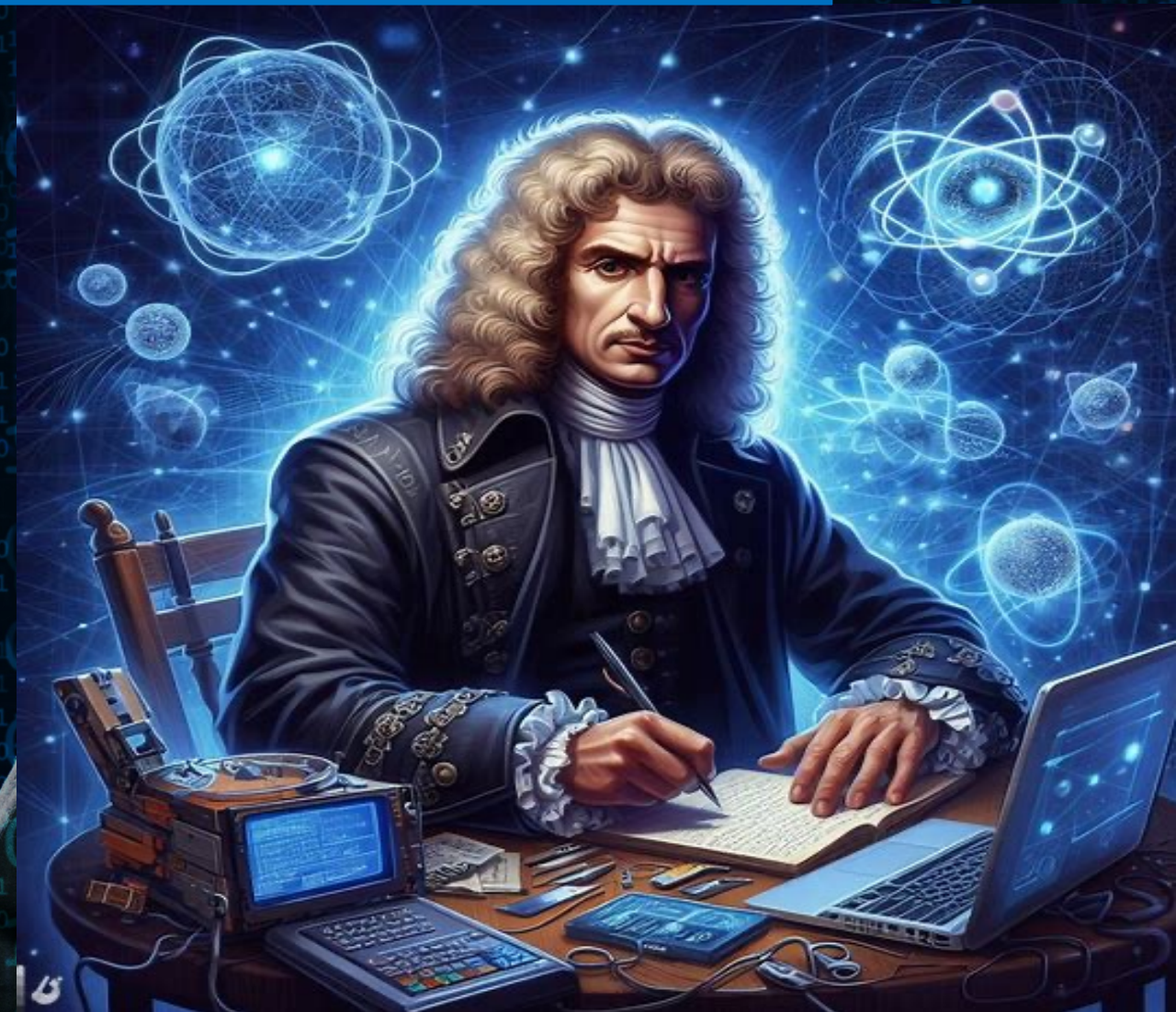
- October 2022
- Atacama Large Millimeter/submillimeter Array (ALMA) in Chile

Source: (Zhao, Gupta, 2023), (Kelvey, 2022)

How Do We Detect the Undetectable “Alien Persistent Threats”?

