SPACE ISAC

Space Information Sharing and Analysis Center

Samuel S. Visner, MITRE, Space ISAC Board Member
Erin Miller, Executive Director
Nick Tsamis, MITRE
William Ferguson, SES, Space ISAC Board Member

The Mission of **Space ISAC** is to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information.

Space Information Sharing and Analysis Center (Space ISAC) is a direct result of a study conducted by the S&T Partnership Forum in 2014.

Public and private sector dialogue during sessions held at the 34th and 35th Space Symposium led NASA, US Space Force (formerly Air Force Space Command), and National Reconnaissance Office to sponsor the first space-dedicated ISAC.

At the Space ISAC's launch in April 2019, several representatives from public and private sectors spoke out about the importance of protecting our critical space assets.

SPACE ISAC

"Space systems are reliant on information systems and networks from design conceptualization through launch and flight operations. Further, the transmission of command and control and mission information between space vehicles and ground networks relies on the use of radio-frequency-dependent wireless communication channels. These systems, networks, and channels can be vulnerable to malicious activities that can deny, degrade, or disrupt space operations, or even destroy satellites."

In partnership with ANSI, Space ISAC established an SPD 5 Task Force to implement this policy directive for the global space community.

Lockheed Martin, The Aerospace Corporation, and Kratos Defense are leading this task force with support from MITRE Corporation, Parsons Corporation, + a dozen more.

NEXT MEETING: MARCH 2021

- $1T by 2040, Space Foundation Report

- 80% commercial space – global space

- Space capable nations face an increasing threat landscape

- Growing human dependency on space assets for food supply chain, Walmart, Post Office, travel, tourism, jobs, gas stations, communications, emergency response, disaster relief, search and rescue, PNT, ATM transactions, and more

- Space is not defined as critical infrastructure by USG/DHS

- Proliferation of LEO, mega-constellations, 5G, 6G

- Space ISAC was launched in April 2019, opened for general membership in May 2020

- Initial Operating Capability: Threat Intel Platform Launch – Dec-Jan 2021

Space ISAC is taking a multi-decade approach to commercial, international and government collaboration.

- National Cybersecurity Center is the Executive, Operational and Administrative function for Space ISAC.

Space ISAC members are leaders in the security for space community.

- Not recreating a new powerbase, we're leveraging an existing one.
- Formed to bring together members that represent across defense, IC, commercial and international critical infrastructure.

Space ISAC is not a political organization; we're operational. Solving problems for analysts and operators across the globe.

- Through public-private partnership infrastructure that exists today, we're building a Space ISAC HQ location that will serve the space community for the long-game.
- Conducting threat sharing, notifications of incidents of compromise, and alerts in a high–trust environment.

Security for space protects humanity and raises the posture of the entire sector.

- Value of space to humans on Earth shows up in our food supply chain, jobs, access to healthcare, education, communications, aviation, emergency services, transportation, and financial services.

Note: see TLP Amber Priority Intelligence Requirements for Space ISAC members only.

Operations Technology

- Supply Chain
- Concept
- Design
- Manufacture
- Integration
- Deployment
- Maintenance
- Retirement

