Cyber Threats to Space Operations

Dr. Josh Sipper
Professor of Cyberwarfare Studies
Air Command and Staff College

Biographical Sketch

Dr. Joshua Alton Sipper is an Assistant Professor of Cyberwarfare Studies at the US Air Force Air Command and Staff College (ACSC). He has over 25 years of experience in intelligence, surveillance, and reconnaissance (ISR), electromagnetic warfare (EW), and cyber operations. Dr. Sipper teaches Airpower Operations and Strategy and Contemporary Warfare in the Airpower Department at ACSC and is the co-director of the Cyberspace Specialization, teaching ISR and Cyberspace and Cyber and Electromagnetic Warfare. Dr. Sipper has been featured as a keynote speaker at numerous conferences and on the Newt’s World podcast (official podcast of Former Speaker Newt Gingrich). Dr. Sipper is the author of numerous articles and book chapters concerning cyber operations, ISR, and EW. He also is the author of several books including his most recent title, The Cyber Meta-reality: Beyond the Metaverse. Dr. Sipper is a fellow with the International Academy, Research, and Industry Association (IARIA) and a lifetime member of the Military Cyber Professionals Association (MCPA) and the Association of Old Crows (AOC).

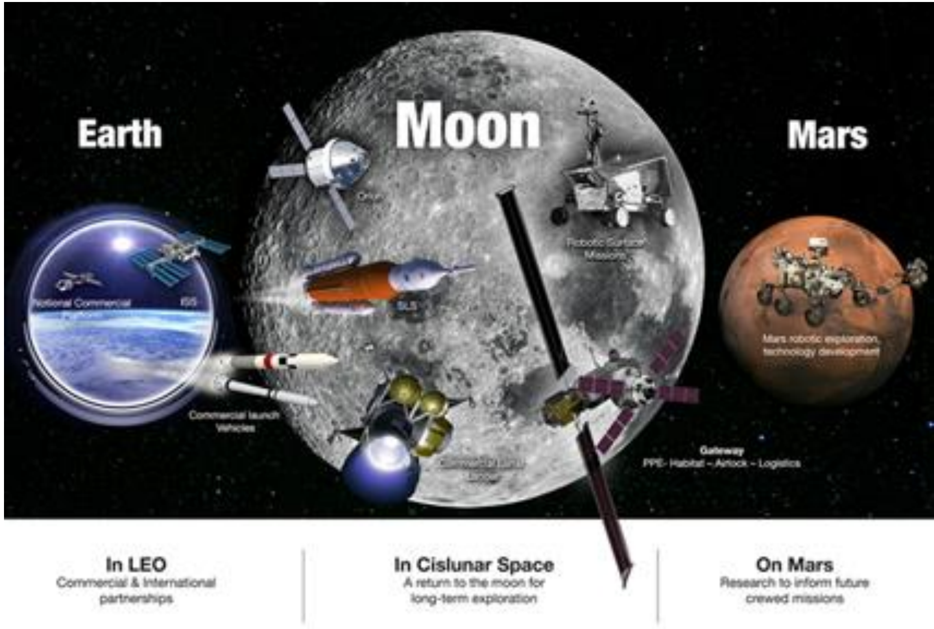
IARIA

Cyber and Space

- Cyber and Space Operational Dependencies
- Threats - Malware and Hacking
- Electromagnetic Warfare
- Emergent Tech
- Conclusion