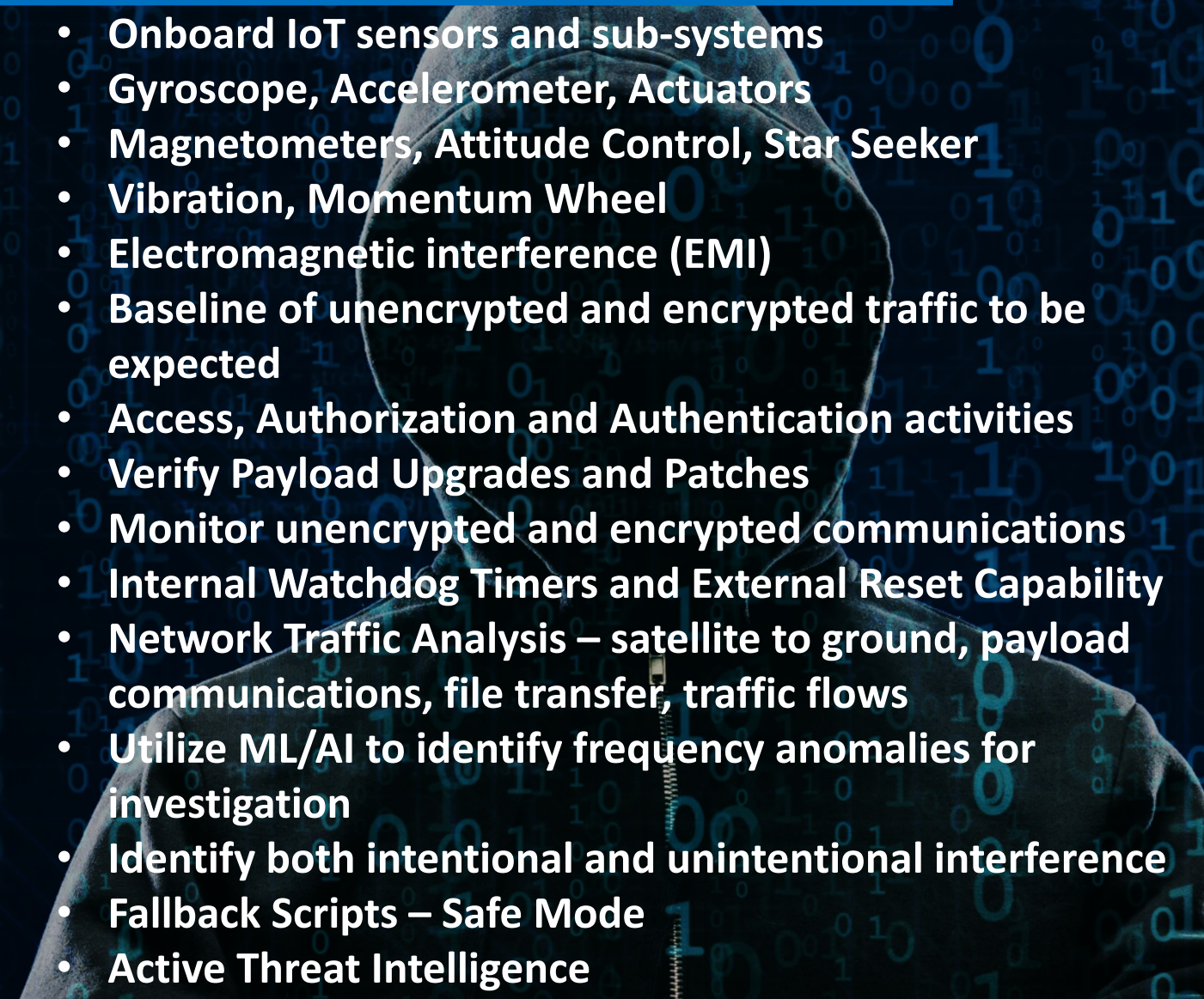
How Would Physicists Detect the "Alien Persistent Threat"?





Spacecraft Systems and Physics-based Sensors Data to Monitor

- Frequency Spectrum Analysis
- Authorized Frequencies
- Frequency Utilization
- Identify Unexpected Signals
- Laser Ranging
- Doppler Tracking
- Classify the Signals – TT&C etc.
- Identify source of interference utilizing geolocation tools
- Frequency signature detection for spoofing, jamming etc.
- Archive frequency data for ML/AI analysis
- Position, Navigation, & Timing
- Temperature, Pressure, & Power



- Onboard IoT sensors and sub-systems
- Gyroscope, Accelerometer, Actuators
- Magnetometers, Attitude Control, Star Seeker
- Vibration, Momentum Wheel
- Electromagnetic interference (EMI)
- Baseline of unencrypted and encrypted traffic to be expected
- Access, Authorization and Authentication activities
- Verify Payload Upgrades and Patches
- Monitor unencrypted and encrypted communications
- Internal Watchdog Timers and External Reset Capability
- Network Traffic Analysis – satellite to ground, payload communications, file transfer, traffic flows
- Utilize ML/AI to identify frequency anomalies for investigation
- Identify both intentional and unintentional interference
- Fallback Scripts – Safe Mode
- Active Threat Intelligence

Satellites Commands That May Indicate Compromise to Monitor

- Login Attempts
- Unauthorized Software Upload
- Unexpected Attitude Change
- Disable Security Mechanisms
- Deactivate Telemetry System
- Alter communication Path
- Initiate unauthorized maneuver
- Enable Unauthorized Payload
- Transmit Malicious Signal
- Unauthorized System Access
- Software Updates and patching

- Critical Command Execution
- Configuration Changes
- Telemetry Data Anomalies
- Unauthorized access to Ground Stations
- Remote Restart or Shutdown
- Orbit changes
- Unexpected Communication
- Power
- Diagnostics
- Data Transfer
- Security

- TT&C
- Navigation
- Sensor
- Maintenance
- Timing
- Authorization Requests
- Collision Avoidance
- Failed Command Execution
- Inject False Commands
- Change Security Keyes
- Emergency

Spacecraft Cybersecurity and Payload AI/ML Models

Adversarial Machine Learning (AML)

