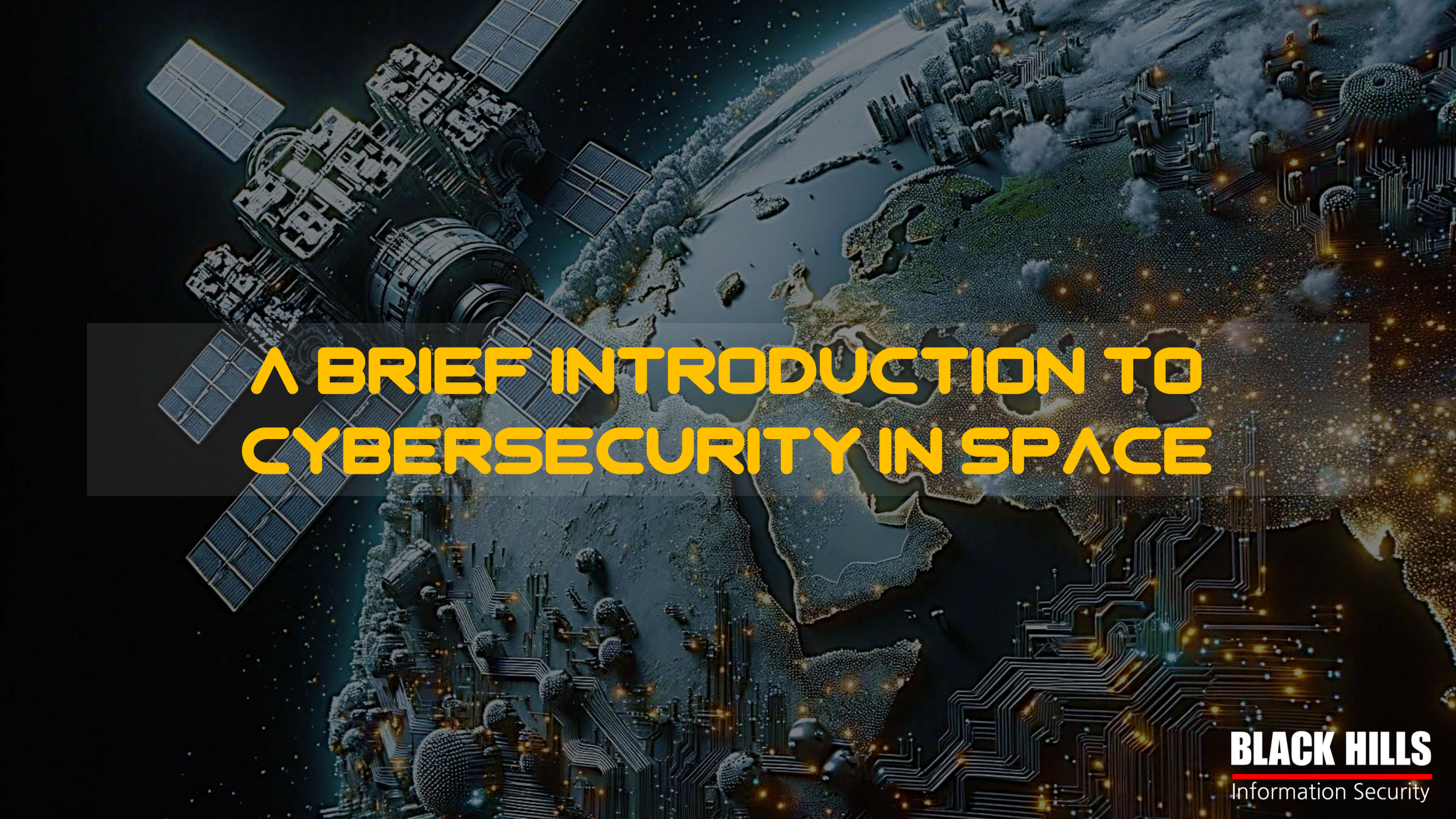
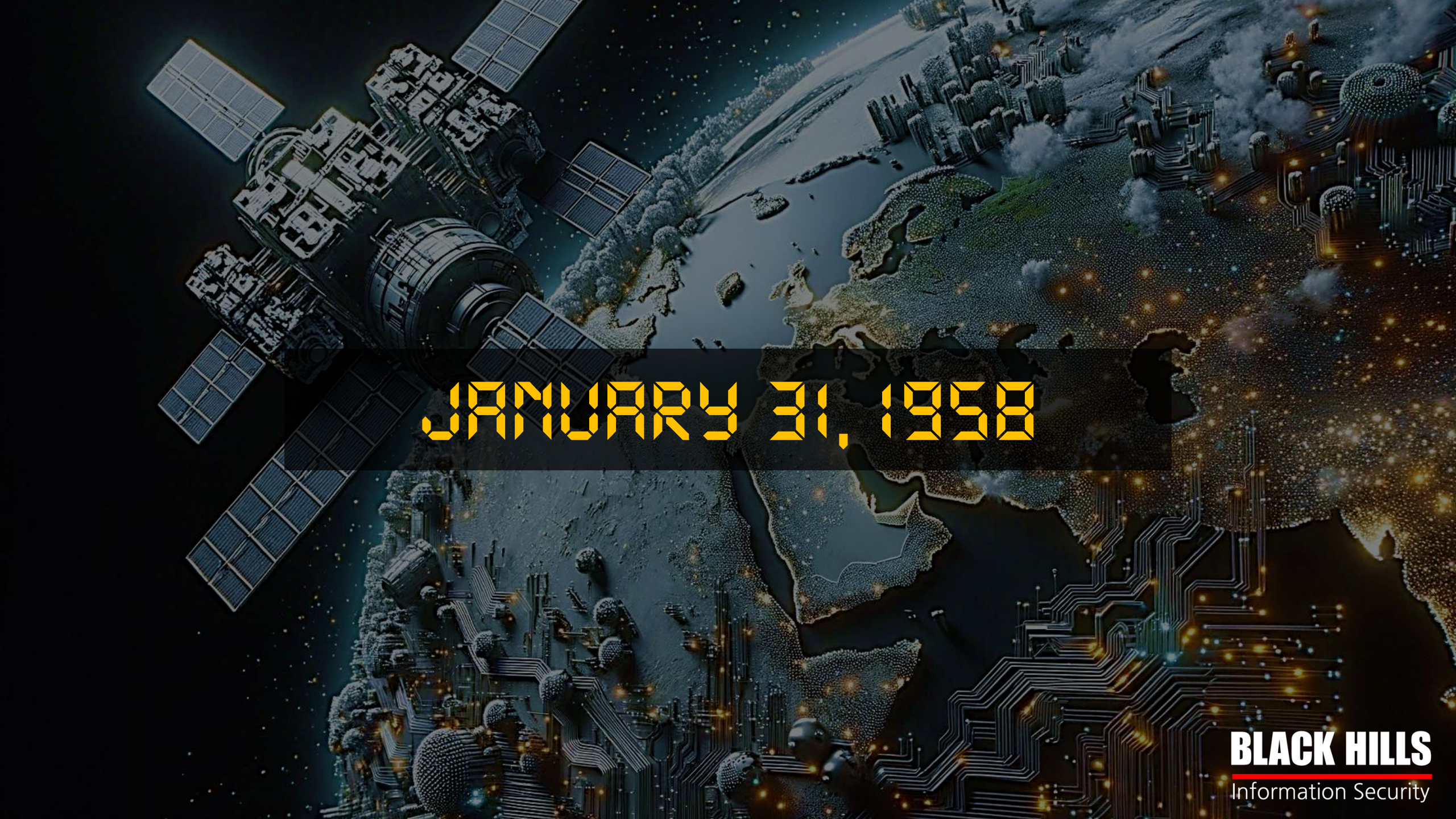

A BRIEF INTRODUCTION TO
CYBERSECURITY IN SPACE
BLACK HILLS
Information Security

BLACK HILLS
Information Security

BLACK HILLS
Information Security



BLACK HILLS
Information Security

Stuxnet pinned for killing Indian satellite

By Liam Tung
Oct 1 2010 6:36AM

RELATED




China-India space race.

As speculation mounted that Israel's military created the Siemens-targeting Stuxnet worm, a US security researcher claimed to have evidence it was also responsible for destroying an Indian broadcasting satellite.

"There are more and better theories to explain Stuxnet's motivation than just Israel and Iran, as others have posited," Jeffrey Carr, author of "Inside Cyber Warfare" and *Forbes' The Firewall* blog wrote.

While Stuxnet had found its way into Iran's first nuclear power plant, Carr said the Indian Space Research Organisation (ISRO) - which used the vulnerable Siemens devices - had also fallen victim to Stuxnet.

WIRED STAFF BUSINESS APR 20, 2009 12:00 PM

The Great Brazilian Sat-Hack Crackdown

Brazilian satellite hackers use high-performance antennas and homebrew gear to turn U.S. Navy satellites into their personal CB radios. Photo: Divulgação/Polícia Federal CAMPINAS, Brazil — On the night of March 8, cruising 22,000 miles above the Earth, U.S. Navy communications satellite FLTSAT-8 suddenly erupted with illicit activity. Jubilant voices and anthems crowded the channel on a [...]

Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault

The satellite hack that took the world by storm was more complex than initially thought, according to a Viasat executive.

BY CHRISTIAN VASQUEZ AND ELIAS GROLL • AUGUST 10, 2023

Spacecraft launch. Elements of this image furnished by NASA. (Getty Images)

LAS VEGAS — The cyberattack that crippled satellite communications on the eve of the Ukraine war was more broad than initially understood and carried out by attackers with detailed knowledge of the compromised system, an executive with Viasat, whose modems were targeted in the attack, revealed during a talk Thursday at the Black Hat cybersecurity conference in Las Vegas.