Examples:
- Suppliers Under Adversary Control
- OT Network Vulnerabilities
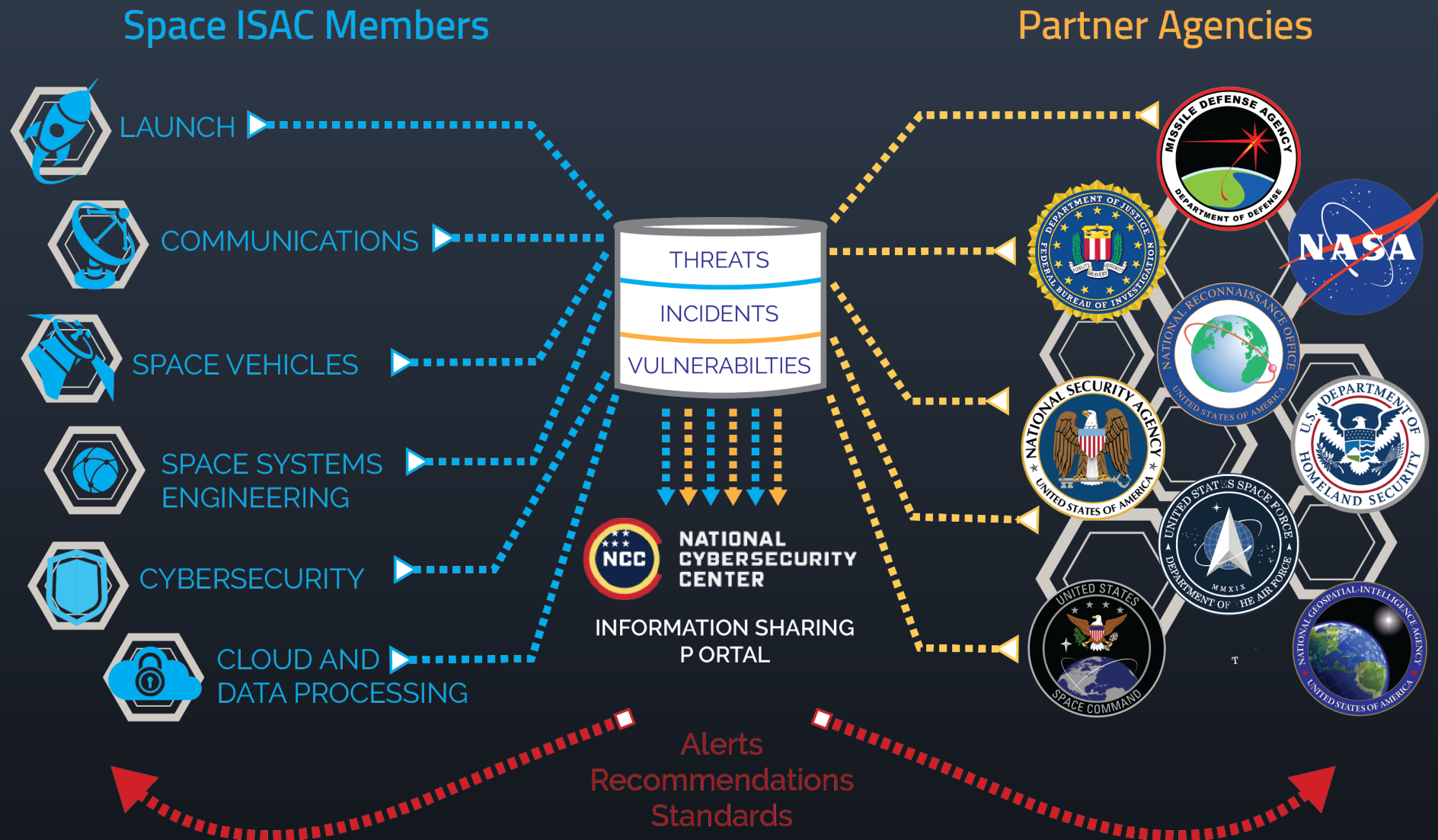- Open-Source Components
- DevOps Environment

Business Systems

- Business Systems/Subsystems
- Enterprise Network
- Data Security
- Software Assurance
- Acquisition Planning
- Commercial Software
- Open-Source Software
- Training Employees
- Public Contractors
- Service Providers
- Finance/Accounting
- ERP/CRM/CMS/BI Software
- Information/Communication Technology

Missions

- Cybersecurity
- Development and Production
- Critical Infrastructure Protection
- Launch, Landing and Recovery
- Space Environment, Weather and Hazards
- Space System Operations

Space ISAC Communities

Space ISAC Members

- LAUNCH
- COMMUNICATIONS
- SPACE VEHICLES
- SPACE SYSTEMS ENGINEERING
- CYBERSECURITY
- CLOUD AND DATA PROCESSING

THREATS
INCIDENTS
VULNERABILTIES

NCC NATIONAL CYBERSECURITY CENTER

INFORMATION SHARING PORTAL

Partner Agencies

Alerts
Recommendations
Standards

Notes: Including International Partner Agencies (ESA, JAXA, DLR, etc.)