- Craft Custom Waveforms to Defeat Jamming and Spoofing Defenses
- Custom Exploits to Evade Detection by Cybersecurity Intrusion Protection System (IPS) ML Models
- Payload Data - Integrity, Confidentiality, Privacy, Availability
- Implant an Exploit in Order to Target the Ground Station

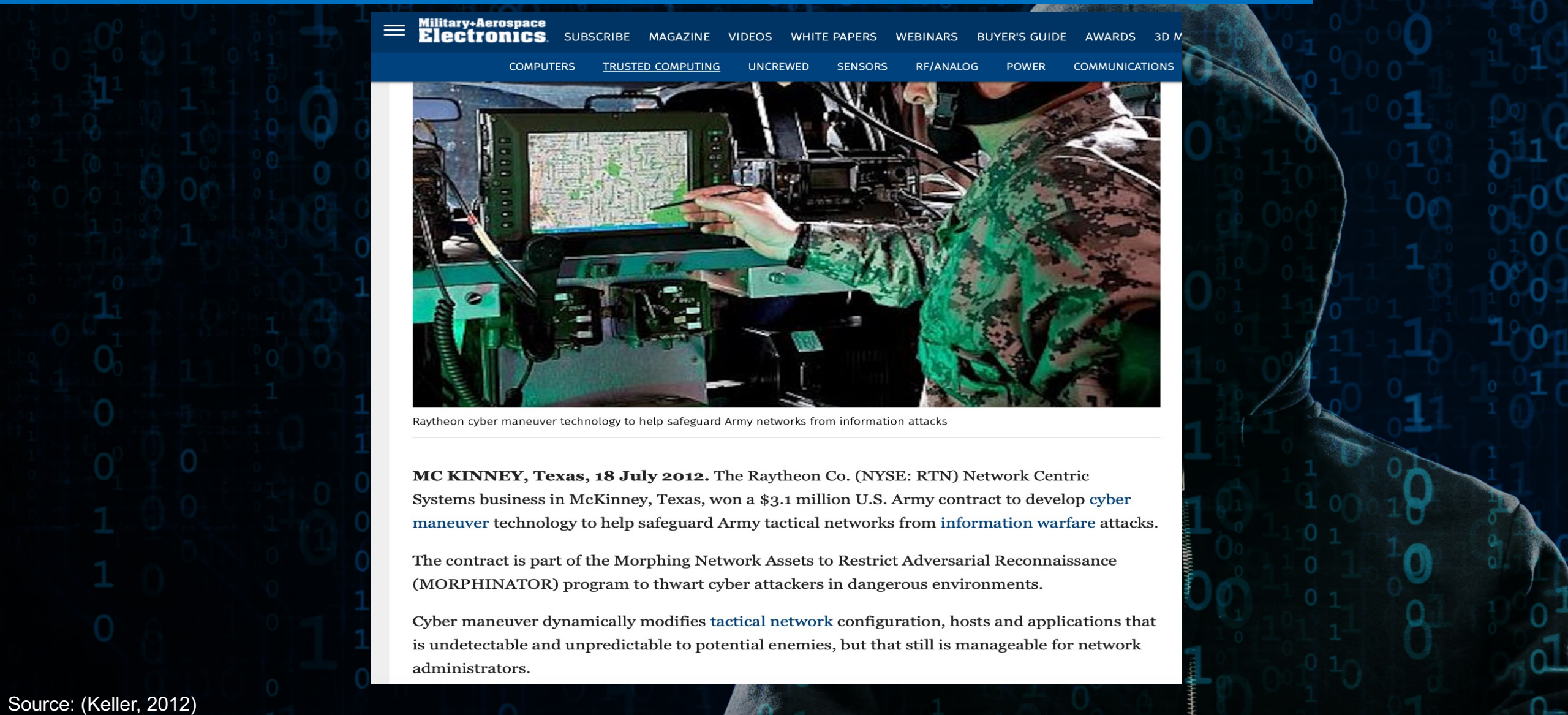
Counter Adversarial Machine Learning (CAML)

- Leverage AML in ML Model Training
- Monitor for Unusual Data Patterns
- Secure the Model System Environment

Sources: (Sagduyu, Shi, Erpek, 2019), (Short, La Pay, Gandhi, 2019), (Haydock, 2023), (Tabassi, Burns, Hadjimichael, Molina-Markham, Sexton, 2019), (Mitre Atlas, 2021), (Kusnezov, Barsoum, Begoli, Henninger, Sadovnik ,2023), (Pultarova, 2022)

Self-healing Dynamic Morphing Deception Spacecraft

Raytheon MORPHINATOR for Tactical Networks



Military+Aerospace Electronics

SUBSCRIBE MAGAZINE VIDEOS WHITE PAPERS WEBINARS BUYER'S GUIDE AWARDS 3D M

COMPUTERS TRUSTED COMPUTING UNCREWED SENSORS RF/ANALOG POWER COMMUNICATIONS

Raytheon cyber maneuver technology to help safeguard Army networks from information attacks

MC KINNEY, Texas, 18 July 2012. The Raytheon Co. (NYSE: RTN) Network Centric Systems business in McKinney, Texas, won a $3.1 million U.S. Army contract to develop cyber maneuver technology to help safeguard Army tactical networks from information warfare attacks.