SHARE

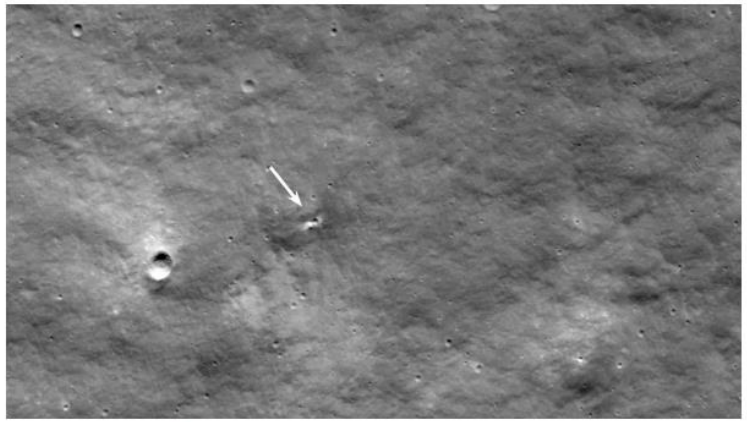
BLACK HILLS
Information Security

Russia pinpoints cause of Luna-25 moon lander's failure

By Mike Wall published 8 days ago

An onboard control unit failed to turn Luna-25's thrusters off at the proper time.

Comments (0)



Lunar Reconnaissance Orbiter image of a crater likely caused by the crash of Russia's Luna-25 probe into the moon on Aug. 19, 2023. (Image credit: NASA's Goddard Space Flight Center/Arizona State University)

Russia says it knows what caused the failure of its first moon shot in nearly 50 years.

The Luna-25 lander — the first Soviet or Russian moon probe since Luna-24 in 1976 — crashed into the moon on Aug. 19, during a maneuver designed to set up a touchdown attempt near the lunar south pole two days later.

Officials with Roscosmos, Russia's federal space agency, announced a proximate cause for the mishap shortly thereafter: Luna-25's engines fired for 127 seconds during the burn instead of the scheduled 84.

https://www.space.com/russia-luna-25-moon-crash-cause-found

Phobos 1

Article Talk

Phobos 1 was an uncrewed Soviet space probe of the Phobos Program launched from the Baikonour launch facility on 7 July 1988.[1] Its intended mission was to explore Mars and its moons Phobos and Deimos. The mission failed on 2 September 1988 when a computer malfunction caused the end-of-mission order to be transmitted to the spacecraft. At the time of launch it was the heaviest interplanetary spacecraft ever launched, weighing 6200 kg.[2]

Phobos 1

https://en.wikipedia.org/wiki/Phobos_1

BLACK HILLS
Information Security

WIRED

MATT BURGESS SECURITY JUL 28, 2023 7:00 AM

Satellites Are Rife With Basic Security Flaws

German researchers gained rare access to three satellites and found that they're years behind normal cybersecurity standards.

Vulnerabilities/Threats | 1 MIN READ | QUICK HITS

Satellite Networks Worldwide at Risk of Possible Cyberattacks, FBI & CISA Warn

Agencies provide mitigation steps to protect satellite communication (SATCOM) networks amid "current geopolitical situation."

Dark Reading Staff
Dark Reading
March 18, 2022

How Hackers Can Hijack a Satellite

We rely on them for communications, military activity, and everyday tasks. How long before attackers really start to look up at the stars?

Nate Nelson
Contributing Writer, Dark Reading
July 14, 2023

telnikov via Alamy Stock Photo

flying hundreds or even thousands of
n the sky, at a speed of tens of thousands
's an hour, is nonetheless still a
nd every connected computer has an

ments

DARKREADING

Attacks/Breaches | 2 MIN READ | QUICK HITS

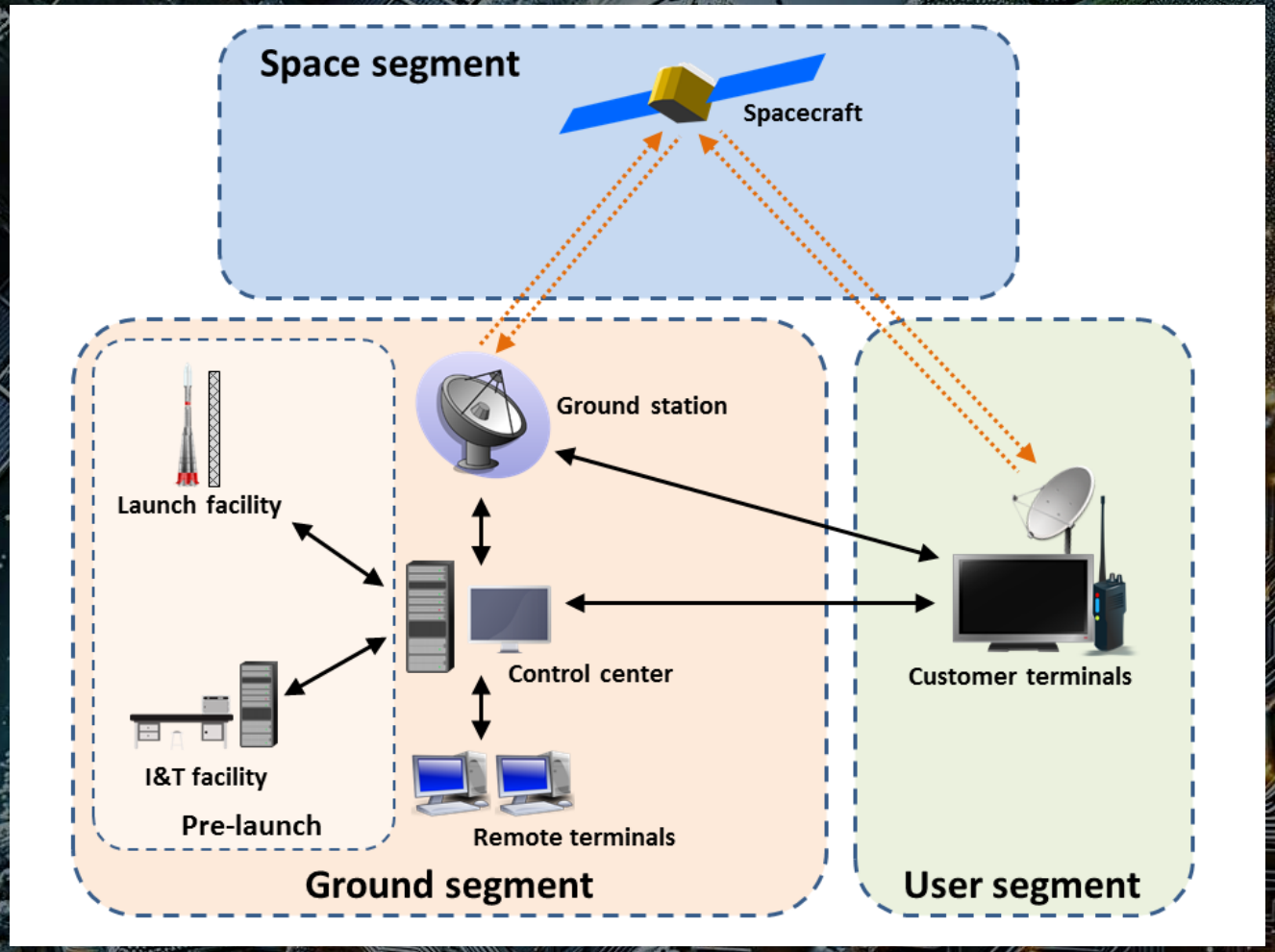
Russian Satellite Internet Downed via Attackers Claiming Ties to Wagner Group

Attribution for the cyberattack on Dozor-Teleport remains murky, but the effects are real — downed communications and compromised data.

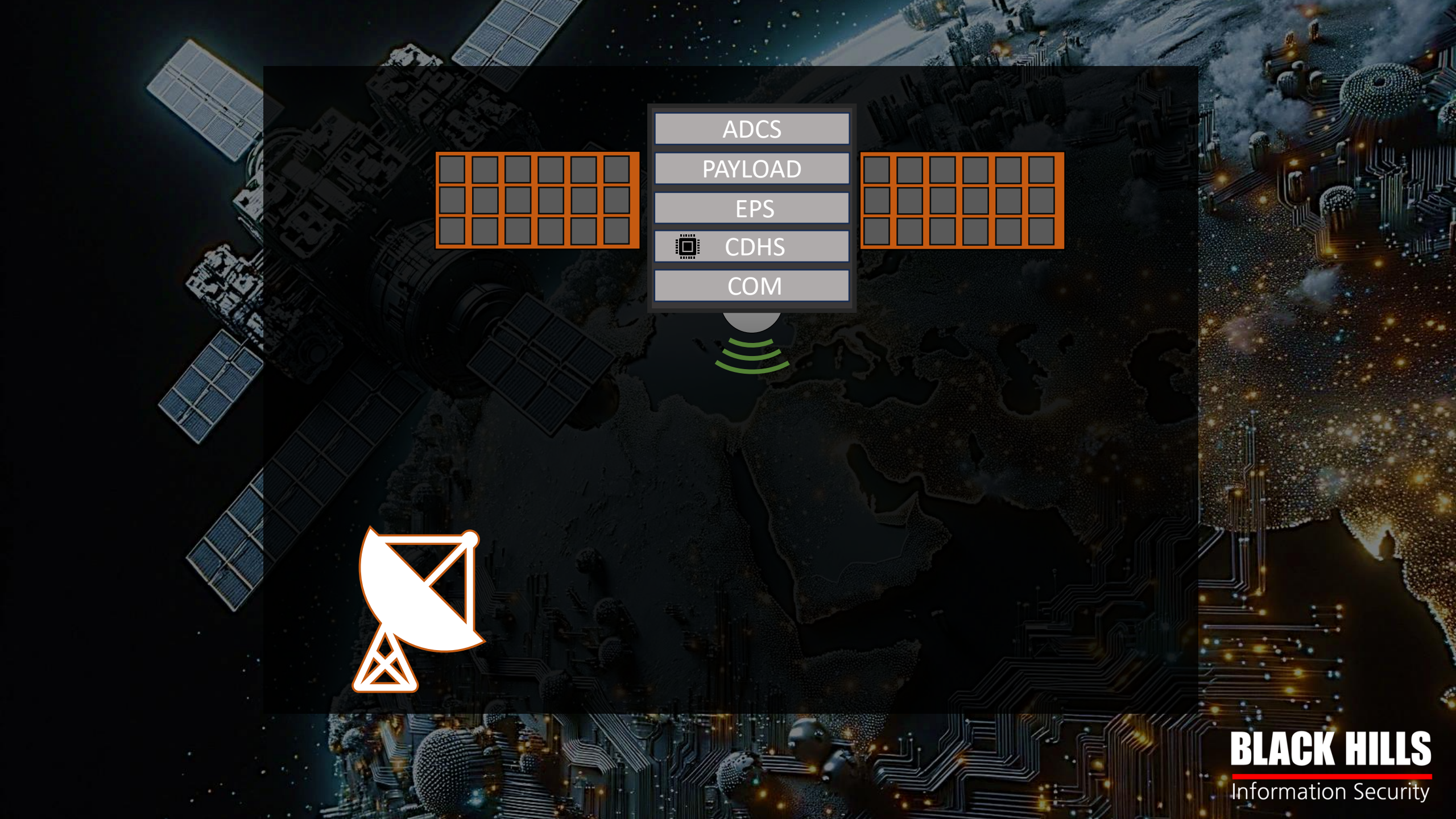
Dark Reading Staff
Dark Reading
July 03, 2023