Space ISAC Information Sharing Working Group
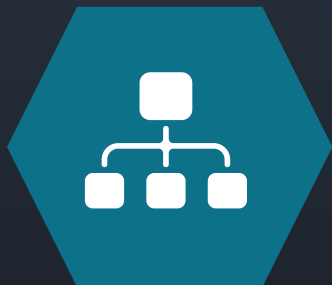
Aerospace Safety Engineer

Critical Mission Analyst

Offensive Security Engineer

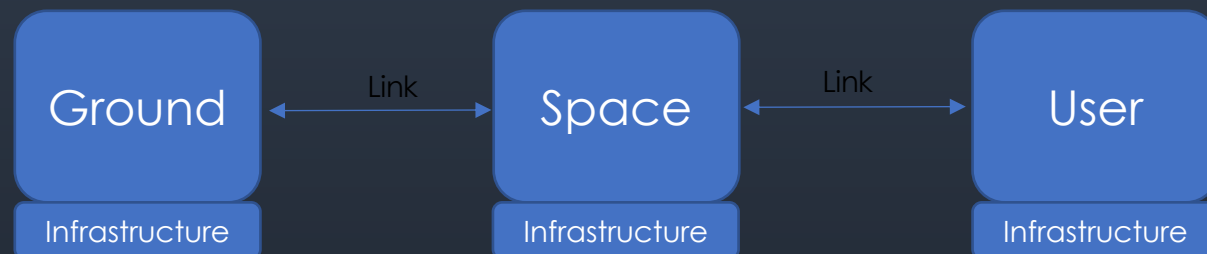End-to-End Mission Analysis

- More than just satellites and rovers:

  - Space Assets
  - Ground Support
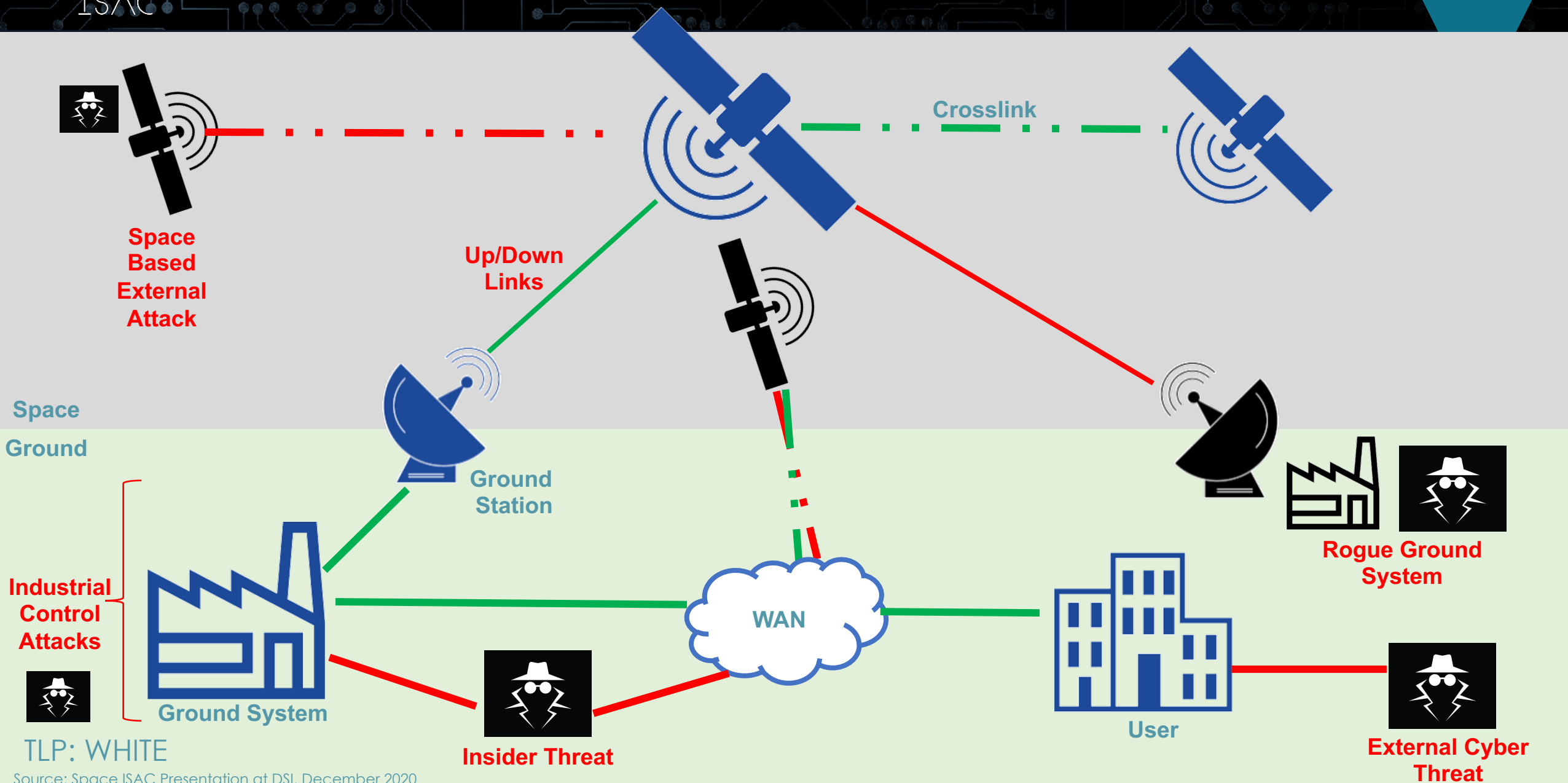 - End Users
  - Link Segment
  - Infrastructure