The contract is part of the Morphing Network Assets to Restrict Adversarial Reconnaissance (MORPHINATOR) program to thwart cyber attackers in dangerous environments.

Cyber maneuver dynamically modifies tactical network configuration, hosts and applications that is undetectable and unpredictable to potential enemies, but that still is manageable for network administrators.

Source: (Keller, 2012)

Satellite Recovery in Orbit – Safe Mode

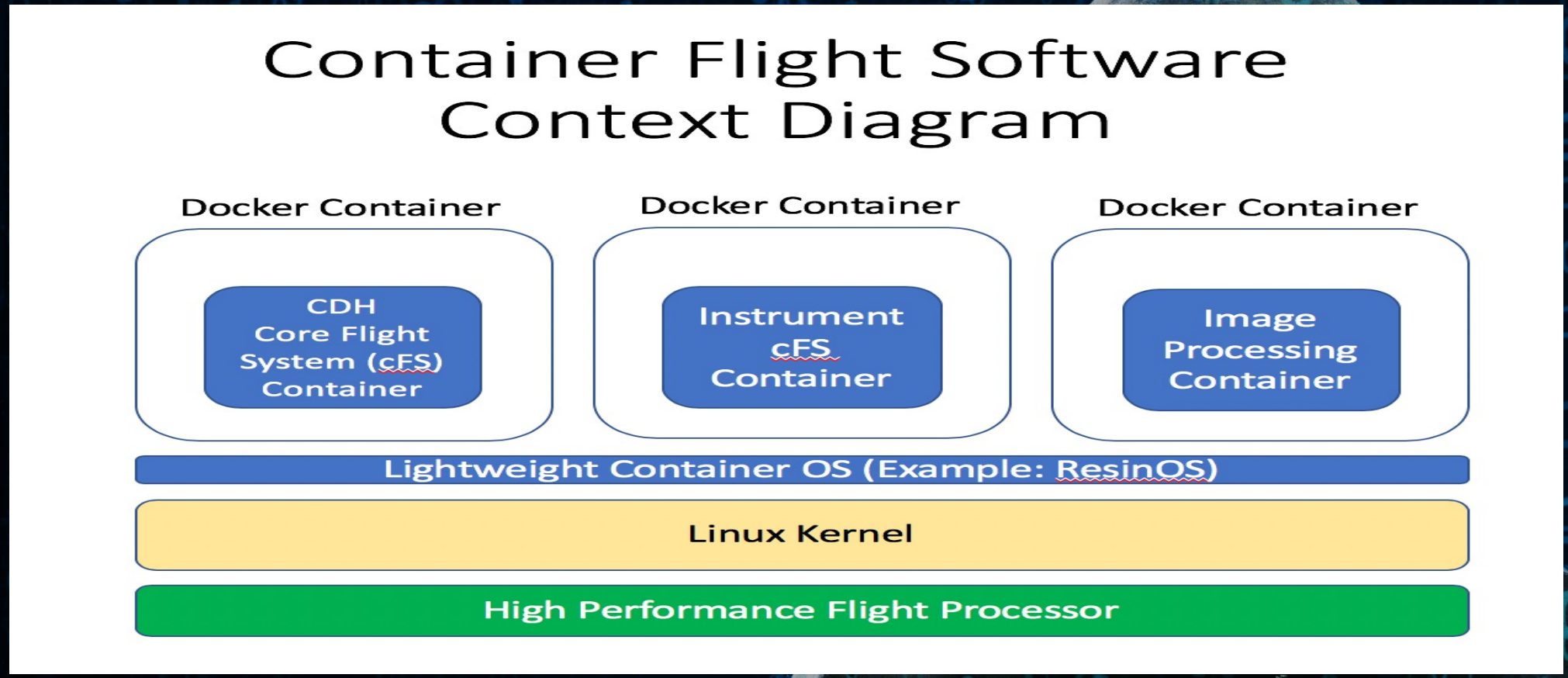
Watchdog Timers
- External Microcontroller
- Integrated Microcontroller
- Software manages the timer settings
- Reset capability

Fallback Scripts
- Golden OS Software Images
- Restore to Known Good Trusted OS

Failsafe scripts
- Unencrypted Communications
- Restore Communications

Source: (Stork, 2017), (Kaczmarek, 2023),
(Langer, Orlandic, Bakken, Birkeland, Garrett, Johansen, Sorensen, 2023)

NASA Container Flight Software



DoD May Use SUSE RGS's K3s Kubernetes For Satellite One

Sources: (NASA, 2019), (Pulley, 2021)

