Hybrid Satellite Networks (HSN) Cybersecurity Framework Profile NIST IR 8441

National Cybersecurity Center of Excellence

Fred Byers / NCCoE

Graham Jenkins / USSF

Karri Meldorf / MITRE

John Wiltberger / MITRE

11/16/2023

This webinar is being recorded

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Welcome and Introduction

Fred Byers, NCCoE

11/16/2023

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NIST welcome and overview – Fred Byers, NIST
- SSC keynote – Graham Jenkins, USSF
- Hybrid Satellite Network (HSN) Cybersecurity Framework (CSF) Profile – Karri Meldorf, MITRE
- Application of the HSN Framework Profile – John Wiltberger, MITRE
- Discussion

NIST CSF Profiles

Cybersecurity for the Space Domain | NCCoE (nist.gov)

- www.nccoe.nist.gov/cybersecurity-space-domain

Overview of NIST Cybersecurity Profiles for the Space Sector:

- NIST IR 8441: Hybrid Satellite Networks (HSN) Cybersecurity Profile
- NIST IR 8323 Rev. 1: Foundational PNT Profile
- NIST IR 8401: Satellite Ground Segment Profile

Although not a CSF Profile, NIST IR 8270: Introduction to Cybersecurity for Commercial Satellite Operations is part of our space domain cybersecurity portfolio.

NIST Cybersecurity Framework

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Magagement & Access Control	PR.AC
	Awareness and Tratining	PR.AT
	Data Securty	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

CSF Profile

Table 1. Asset Management Category for the Identity Function

Subcategory	Applicability to HSNs	Informative References
ID.AM-1		
Physical devices and systems within the organization are inventoried	Focus on the interfaces of the physical devices that interact with external organizations. Successful interfaces will depend on a working knowledge of physical systems owned vs leased by external organizations as well as any constraints, performance requirements, and tolerances. Collaboration with external organizations is necessary to execute a physical inventory that spans organization locations and ownership. Be aware that in the HSN ecosystem, there are limits on the ability to execute a physical inventory (relative to an internal inventory).	**NIST SP 800-53r5,** CM-8, PM-5 **3GPP TS 32.690** **3GPP TS 36.305**
ID.AM-2		
Software platforms and applications within the organization are inventoried	Focus on the interface between organizations. Understand software configurations and version control to ensure interoperability (internal and external). Typically, HSNs have a large and dynamic inventory. Understand the limitations associated with complex inventory processes and procedures. Consider some level of automation.	**NIST SP 800-53r5,** CM-8, PM-5

NIST Cybersecurity Framework

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Function

Category

CSF Profile

Table 1. Asset Management Category for the Identity Function

Subcategory	Applicability to HSNs	Informative References
ID.AM-1		
Physical devices and systems within the organization are inventoried	Focus on the interfaces of the physical devices that interact with external organizations. Successful interfaces will depend on a working knowledge of physical systems owned vs leased by external organizations as well as any constraints, performance requirements, and tolerances. Collaboration with external organizations is necessary to execute a physical inventory that spans organization locations and ownership. Be aware that in the HSN ecosystem, there are limits on the ability to execute a physical inventory (relative to an internal inventory).	**NIST SP 800-53r5,** CM-8, PM-5 **3GPP TS 32.690** **3GPP TS 36.305**
ID.AM-2		
Software platforms and applications within the organization are inventoried	Focus on the interface between organizations. Understand software configurations and version control to ensure interoperability (internal and external). Typically, HSNs have a large and dynamic inventory. Understand the limitations associated with complex inventory processes and procedures. Consider some level of automation.	**NIST SP 800-53r5,** CM-8, PM-5

Subcategory ID

CSF language

Sector

Guidance on how to apply the subcategory to sector

Informative references provide insight on applying controls to achieve the desired outcomes.