- Increasing Earth-bound reliance on space systems:

  - Commodity Navigation
  - Energy Resilience
  - Transportation Services
 - National Defense
  - Disaster Warning
  - ...

"Space impacts almost every aspect of our daily lives."

TLP: WHITE

High-Level Space Cyber Threat Vectors

Crosslink

Space Based External Attack

Up/Down Links

Space

Ground

Ground Station

Rogue Ground System

Industrial Control Attacks

WAN

Ground System

Insider Threat

User

External Cyber Threat

TLP: WHITE

Source: Space ISAC Presentation at DSI, December 2020

- Convergence and Connectivity ++

  - Commercial prevalence of the space domain

  - Security boundaries are less defined

  - Commodity HW/SW

- Supply Chain**s** Complexity ++

  - Increased integration == Increased attack surface

  - What did we learn from IoT, Cloud, OT?

  - Requires coordinated approach to security monitoring
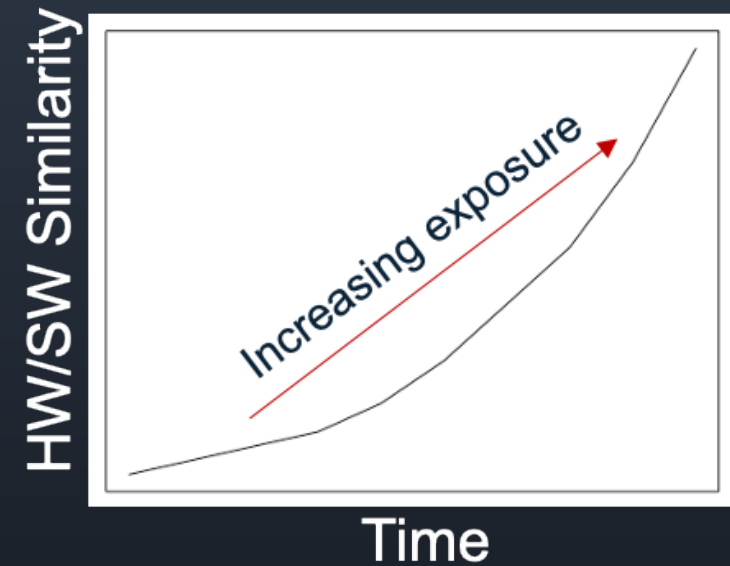
Space systems represent <u>two-way dependencies</u> with our everyday infrastructure.

TLP: WHITE

How can we enable each other?

What information do you need? What information can you share?

How do we leverage what we've learned prior?

Enable all stakeholders: How does your organization interact with space?

TLP: WHITE

Intelligence Liaison Officer for Space-ISAC
Analyst Working Group (AWG)

Participant in the Space-ISAC Threat Intelligence Platform
Deployment

Former Cyberspace Operations Officer

175th Network Warfare Squadron

Former NATO NCIA Security Platform and Analyst

Former Pentagon Cybersecurity Analyst