Autonomous Container Orchestration on the Satellite Possible

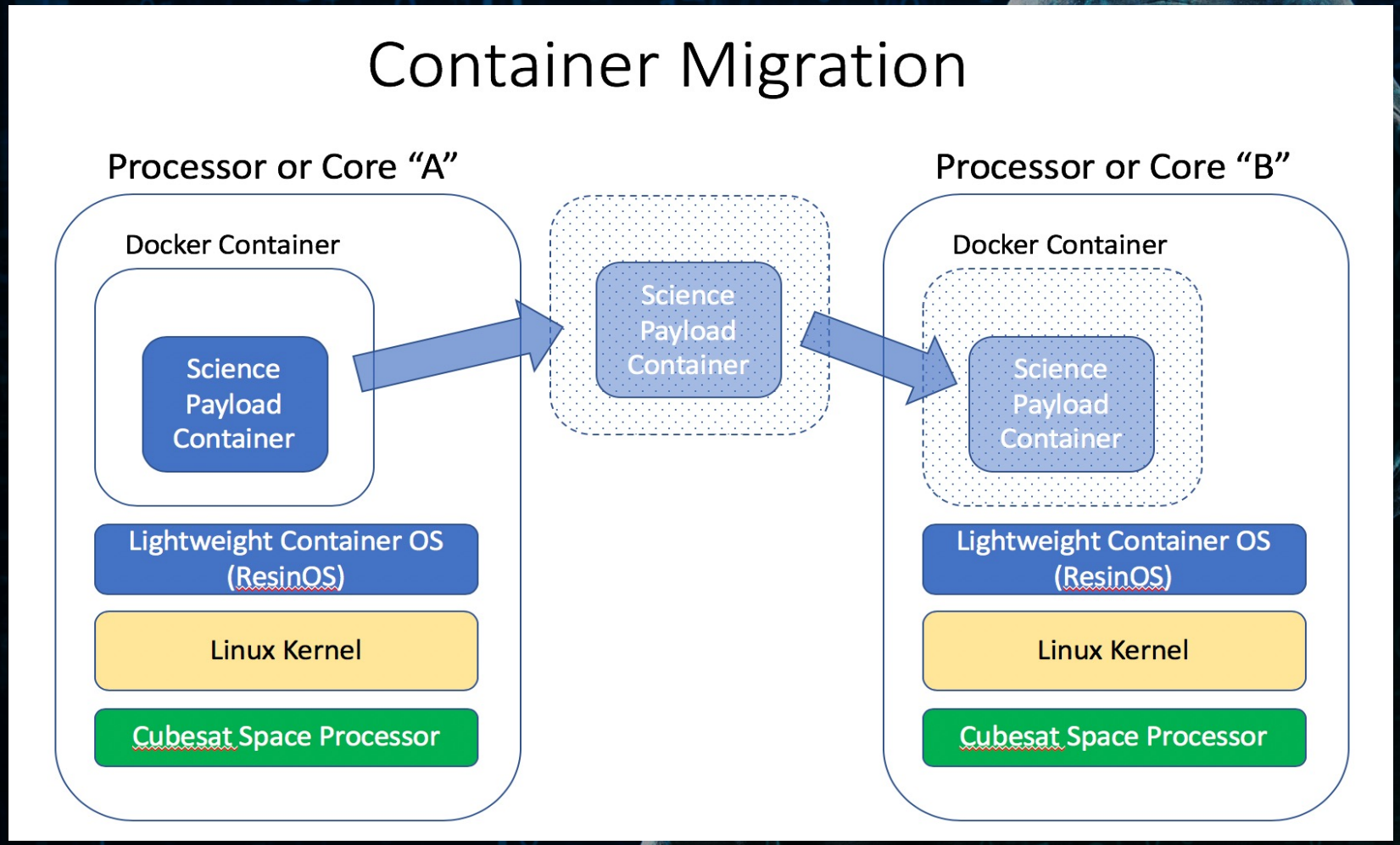


Image source: (NASA, 2021)
Reference: (Seffers, 2019)

Satellite Autonomous Moving Target Defense (SAMTD)

- Create a Moving Target for Attacker
- Automated Container Orchestration
- Dynamic Morphing Configuration
- Honeypot Payload Containers
- Golden Trusted Containers
- Dynamic Communications
- Software Defined Radio (SDR)
- Spread Spectrum & Frequency Hopping
- Keep the Adversary Uncertain
- Create Perception of Randomness
- Large Language Models
- Game Theory
- Collect Cyber and EW Intelligence
- Increase Time, Cost, Complexity, Skills, Intel
- Extensive Red Team Testing and Calibration