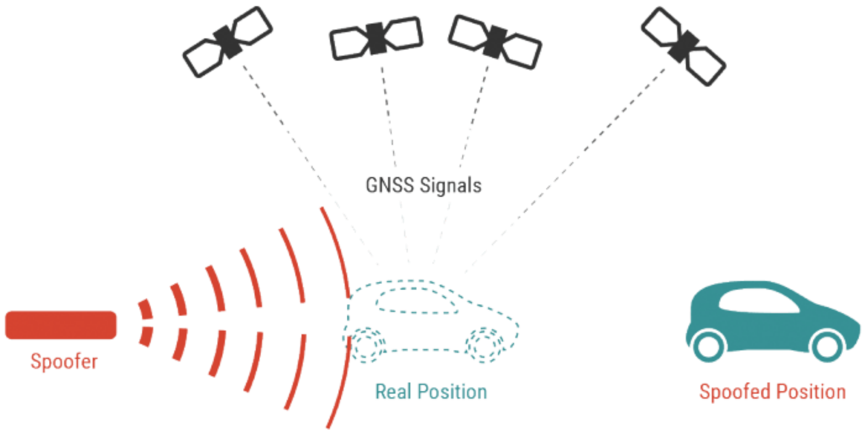
Cyber and Space Operational Dependencies

- Space does not work without cyber and to a great extent, vice versa
- Protecting space assets through cyber
- Space could become the primary cyber pathway with emergent tech advances


Earth
Moon
Mars
Orion
Robotic Surface Missions
National Commercial
ISS
SLS
Mars robotic exploration, technology development
Commercial launch Vehicles
Gateway
PPE- Habitat – Airlock – Logistics
In LEO
Commercial & International partnerships
In Cislunar Space
A return to the moon for long-term exploration
On Mars
Research to inform future crewed missions

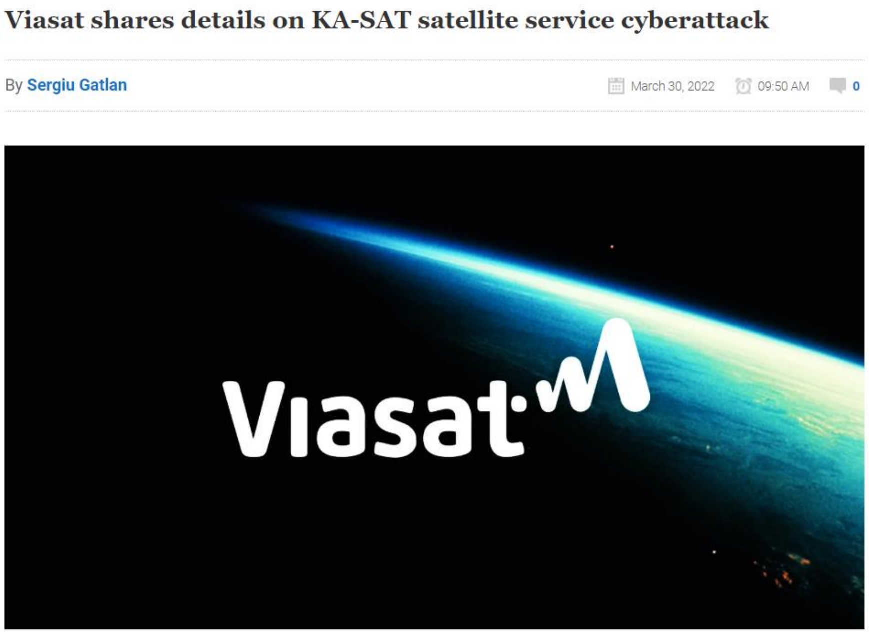
Cyber and Space Operational Dependencies

- Dependence of air, land, and sea operations on cyber and space situational awareness, navigation, and C4ISR carries with it myriad opportunities for mission failure
- GPS jamming/spoofing just one example of how dependent our forces are on space/cyber capabilities



Cyber and Space Operational Dependencies

- US satellite communications provider Viasat experienced a cyberattack that affected its KA-SAT satellite broadband service on February 24, the day Russia invaded Ukraine
- Used extensively by Ukraine military
- Breached the management network and issued management commands to overwrite the devices' flash memory, rendering them unable to reconnect to the network but not bricking them altogether
- Ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access
- US government is now investigating the Viasat hack as a potential Russian state-sponsored cyberattack
- CISA and the FBI also published a joint advisory warning US organizations of "possible threats" to satellite communication (SATCOM) networks in the US and worldwide