BLACK HILLS
Information Security

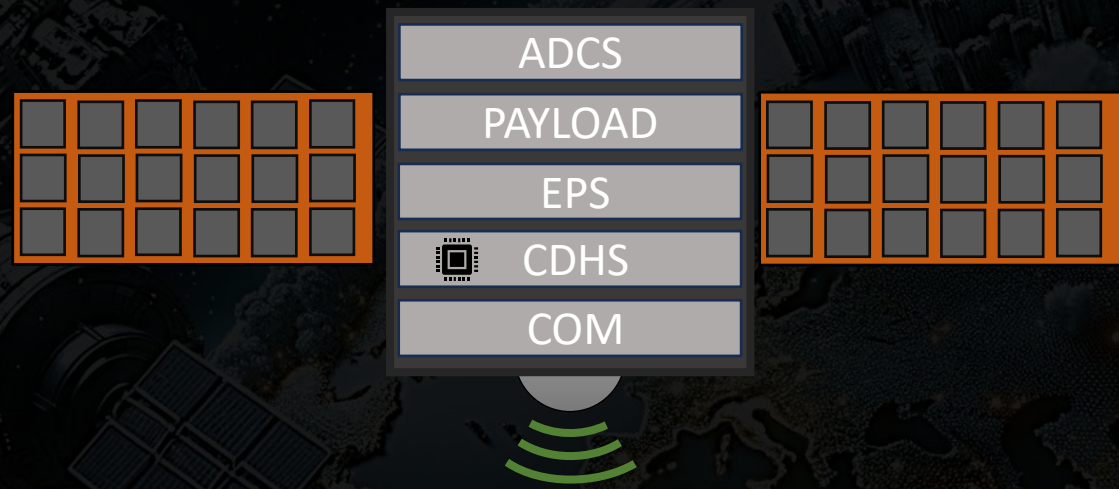
SPACE SYSTEM



BLACK HILLS
Information Security

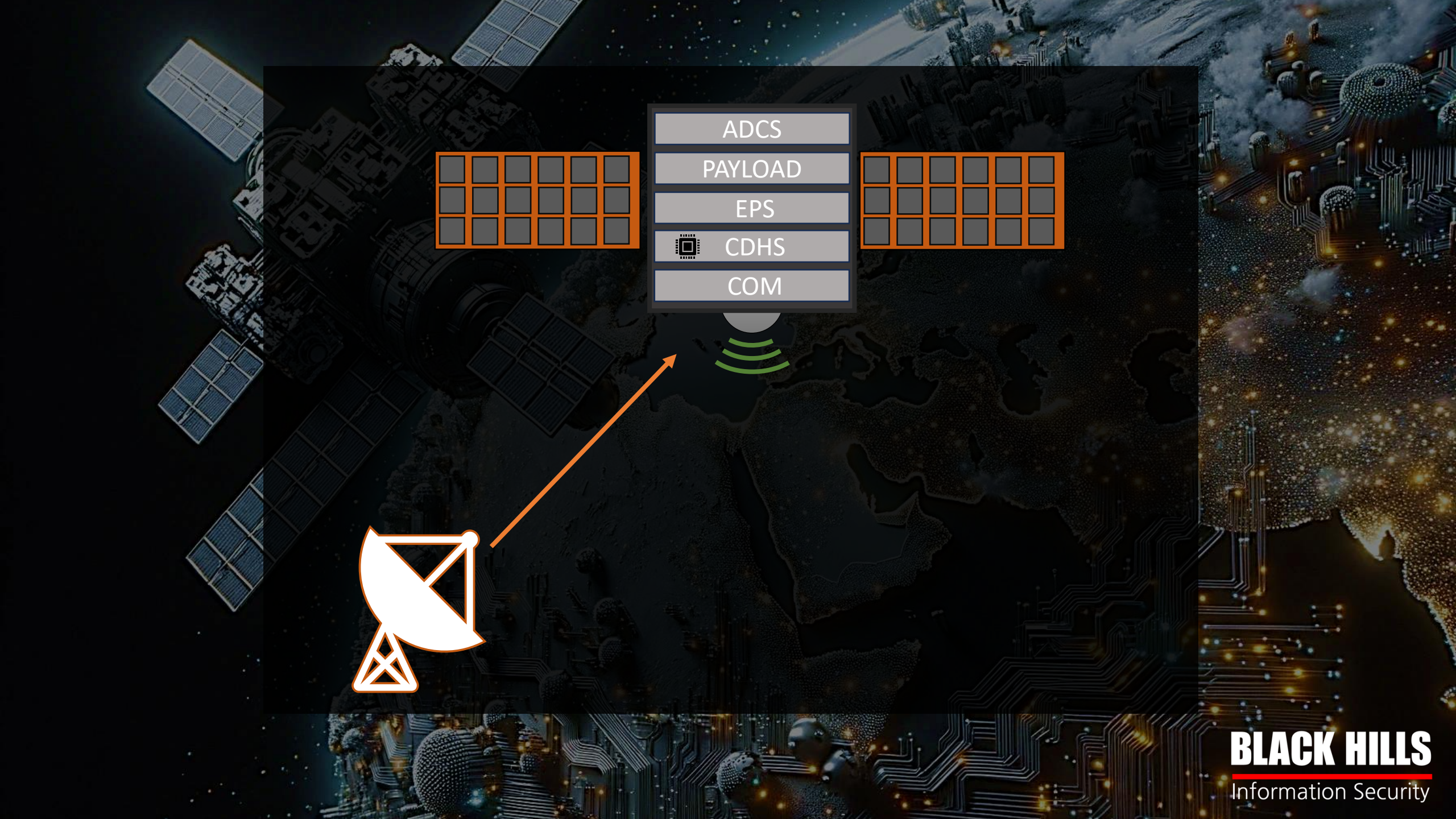


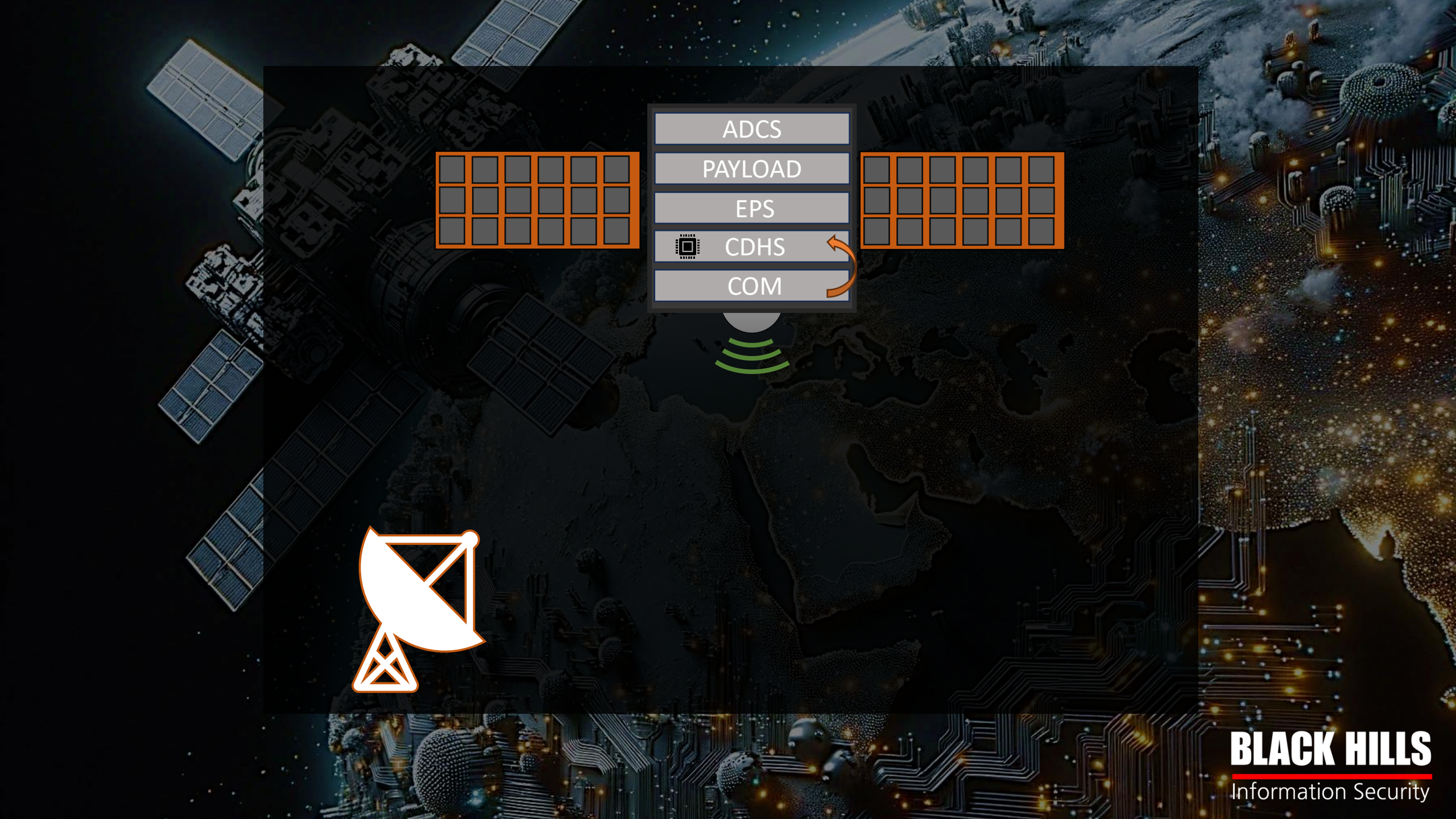
BLACK HILLS
Information Security



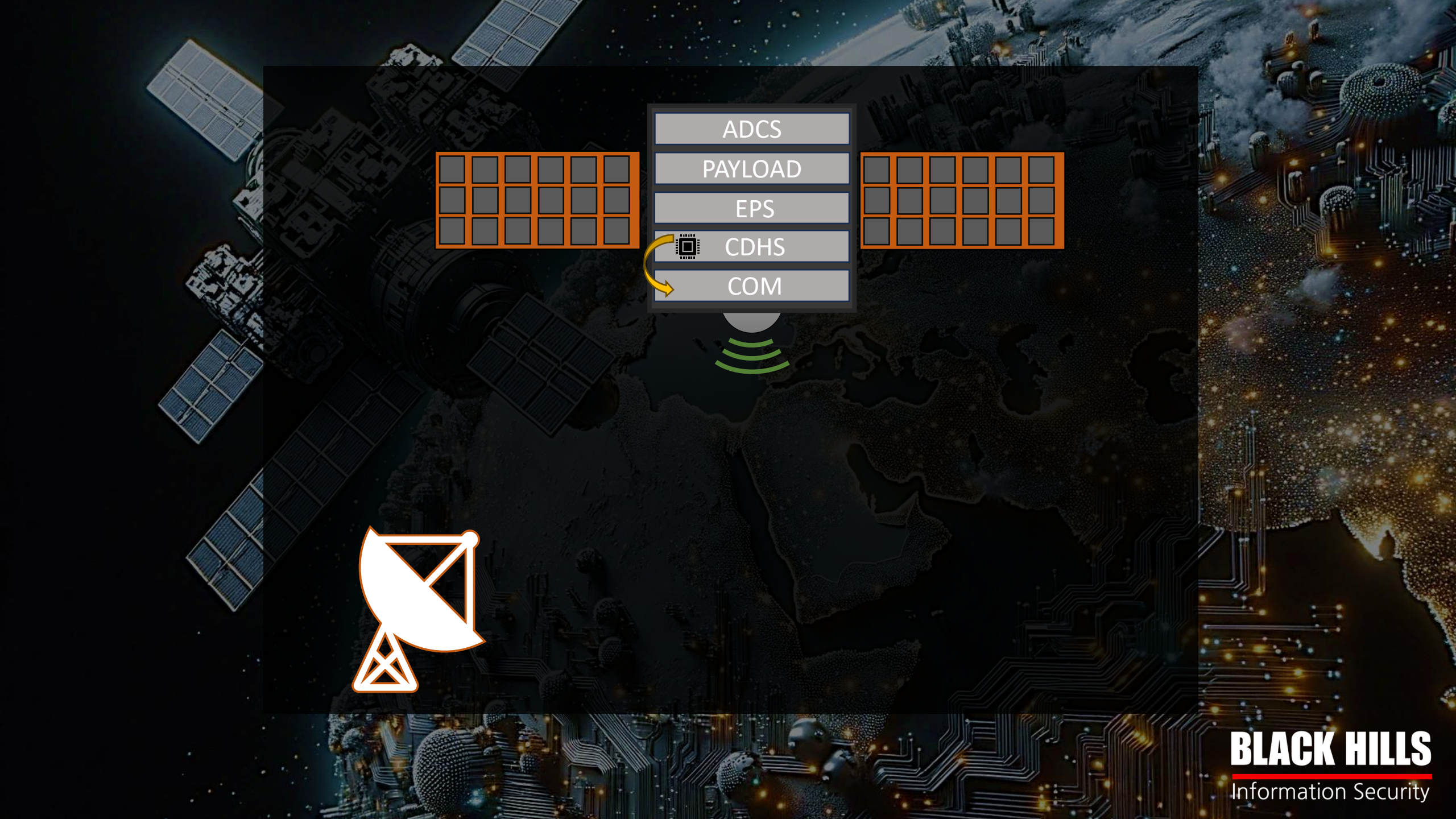
ADCS – Attitude Determination & Control System
PAYLOAD - <insert mission here>
EPS – Electrical Power System
CDHS – Command & Data Handling System
COM - Communications