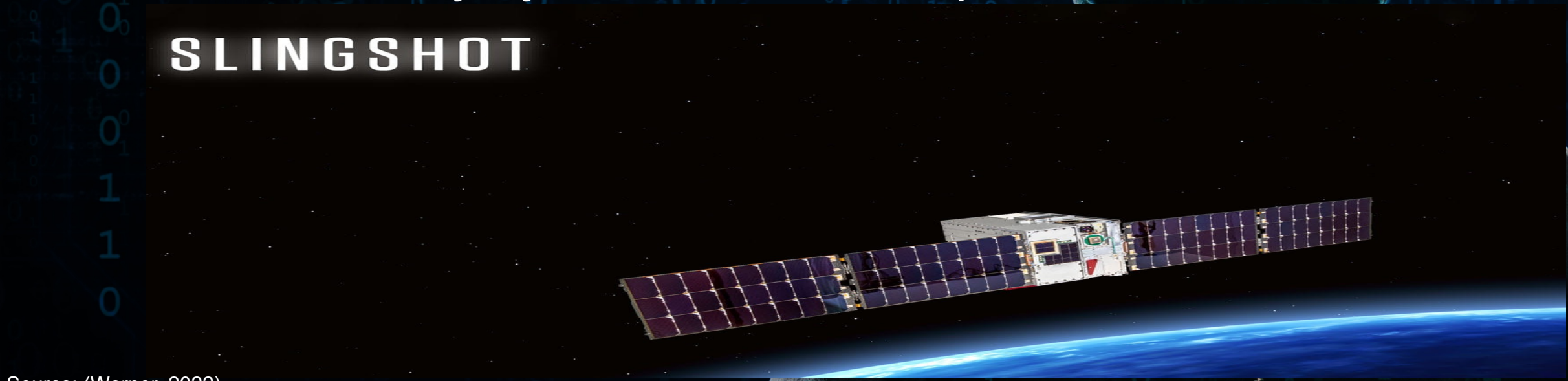
Sources: (Werner, 2019), (Pultarova, Via Satellite), (NSTC, 2011), (Gini, 2014), (Airbus, 2024), (Obering, Paran, Montgomery-Recht, Snipes, Courey, 2024)

Space Cybersecurity Immunity

- Electronic Warfare Detection
- Reconfigurable Software Defined Radio
- Cybersecurity Detection
- Intrusion Protection System
- Counter Adversarial ML (CAML)
- Large Language Models
- Autonomous Container Orchestration
- Deception Containers
- Moving Target
- Intelligence Gathering
- Fallback Scripts \ Watchdog – Safe Mode
- Intelligent Cybersecurity Immune System

First Satellite with Cybersecurity Monitoring and Threat Hunting Capabilities

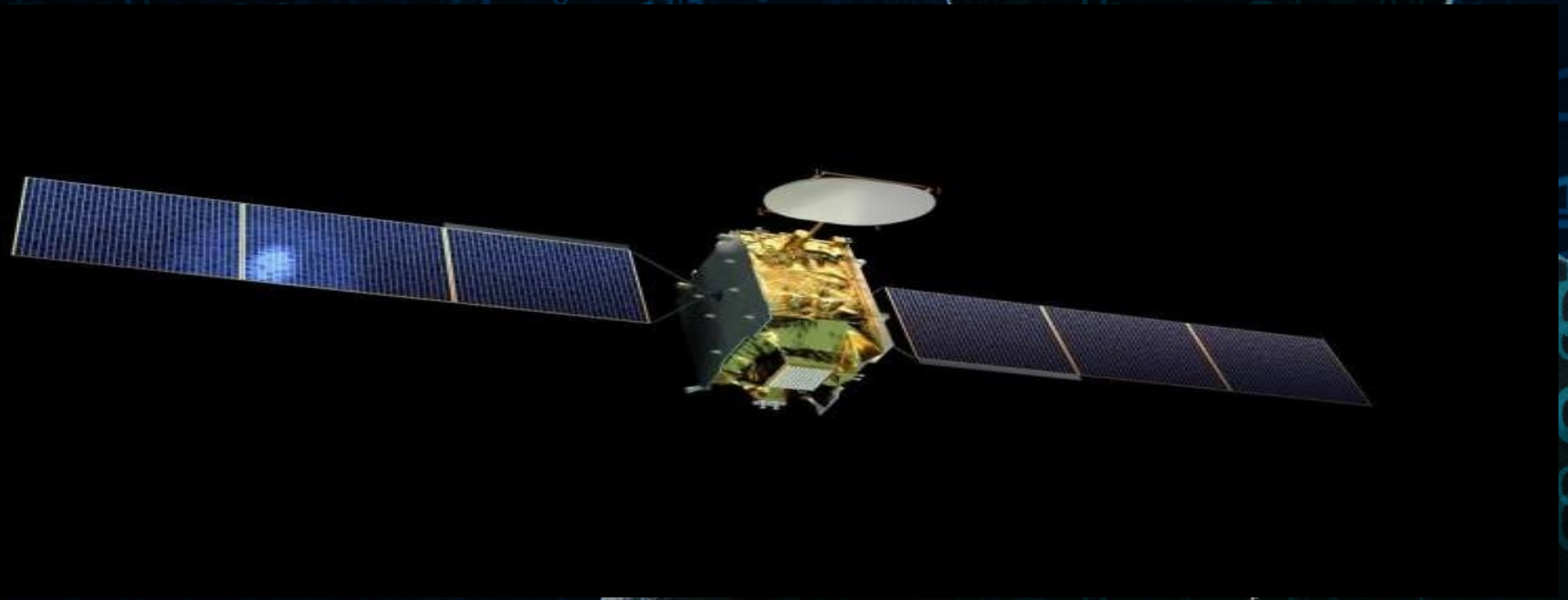
- SLINGSHOT Satellite launched in September 2022
- Intrusion Protection System (IPS)
- Continuously monitors and logs satellite telemetry
- Commands and flight software configuration are monitored
- AI/ML utilized to identify any commands that are unexpected



Source: (Werner, 2022)