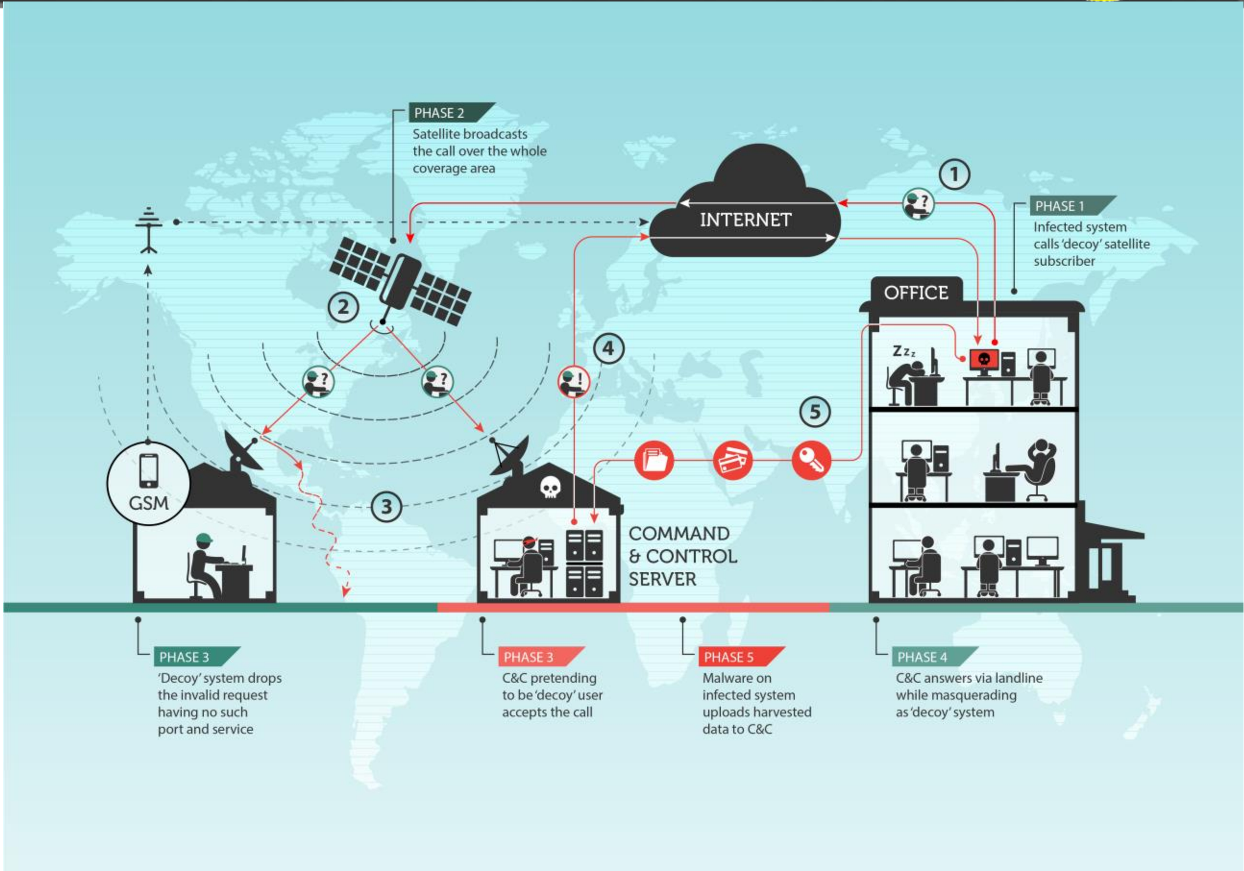


Viasat shares details on KA-SAT satellite service cyberattack

By Sergiu Gatlan March 30, 2022 09:50 AM 0

Threats - Malware and Hacking

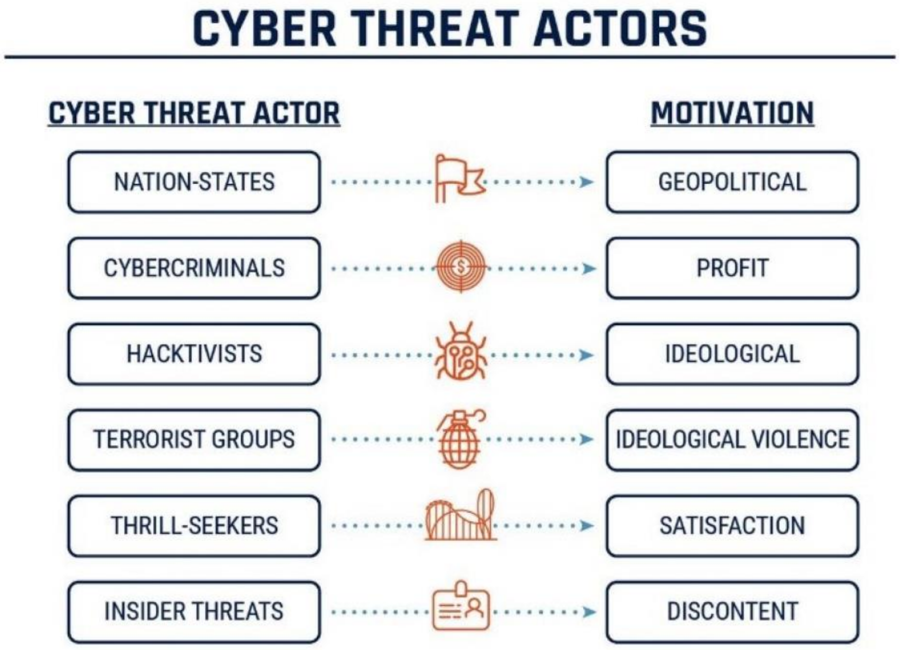
- Viruses
- Worms
- Trojans
- DDoS
- XSS
- SQL Inject
- Ransomware
- SDR and EMS
- Etc.



PHASE 2
Satellite broadcasts the call over the whole coverage area
1
PHASE 1
Infected system calls 'decoy' satellite subscriber
INTERNET
OFFICE
2
4
5
3
GSM
Zzz
COMMAND & CONTROL SERVER
PHASE 3
'Decoy' system drops the invalid request having no such port and service
PHASE 3
C&C pretending to be 'decoy' user accepts the call
PHASE 5
Malware on infected system uploads harvested data to C&C
PHASE 4
C&C answers via landline while masquerading as 'decoy' system

Threats - Malware and Hacking