BLACK HILLS
Information Security

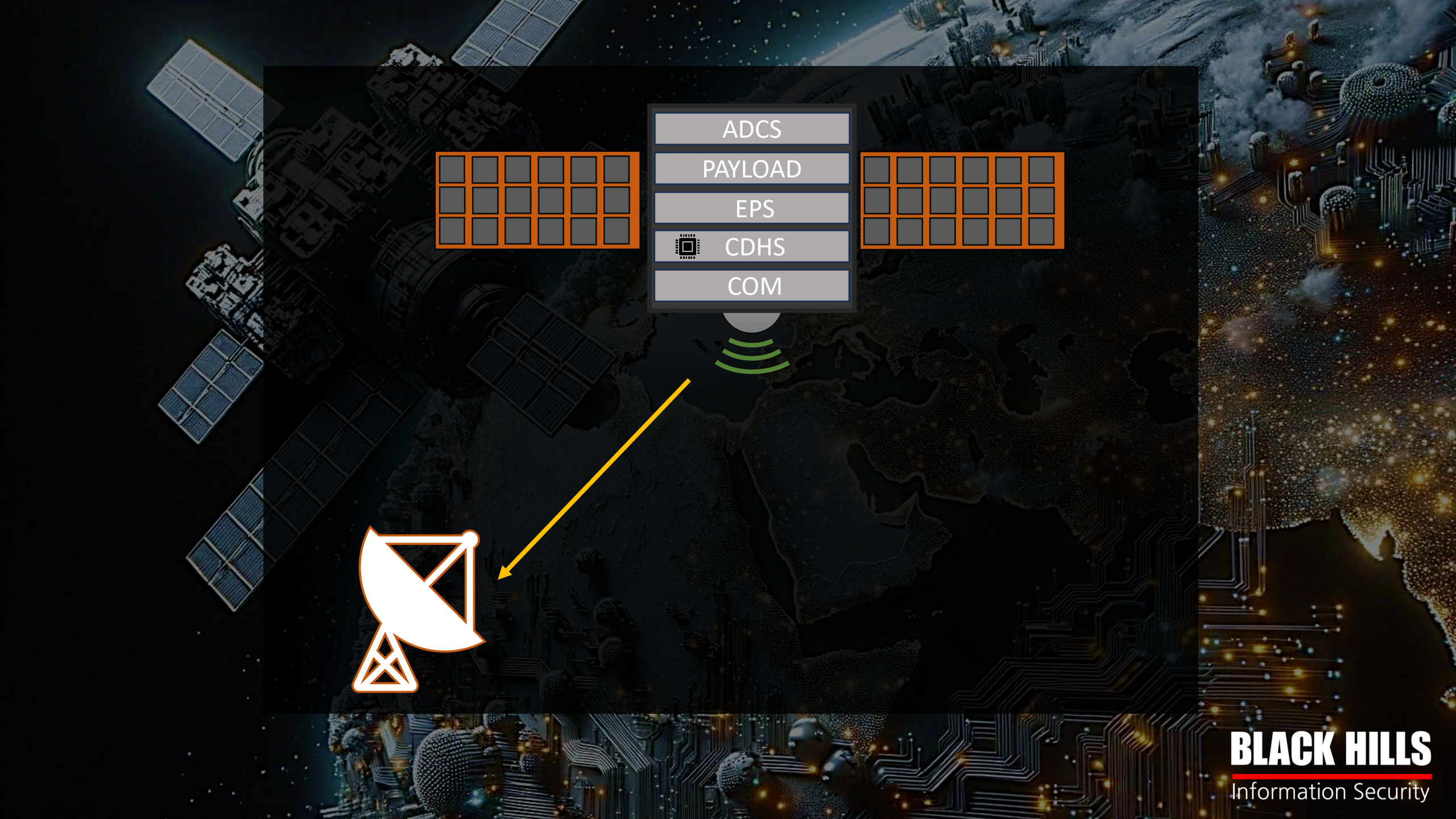


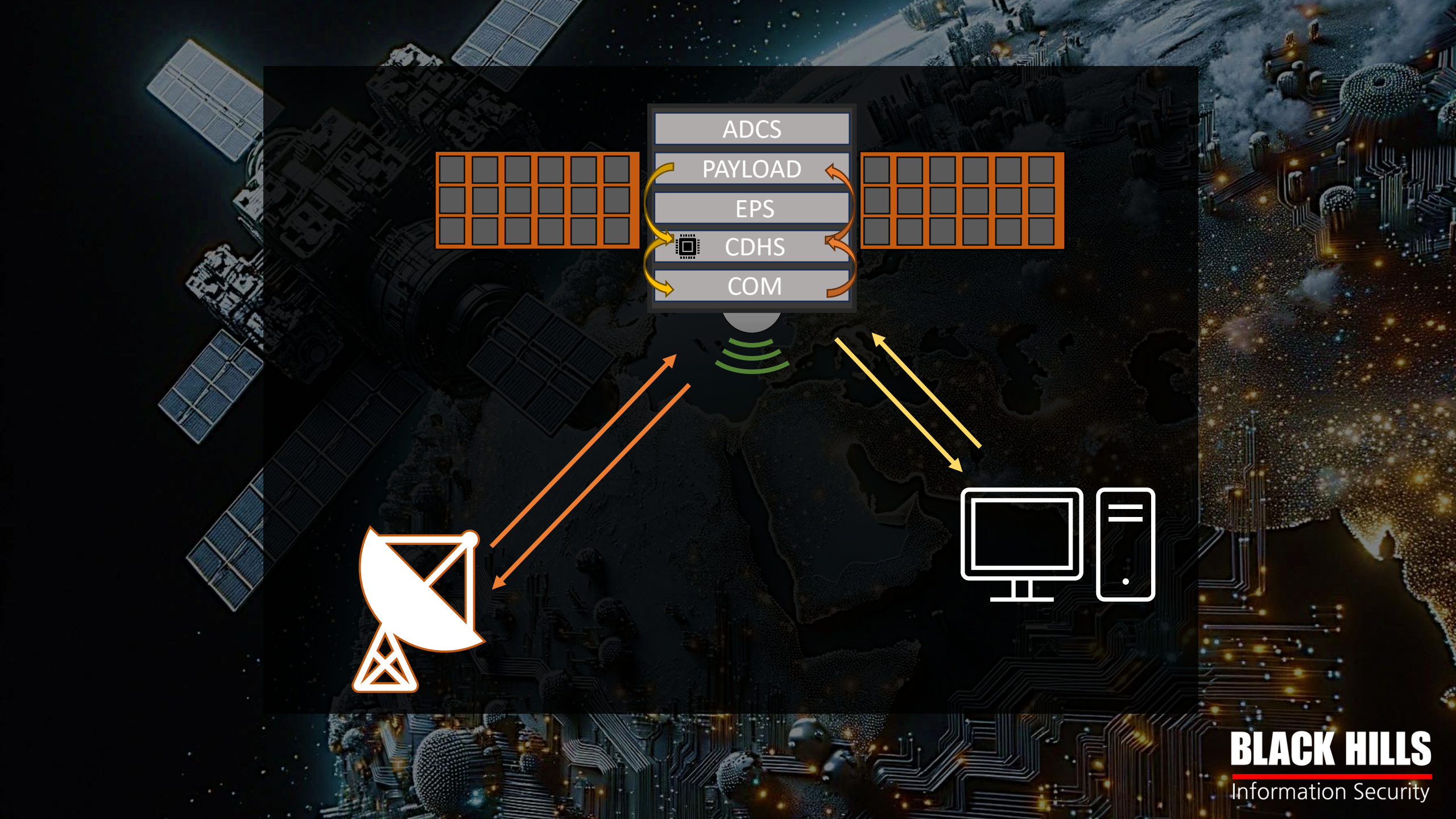


BLACK HILLS
Information Security



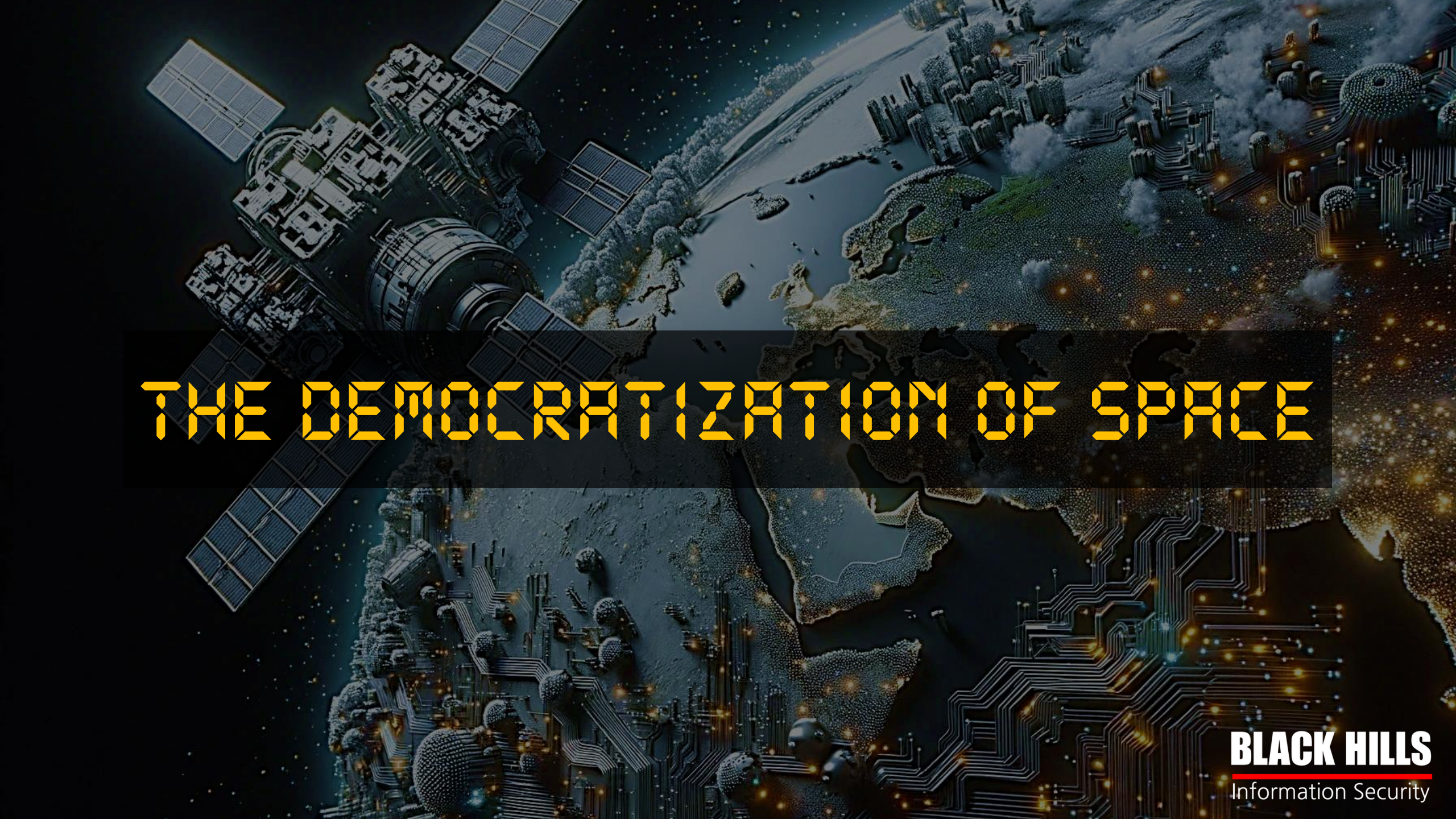
BLACK HILLS
Information Security





THE CONSTRAINTS

- Technical
- Economical
- Orbital
- Operational
- Regulatory
- Environmental
- Reliability & Redundancy
- Launch
- End-of-Life
- Security


THE DEMOCRATIZATION OF SPACE
BLACK HILLS
Information Security

https://eos.com/wp-content/uploads/2022/10/three-earth-orbits.jpg.webp

BLACK HILLS
Information Security

BLACK HILLS
Information Security

A NEW PLAYER ENTERS...

hackaday.com

DEMOCRATIZING SPACE, ONE PICOSATELLITE AT A TIME

June 28, 2023 by Tom Nardi 50 Comments

There was a time when putting an object into low Earth orbit was the absolute pinnacle of human achievement. It was such an outrageously expensive and complex undertaking that only a world superpower was capable of it, and even then, success wasn't guaranteed. As the unforgiving physics involved are a constant, and the number of entities that could build space-capable vehicles remained low, this situation remained largely the same for the remainder of the 20th century.

Want to pwn a satellite? Turns out it's surprisingly easy

PhD student admits he probably shouldn't have given this talk

Iain Thomson

Fri 11 Aug 2023 // 13:01 UTC

BLACK HAT A study into the feasibility of hacking low-Earth orbit satellites has revealed that it's worryingly easy to do.

In a presentation at the Black Hat security conference in Las Vegas, Johannes Willbold, a PhD student at Germany's Ruhr University Bochum, explained he had been investigating the security of satellites. He studied three types of orbital machinery and found that many were utterly defenseless against remote takeover because they lack the most basic security systems.

"People think that satellites are secure," he said. "Those are expensive assets and they should have encryption and authentication. I assume that criminals think the same and they are too hard to target and you need to be some kind of cryptography genius. Maybe it wasn't a good idea to give this talk."