European Space Agency
Satellite with EW Monitoring Capability

- Satellite was launched on 30 July 2021
- Software-defined satellite
- Can be reprogrammed in orbit
- Detect and dynamically defend itself from any accidental interference or intentional jamming



Source: (European Space Agency, 2021)


Questions?
@PaulCoggin

References

- Payo, F. (2023) Russian hacker claims to have hacked INPE satellites. *Tecmundo*. Retrieved from https://www.tecmundo.com.br/seguranca/266902-hacker-russo-diz-ter-invadido-satelites-inpe.htm
- Petkauskas, V. Prominent hackers target Russia's satellite infrastructure. (2022) *Cybernews*. Retrieved from https://cybernews.com/news/prominent-hackers-target-russias-spy-satellites/
- Papadopoulos, L. (2022) Anonymous says Russia's spy satellites are now hacked. But the nation denies everything. *Interesting Engineering*. Retrieved from https://interestingengineering.com/science/says-russia-denies-anonymous-hack-claims
- Twitter: @YourAnonTV , @LatestAnonNews
- Petkauskas, V. (2023). Russian satellite telecom confirms hacker attack, Vilius Petkauskas. Cybernews. Retrieved from https://cybernews.com/cyber-war/russian-satellite-telecom-confirms-hacker-attack/
- Eswar. (2023) Hackers Compromised the Russian Defense Satellite Communications Provider. *GB Hackers on Security*. Retrieved from https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/russian-satellite-hacked/amp/
- Petkauskas, V. (2023) We breached Russian satellite network, say pro-Ukraine partisans. Retrieved from https://cybernews.com/cyber-war/we-breached-russian-satellite-network-say-pro-ukraine-partisans/
- Howell, P. (2022) Russia hacked an American satellite company one hour before the Ukraine invasion, Retrieved from https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/
- Boschetti, N., Gordon, G., & Falco, G. (2022) Space Cybersecurity lessons learned from the ViaSat cyberattack. *Aerospace Research Central.* Retrieved from https://arc.aiaa.org/doi/abs/10.2514/6.2022-4380

References

- Bajak, F. (2022). Satellite modems nexus of worst cyberattack of Ukraine war. *Associated Press News*. Retrieved from https://apnews.com/article/russia-ukraine-technology-business-europe-broadband-internet-895f8aad2e71f56a5930aeaf833ff20f
- Defense Express. (2023). Does Russian 14Ts227 Tobol system have the power to suppress Starlink. *Defense Express*. Retrieved from https://en.defence-ua.com/weapon_and_tech/does_russian_14ts227_tobol_system_have_the_power_to_suppress_starlink-6454.html
- Zhao, C. & Gupta T. (2023) Cyberattack shutters major NSF-funded telescopes for more than 2 weeks. *Science.* Retrieved from https://www.science.org/content/article/cyberattack-shutters-major-nsf-funded-telescopes-more-2-weeks
- Kelvey, J. (2022) Alma radio telescope in Chile taken down by cyber attack. *Independent*. Retrieved from https://www.independent.co.uk/space/alma-radio-telescope-chile-attack-b2216170.html
- Sagduyu, Y., Shi, Y., & Erpek, T. (2019). Adversarial deep learning for over-the-air spectrum poisoning attacks, *IEEE.*
- Short, A. LaPay, T., & Gandhi, A. (2019) Defending Against Adversarial Examples. *Sandia National Laboratory,* https://www.osti.gov/biblio/1569514
- Mitre Atlas, https://atlas.mitre.org

References

- Haydock, W. (2023). The Artificial Intelligence Risk Scoring System (AIRSS). *Deploy Securely*. Retrieved from https://blog.stackaware.com/p/artificial-intelligence-risk-scoring-system-p1
- Tabassi, E., Burns, K., & Hadjimichael, M. (2019). A taxonomy and terminology of adversarial machine learning. *National Institute of Standards and Technology.* Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8269-draft.pdf
- Kusnezov, D., Barsoum, Y., Begoli, E., Henninger, A., & Sadovnik, A. (2023) Adversarial artificial intelligence threats: A DHS S&T study. *Department of Homeland Security.* Retrieved from https://www.dhs.gov/sites/default/files/2023-12/23_1222_st_risks_mitigation_strategies.pdf
- Pultarova, T. (2022) Amazon tests machine learning software to analyze satellite images from space. *Space.com.* Retrieved from https://www.space.com/amazon-satellites-machine-learning-in-orbit-first
- Keller, J. (2012). Raytheon cyber maneuver technology to help safeguard Army networks from information attacks. *Military and Aerospace Electronics*. Retrieved from https://www.militaryaerospace.com/trusted-computing/article/16720243/raytheon-cyber-maneuver-technology-to-help-safeguard-army-networks-from-information-attacks
- Stork, T. (2017). Using a watchdog in a multi-task (RTOS) environment. *Segger.* Retrieved from https://blog.segger.com/using-a-watchdog-in-a-multi-task-rtos-environment/
- NASA Goddard Space Flight Center (2021). Important ROSAT Dates. Retrieved from https://heasarc.gsfc.nasa.gov/docs/rosat/rosat_history.html