- Technology can be lost in microseconds through cyber espionage, giving rogue nations the ability to catch up without the time or investment devoted by first movers
- Cyber has a "low level of entry" compared to space with myriad threat actors
- However, these threat actors, through cyberspace, can pose threats in the space domain through cyber operations



CYBER THREAT ACTORS

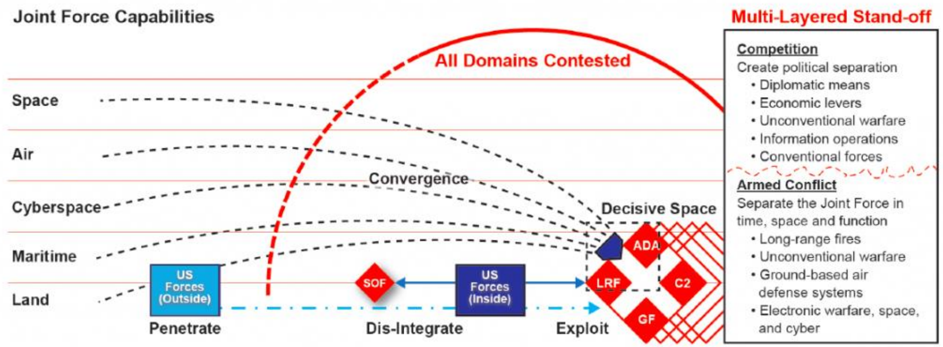
CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Threats - Malware and Hacking

- Both space and cyber also contain imbedded operational vulnerabilities special to their battlespace environs
- While space suffers the tyranny of distance, cyber suffers a tyranny of locality, both of which present different and convoluted vulnerabilities
- Space and cyber have grown rapidly, creating capabilities that make IW and JADO realities