Satellite operators have been lucky so far. The prevailing wisdom is that hacking this kit would be prohibitively expensive due to the high cost of ground stations that communicate with the orbital birds, and that such hardware benefited from security by obscurity – that getting hold of the details of the firmware would be too difficult. Neither is true, the research indicates.

> **Those are expensive assets and they should have encryption and authentication. I assume that criminals think the same and they are too hard to target**

For example, both AWS and Microsoft's Azure now offer Ground Station as a Service (GSaaS) to communicate with LEO satellites, so communication is simply a matter of plonking down a credit card. As for getting details on firmware, the commercial space industry has flourished in recent years and many of the components used on multiple platforms are easy to buy and study – Willbold estimated a hacker could build their own ground station for around $10,000 in parts.

Low priority

Intrigued by the results, Willbold decided to dig deeper. He contacted developers working on sat systems to check the data, and got nine responses from devs who worked on a total of 132 satellites over their careers. This wasn't easy – it took four months to garner those responses.

The results showed that security systems were way down on the list of priorities when it comes to satellite design. Only two of the respondents had tried any kind of penetration testing. The problem, he opined, was that space science is such a rarefied field that the developers just didn't have the security skills to do a rigorous shakedown of a satellite in the first place.

One surprising result was that the larger the satellite (and thus more expensive to build and launch), the more vulnerable it was. Larger machinery typically used more commercial off-the-shelf components and was thus more vulnerable since the code base was public, whereas smaller CubeSats tended to use custom code.

https://www.theregister.com/2023/08/11/satellite_hacking_black_hat/

BLACK HILLS
Information Security

GROUND STATION THREATS

Most Vulnerable Segment in a Space System

- Direct Network Attack
- Software Vulnerabilities
- Jamming of Signals
- Physical Attacks

BLACK HILLS
Information Security

COMM LINK THREATS

- Uplink/Downlink Jamming
- Spoofing
- Replay Attacks
- Weak or No encryption (Fallback)
- Jamming of Signals
- Weather if using optical based Comms