References

- Langer, D., Orlandić, M., Bakken, S., Birkeland, R., Garrett, J., Johansen, T., & Sørensen, A. (2023). Robust and reconfigurable on-board processing for a hyperspectral imaging small satellite. *Remote Sensing,* 15(15), 3756.Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/3087639/remotesensing-15-03756 .pdf?sequence=1&isAllowed=y
- Kaczmarek, S. (2021). Cybersecurity for space assets: Focusing on smallsats and cubesats. *Sylvester Kaczmarek,* Retreived from https://sylvesterkaczmarek.com/blog/cybersecurity-for-space-assets-focusing-on-smallsats-and-cubesats/
- Lowery, A. (2019). Container Flight Software. *NASA*. Retrieved from https://techport.nasa.gov/view/94827
- Pulley, J. (2021) How kubernetes could transform DoD's satellite fleet. *Govloop*. https://www.govloop.com/how-kubernetes-can-transform-dods-satellite-fleet/
- Seffers, G. (2019) Teaching satellites self-defense. *AFCEA*. Retrieved from https://web.archive.org/web/20220706014843/https://www.afcea.org/content/teaching-satellites-self-defense
- Werner, D. (2019) Small satellites, big weakness. *Aerospace America.* Retrieved from https://aerospaceamerica.aiaa.org/features/small-satellites-big-weakness/
- Pultarova, T. (n.d.) Battle in cyberspace. *Via Satellite.* Retrieved from https://interactive.satellitetoday.com/battle-in-cyberspace/
- Executive Office of the President National and Science Technology Council. (2011) Trustworthy cyberspace: Strategic plan for the Federal cybersecurity research and development program. Retrieved from https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

References

- Werner, D. (2022). Satellite to test-fly new cyber software. *Spacenews.* Retrieved from https://spacenews.com/satellites-to-test-fly-new-cyber-software/
- Gini, A. (2014). Cyber crime – From cyber space to outer space. *Space Safety Magazine*. Retrieved from http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/
- Defense in Space. (2019). Honeypot – A deceptive security. *Airbus*. Retreived from https://www.cyber.airbus.com/defence-bespoke-security/deceptive-security/
- Rowlands, G. (2019) Astrosubterfuge: Deception & disguise in the space domain. *Australian Army Research Centre.* Retrieved from https://researchcentre.army.gov.au/library/land-power-forum/astrosubterfuge-deception-disguise-space-domain
- Werner, D. (2022) Satellite to test-fly new cyber software. *Spacenews.* Retrieved from https://spacenews.com/satellites-to-test-fly-new-cyber-software/
- European Space Agency. (2021). European software-defined satellite starts service. *Tech Xplore*. Retrieved from https://techxplore-com.cdn.ampproject.org/c/s/techxplore.com/news/2021-11-european-software-defined-satellite.amp
- Obering, T., Parin, C., Montgomery-Recht, E., Snipes, T., & Courey, K. (2024) Using large language models to protect satellites from attack. *U.S. Naval Institute*. Retrieved from https://www.usni.org/magazines/proceedings/sponsored/using-large-language-models-protect-satellites-attack

References

- Fritz, J. (2013). Satellite hacking: A guide for the perplexed. *Culture Mandala*, 10(1), 5906. Retrieved from https://cm.scholasticahq.com/article/5906.pdf
- Wess, M. (2021). ASAT goes cyber. *U.S. Naval Institute*. Retrieved from https://www.usni.org/magazines/proceedings/2021/february/asat-goes-cyberSource
- Arthur, C. (2011). Chinese hackers suspected of interfering with US satellites. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected
- Grossman, L. (1999) Did hackers hijack a British military satellite? *Time.* Retrieved from http://content.time.com/time/magazine/article/0,9171,20673,00.html
- Gibbs, S. (2013). International Space Station attacked by 'virus epidemics'. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/nov/12/international-space-station-virus-epidemics-malware
- Telegraph. (1999) British hackers attack MoD satellite. *Telegraph.* Retrieved from https://web.archive.org/web/20070510032306/http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/1999/03/04/ecnhack04.xml
- Grossman, L. (1999). Did hackers hijack a British military satellite. *Time*. Retrieved from http://content.time.com/time/magazine/article/0,9171,20673,00.html
- BBC News. (n.d.) Satellite hijack 'impossible'. *BBC News.* Retrieved from http://news.bbc.co.uk/2/hi/science/nature/288965.stm
- *Sightings*. (n.d.) Hackers Seize British Military satellite. Retrieved from https://rense.com/ufo2/hackuk.htm
- Maguire, P. (2024) Satellites and the specter of IoT attacks. Space News. Retreived from https://spacenews.com/satellites-specter-iot-attacks/

Backups

Space Threat Hunting

Space Systems
Tactical Systems
IoT\OT\ICS\SCADA
Service Provider
Critical Infrastructure
Internet of Military Things
Internet of Battle Things
Internet of Space Things

In-band Network Data Sources
Out-of-band Network Data Sources
Over 22 Satellite Operating Systems
Over 37 Satellite Command Languages
Over 21 Satellite Network Protocols

Apply ML/AI Analysis
Detailed Airgap Architecture