Threats - Malware and Hacking

- Space and cyber cross-domain effects and concepts will continue to pervade every domain
- The most vital components for discussion are cross-domain platforms, hardening across technologies, and IW and JADO superiority



Joint Force Capabilities

All Domains Contested

Space

Air

Cyberspace

Maritime

Land

Convergence

Decisive Space

US Forces (Outside)

SOF

US Forces (Inside)

ADA

LRF

C2

GF

Penetrate

Dis-Integrate

Exploit

Multi-Layered Stand-off

Competition

Create political separation

- Diplomatic means
- Economic levers
- Unconventional warfare
- Information operations
- Conventional forces

Armed Conflict

Separate the Joint Force in time, space and function

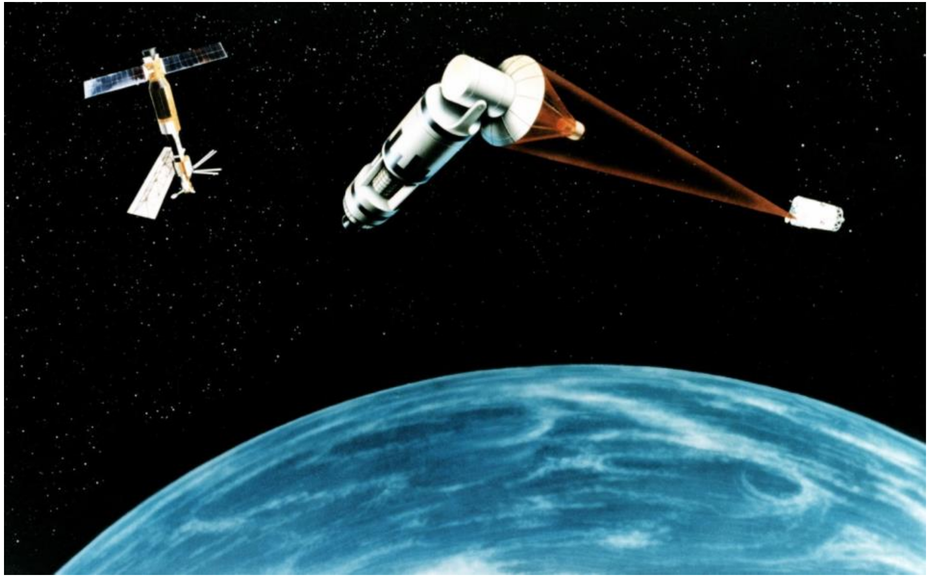
- Long-range fires
- Unconventional warfare
- Ground-based air defense systems
- Electronic warfare, space, and cyber

Electromagnetic Warfare

- Space and cyber have several technological cause and effect relationships
- Cybersecurity:
  - Supports and defends space assets
  - Provides authentication and encryption
  - Use filtering shielding and spread spectrum techniques to protect from jamming, spoofing, etc.