BLACK HILLS
Information Security

SPACECRAFT THREATS/CHALLENGES

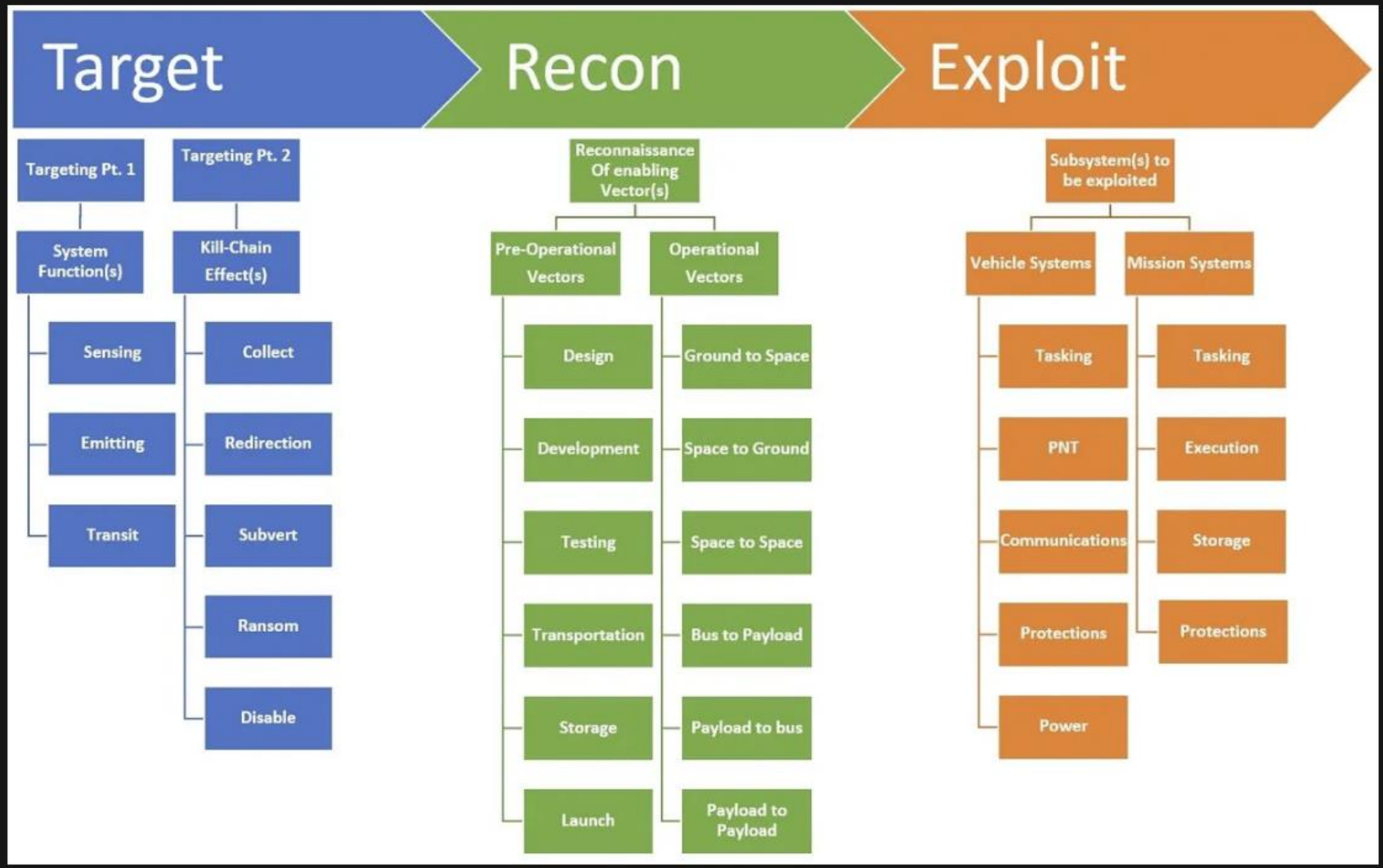
- Space Debris
- Resource Based Constraints Abuses (DoS)
- Software Vulnerabilities
- Kinetic Weapons
- Environmental
  - Radiation
  - Temperature
  - Gravity
- Redundancy
- Supply Chain

BLACK HILLS
Information Security

BLACK HILLS
Information Security


ATT&CK®
TREKS
SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS
SPACE-SHIELD
BLACK HILLS
Information Security

The Framework



BLACK HILLS
Information Security

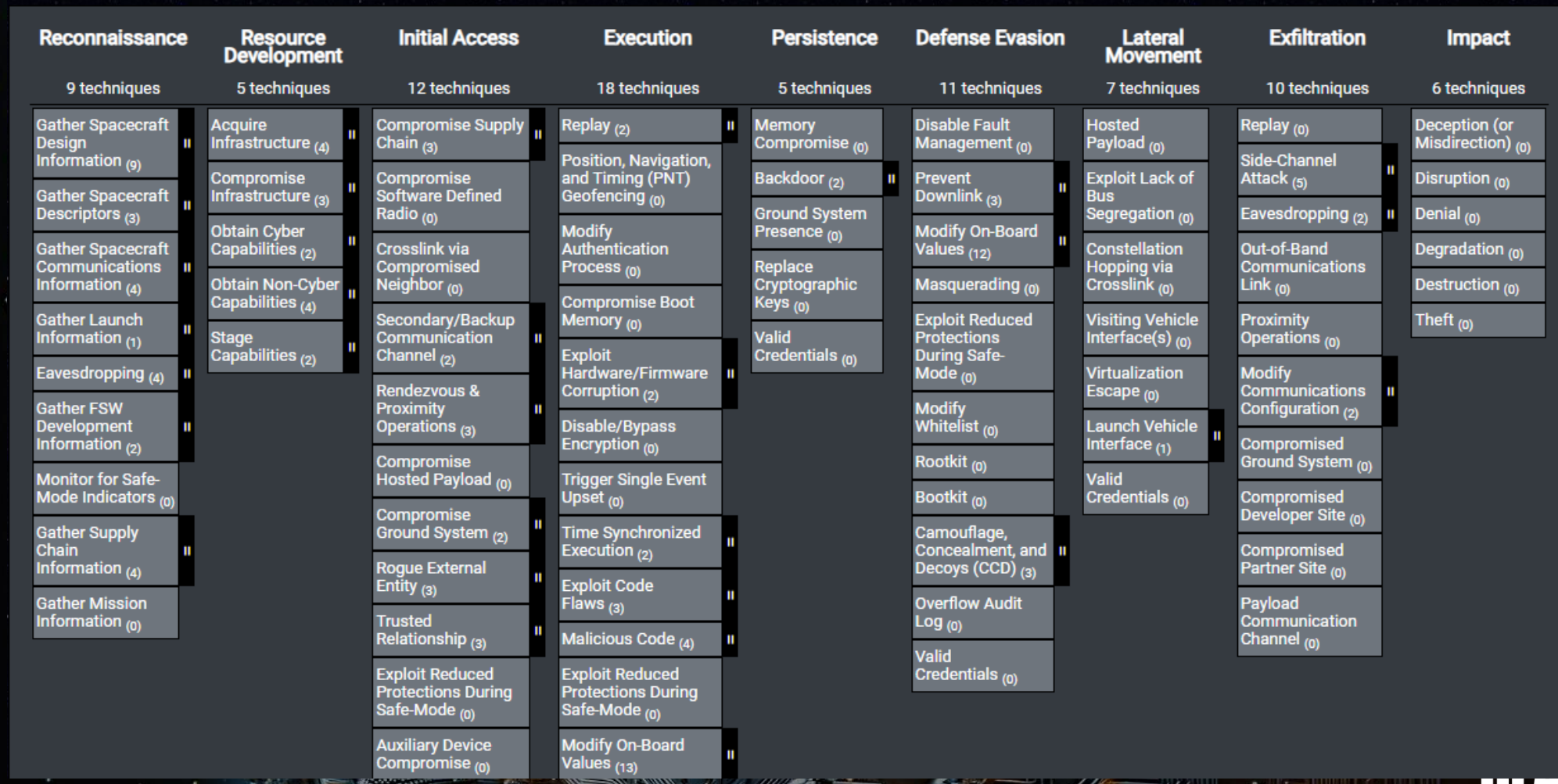
Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD)

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
6 techniques	4 techniques	5 techniques	3 techniques	4 techniques	2 techniques	4 techniques	4 techniques	4 techniques	4 techniques	2 techniques
Active Scanning (RF/Optical) (4)	Acquire or Build Infrastructure (4)	Direct Attack to Space Communication Links (2)	Modification of On Board Control Procedures modification	Backdoor Installation (5)	Become Avionics Bus Master	Impair Defenses (1)	Adversary in the Middle (1)	Key Management Policy Discovery	Compromise a Payload after compromising the main satellite platform	Adversary in the Middle (2)
Gather Victim Mission Information (3)	Compromise Account (1)	Ground Segment Compromise (2)	Native API	Key Management Infrastructure Manipulation (2)	Escape to Host (1)	Indicator Removal on Host (1)	Brute Force (1)	Spacecraft's Components Discovery	Compromise of another partition in Time and Space Partitioning OS or other types of satellite hypervisors	Data from link eavesdropping (3)
Gather Victim Org Information (3)	Compromise Infrastructure (2)	Supply Chain Compromise (3)	Payload Exploitation to Execute Commands	Pre-OS Boot (1)		Masquerading	Communication Link Sniffing (1)	System Service Discovery	Compromise the satellite platform starting from a compromised payload	
In orbit proximity intelligence (6)	Develop/Obtain Capabilities (9)	Trusted Relationship (3)		Valid Credentials (3)		Pre-Os Boot (1)	Retrieve TT&C master/session keys (3)	Trust Relationships Discovery	Lateral Movement via common Avionics Bus	
Passive Interception (RF/Optical) (4)		Valid Credentials (3)								
Phishing for Information (2)										

Space Attack Research & Tactic Analysis (SPARTA)

show sub-techniques | hide sub-techniques



Cyber | Etats-Unis | Europe | Hacking | Russie | Satellite

An analysis of the Viasat cyber attack with the MITRE ATT&CK® framework

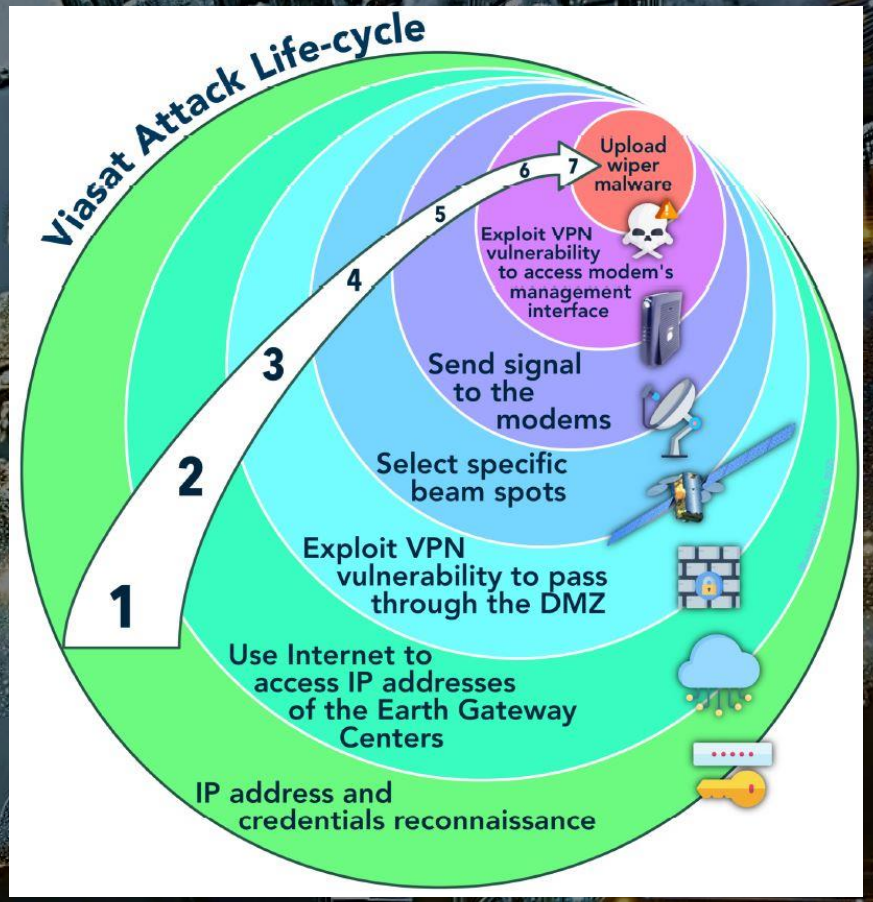
Par **François Quiquet** - 10 octobre 2023

In this article, we will go through the Viasat cyber attack that occured on 24 February, 2022. The goal is to do a modelisation of this attack based on the MITRE ATT&CK framework.