Electromagnetic Warfare

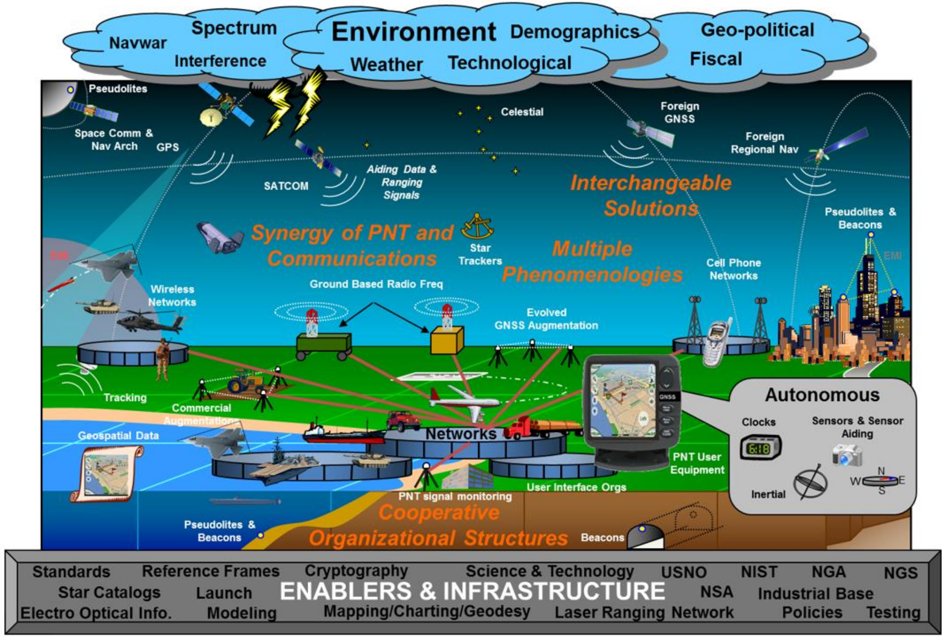
- Cyber and space domains share a similar kinetic/non-kinetic threshold
- Both space and cyber may be used consistently to degrade, deny, and deceive adversaries, leading to conflict below the threshold of kinetic operations
- What type of operations define the level of anti-satellite (ASAT) weapons, whether lasing or jamming are considered ASAT, for example?



Electromagnetic Warfare

- Cross-domain operations are, more often than not, supported and assured through platform integration and interoperability
  - Kinetic/traditional - close air support, ground support to naval activities, and other integral platform-dependent undertakings
  - network support to space operations and space platform network support to cyber operations
- PNT information is a critical enabler for precision-guided munitions (PGMs): aircraft missiles, naval gunnery and land-based artillery shells. Synchronous timing provided by space-based PNT services is also a vital element of many communication and information systems

National PNT Architecture

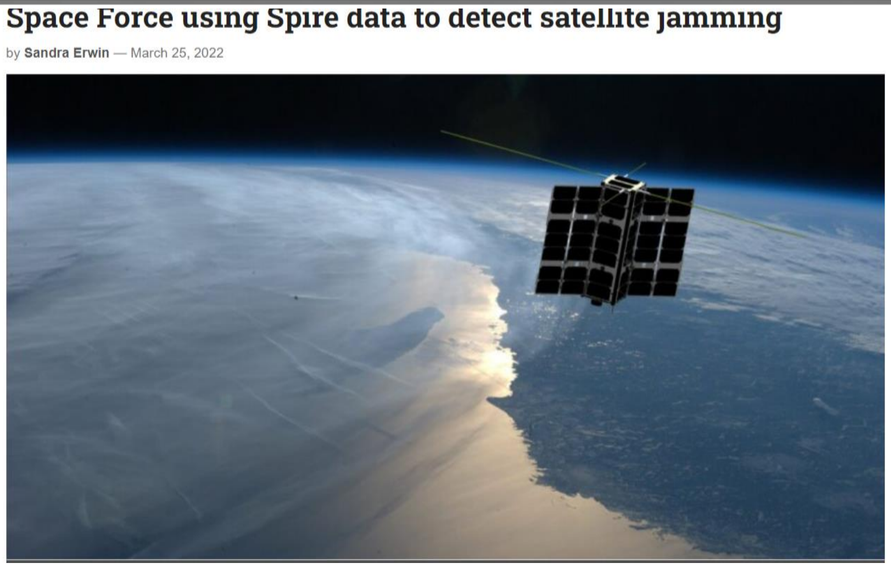


Electromagnetic Warfare

- Threats to space and cyber tend to overlap often as the technological vulnerabilities associated with electronic traffic through the electromagnetic spectrum (EMS) pervade every corner of space and cyber operations
  - jamming, spoofing and hacking attacks on communication networks via space infrastructure
  - targeting satellite control systems or mission packages
  - taking control of a satellite to exploit its capabilities
  - shut down, cook/grill solar cells through EMS exposure
  - can lead to potential global cascading effects on critical information infrastructure and networks