The first question will be to explain why to use the MITRE ATT&CK framework to do this analysis while there are others frameworks and methodologies that can be used for the space sector

The next work will be to identify Tactics, Techniques and Procedures (TTPs) from the MITRE ATT&CK matrix that have been used by the hackers during the Viasat attack. To learn more about the MITRE ATT&CK framework, you can go to this article about the ATT&Ck v13 release.

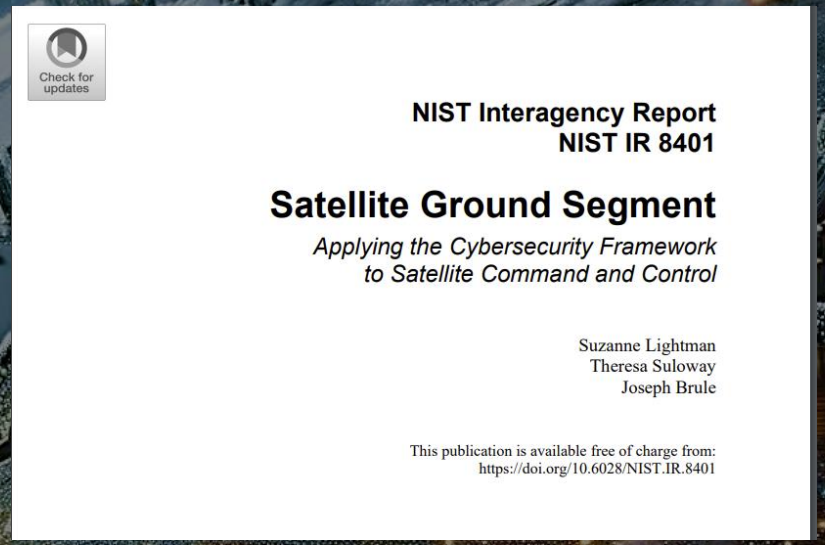
Once TTP identified, we will map the TTPs on the ATT&CK Navigator in order to have the complete attack chain as a cyber kill chain.



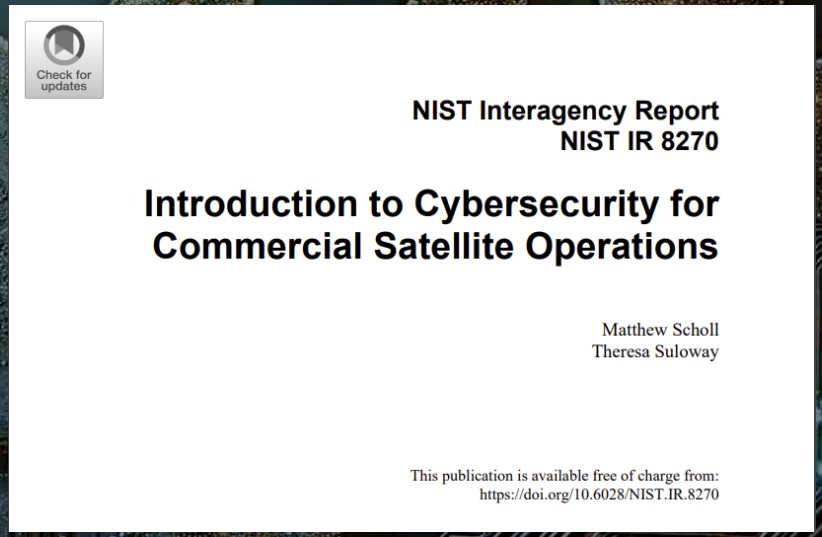
https://www.spacesecurity.info/an-analysis-of-the-viasat-cyber-attack-with-the-mitre-attck-framework/

BLACK HILLS
Information Security

https://public.ccsds.org/Pubs/350x1g3.pdf

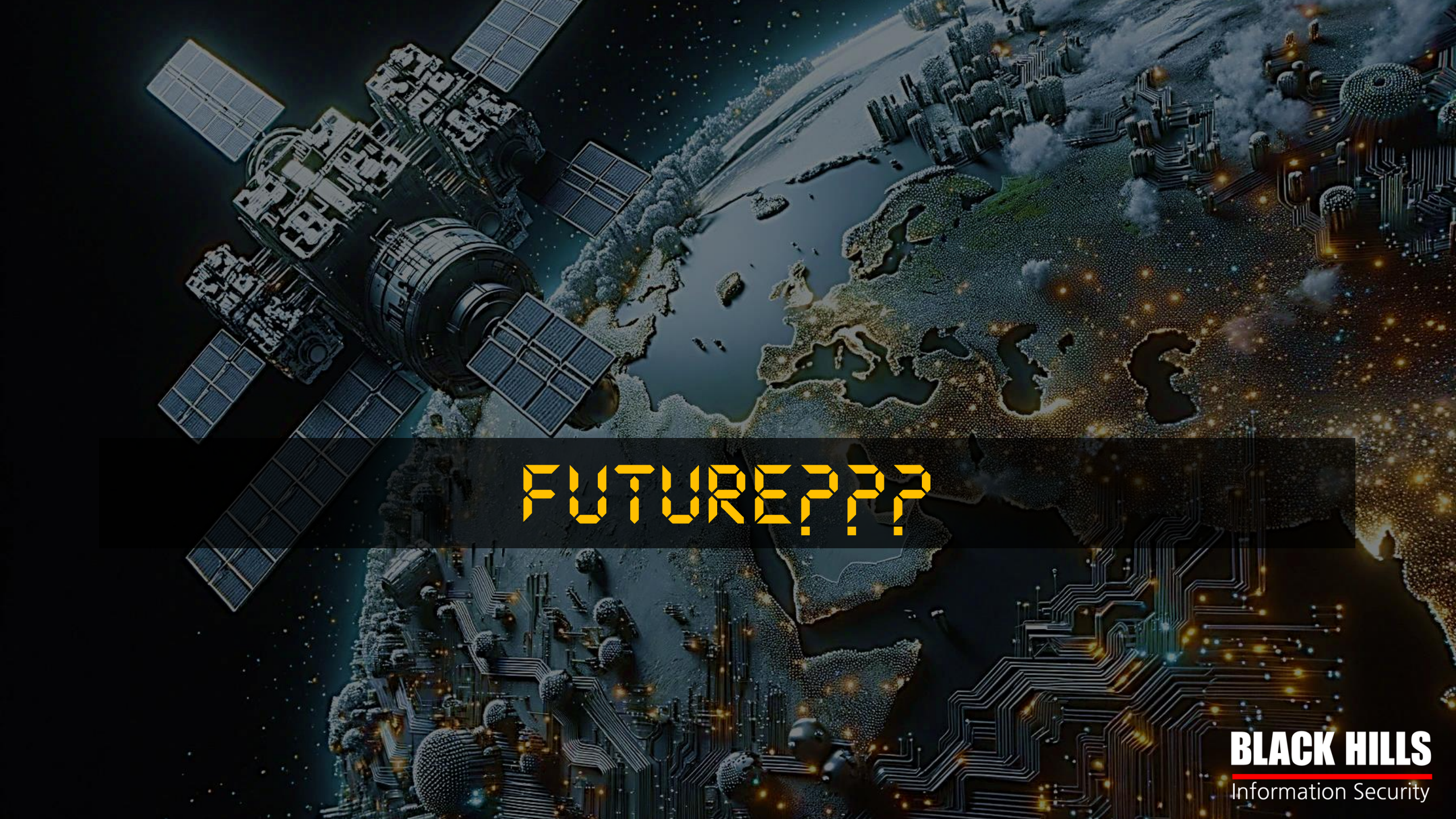


https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf



https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf

BLACK HILLS
Information Security



BLACK HILLS
Information Security

WANT TO PLAY THE GAME?

SatNOGS

OPEN SAT KIT

NASA cFS core Flight System

TINY GS

OPENC3

nos3 NASA Operational Simulator for Small Satellites

BLACK HILLS Information Security

World's first Raspberry Pi-powered CubeSat celebrates record-making orbit

22nd Jun 2022 Ashley Whittaker 9 comments

Mission complete! The NASA-sponsored GASPACS (Get Away Special Passive Attitude Control Satellite) CubeSat deorbited last month, following a record-making 117 days in space.

The team visiting the Kennedy Space Center Visitor Center

We've previously blogged about GASPACS, so have a quick read to learn how a Utah State University team made it, and what its unique AeroBoom self-stabilising design is all about. It was excellent hearing from the team again to tell us how successful the flight had been.

BLACK HILLS
Information Security

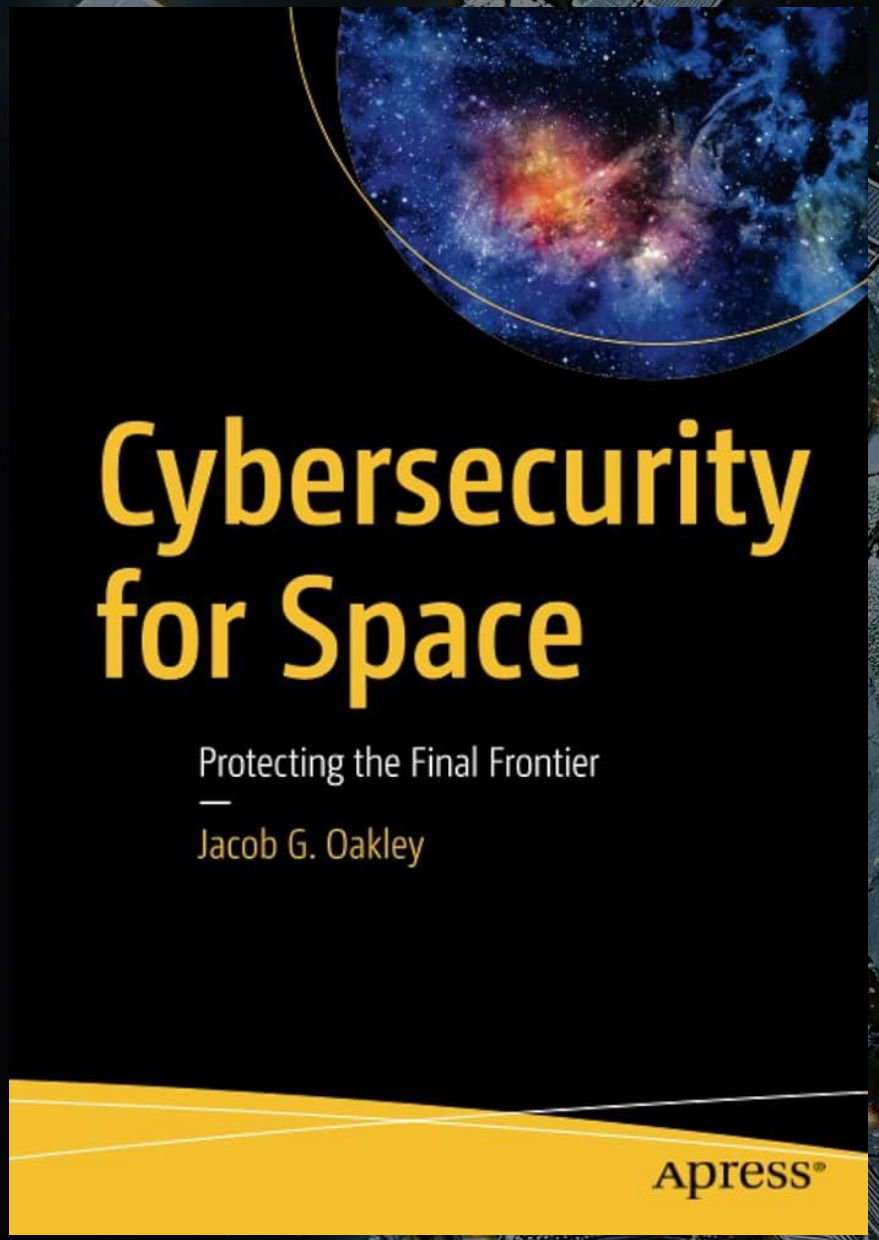
Mission status [edit]

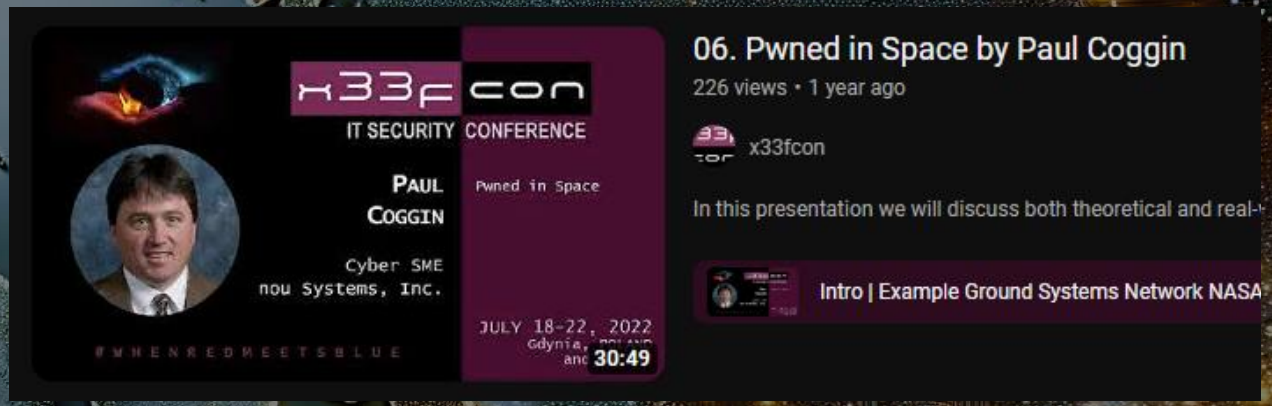
The North American Aerospace Defense Command designated GASPACS as NORAD ID 51439.[35]

Three days after deployment, on January 29, 2022, GASPACS faced a major setback when power was lost on the Y-channel. This caused a significant reduction in the available power. GASPACS entered a perpetual charge cycle, charging up for approximately six hours on its remaining solar panels before reaching the power required to turn back on. Once booted up, GASPACS would stay powered on for approximately an hour before shutting off due to low power, and repeating the cycle. This continuous power cycle greatly reduced the quantity of data GASPACS was able to transmit to Earth.[6]

On May 6, 2022, loss of the Z-channel was confirmed. This once again drastically reduced GASPACS's available power. Despite this, GASPACS continued to power on when possible, and ground operators were able to receive several packets of telemetry data, photo data, and AX.25 beacons.

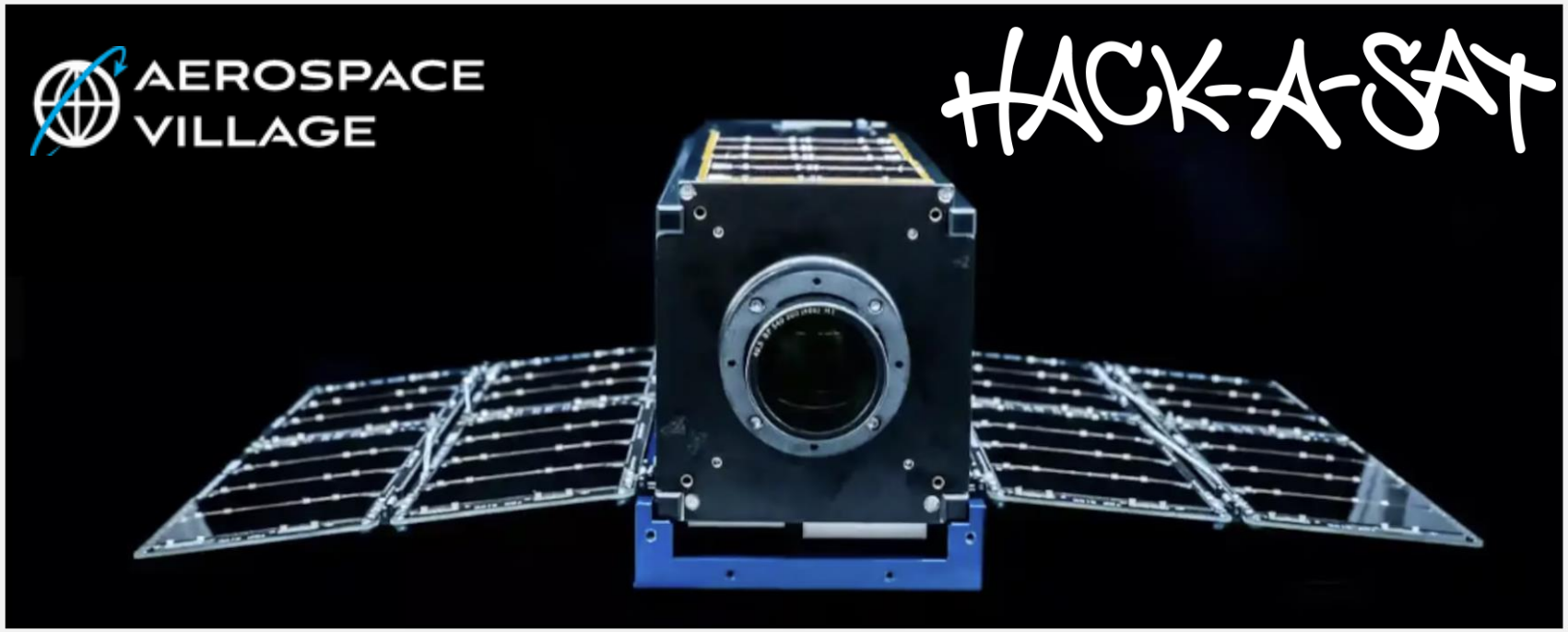
The satellite decayed from orbit on 22 May 2022.[1]





PWNED in Space – Paul Coggin
https://youtu.be/vDTSzfoJnus?si=ZTYyBdTe9J69iO3I

BLACK HILLS
Information Security



Hack-A-Sat's Moonlighter satellite deploys to low earth orbit after last month's successful launch

Published July 17, 2023

By Marc Denofio

ROME, N.Y. (AFRL) -- Moonlighter reached low earth orbit July 5 after a short visit at the International Space Station and is on track for its inaugural mission: to host an on-orbit cybersecurity challenge during Hack-A-Sat 4 finals, making it the first on-orbit Capture the Flag, or CTF, hacking competition.

Low priority

Intrigued by the results, Willbold decided to dig deeper. He contacted developers working on sat systems to check the data, and got nine responses from devs who worked on a total of 132 satellites over their careers. This wasn't easy – it took four months to garner those responses.

The results showed that security systems were way down on the list of priorities when it comes to satellite design. Only two of the respondents had tried any kind of penetration testing. The problem, he opined, was that space science is such a rarefied field that the developers just didn't have the security skills to do a rigorous shakedown of a satellite in the first place.

One surprising result was that the larger the satellite (and thus more expensive to build and launch), the more vulnerable it was. Larger machinery typically used more commercial off-the-shelf components and was thus more vulnerable since the code base was public, whereas smaller CubeSats tended to use custom code.

BLACK HILLS
Information Security