Electromagnetic Warfare

- Constellation of about 40 geolocation satellites operated by Spire Global is collecting data used by the U.S. Space Force to detect GPS jamming
- Issue now gaining worldwide attention due to Russia's use of electronic warfare tactics in the run-up to the invasion of Ukraine
- Spire is providing GPS telemetry data to help detect jamming to figure out way to automate manual data analysis techniques and produce more timely intelligence for military operations
- Cluster of four 6U cubesats deployed to detect and geolocate objects based on targeted RF emissions
- Data intended to help military and government organizations manage RF emissions and safeguard against RF and GPS interference



Space Force using Spire data to detect satellite jamming

by Sandra Erwin — March 25, 2022

https://spacenews.com/space-force-using-spire-data-to-detect-satellite-jamming/

Emergent Tech

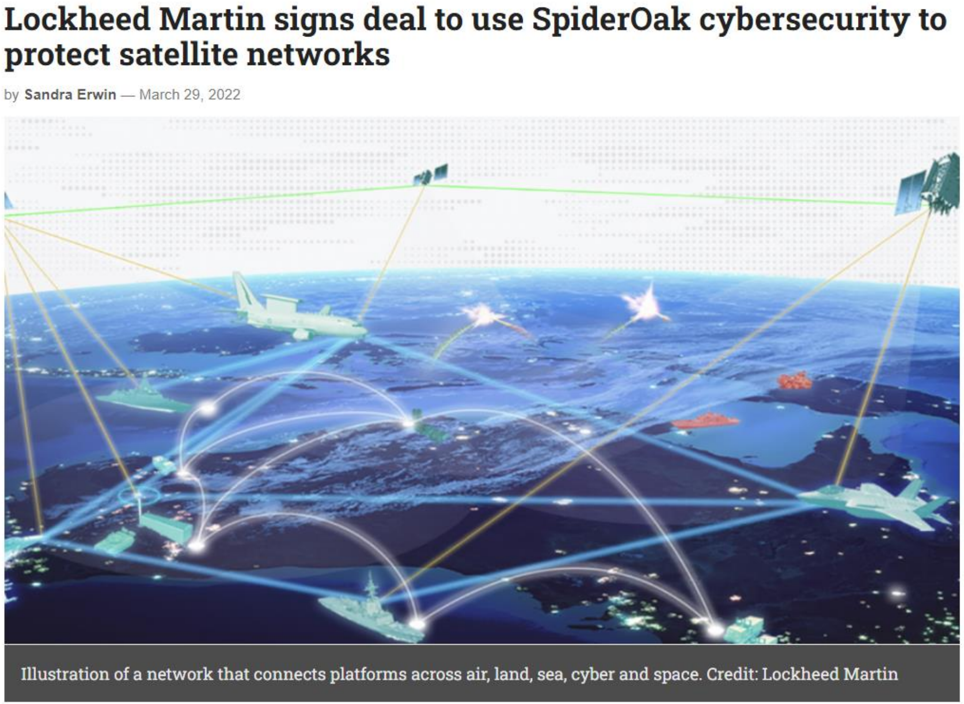
- AI, ML, DL, AA
- Nanotechnology
- Quantum computing
- Hybrid on chip quantum
- Quantum EMS sensing

Emergent Tech

- Russia's and China's pursuit of anti-satellite weapons (ASAT), including laser-armed, satellite-hunting aircraft
  - reduce U.S. and allied military effectiveness
  - offset any perceived US military advantage derived from military, civil, or commercial space systems

Emergent Tech

- Commercial technology that was developed for terrestrial applications and has been repurposed for the space business, specificall for low Earth orbit
- Uses a “zero-trust network architecture”(ZTNA) where network users by default are not trusted and special keys are required to access encrypted data
- OrbitSecure also uses blockchain for data transactions so every modification made to the ledger is time stamped and signed, ensuring traceability



Lockheed Martin signs deal to use SpiderOak cybersecurity to protect satellite networks

by Sandra Erwin — March 29, 2022

Illustration of a network that connects platforms across air, land, sea, cyber and space. Credit: Lockheed Martin