Strategic Overview and SSC Approach

16 November 2023

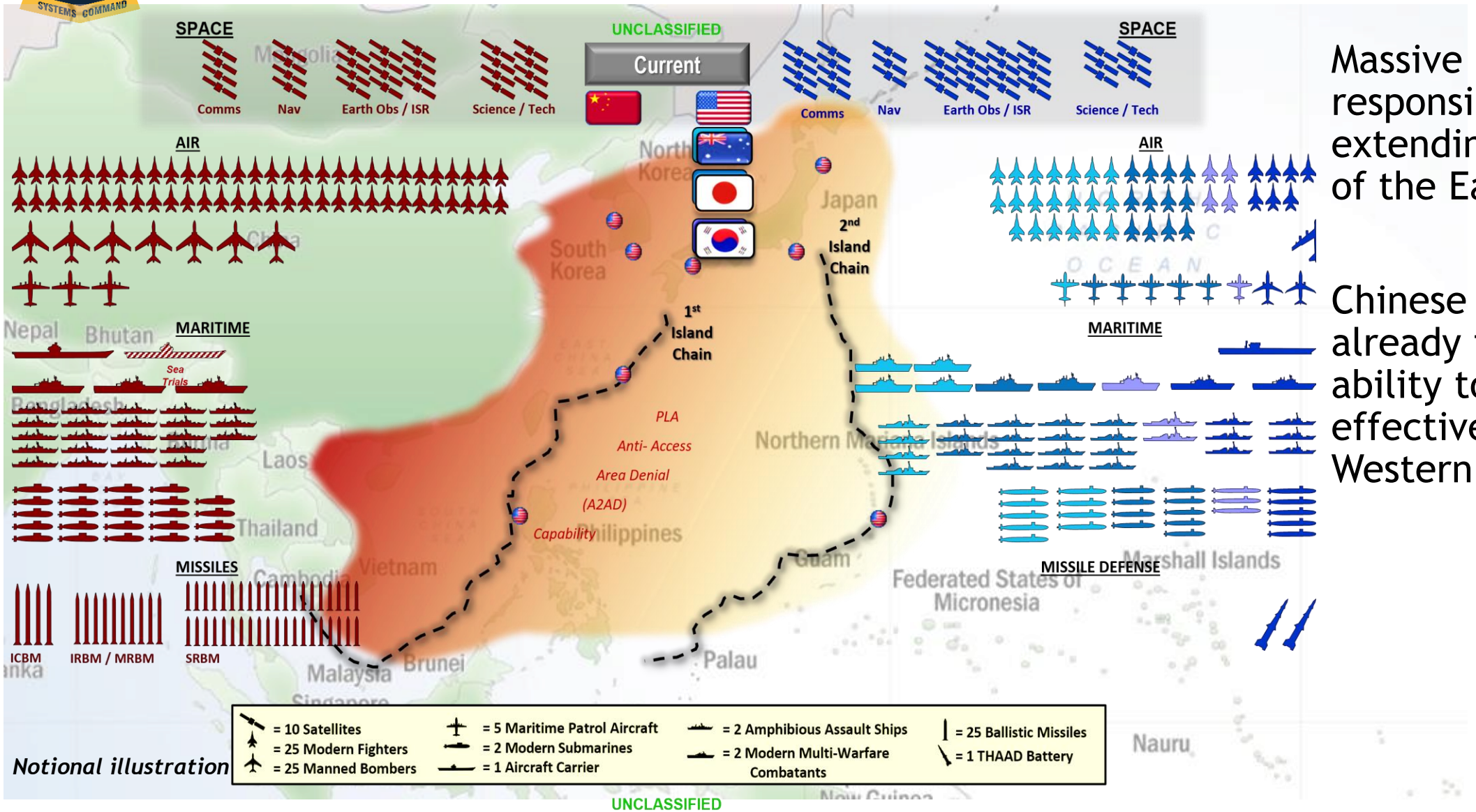
Graham W. Jenkins, Intelligence Specialist
Space Systems Command/OCIO

Transpacific Strategic Environment

Tyranny of Distance

Massive area of responsibility extending over a third of the Earth's surface

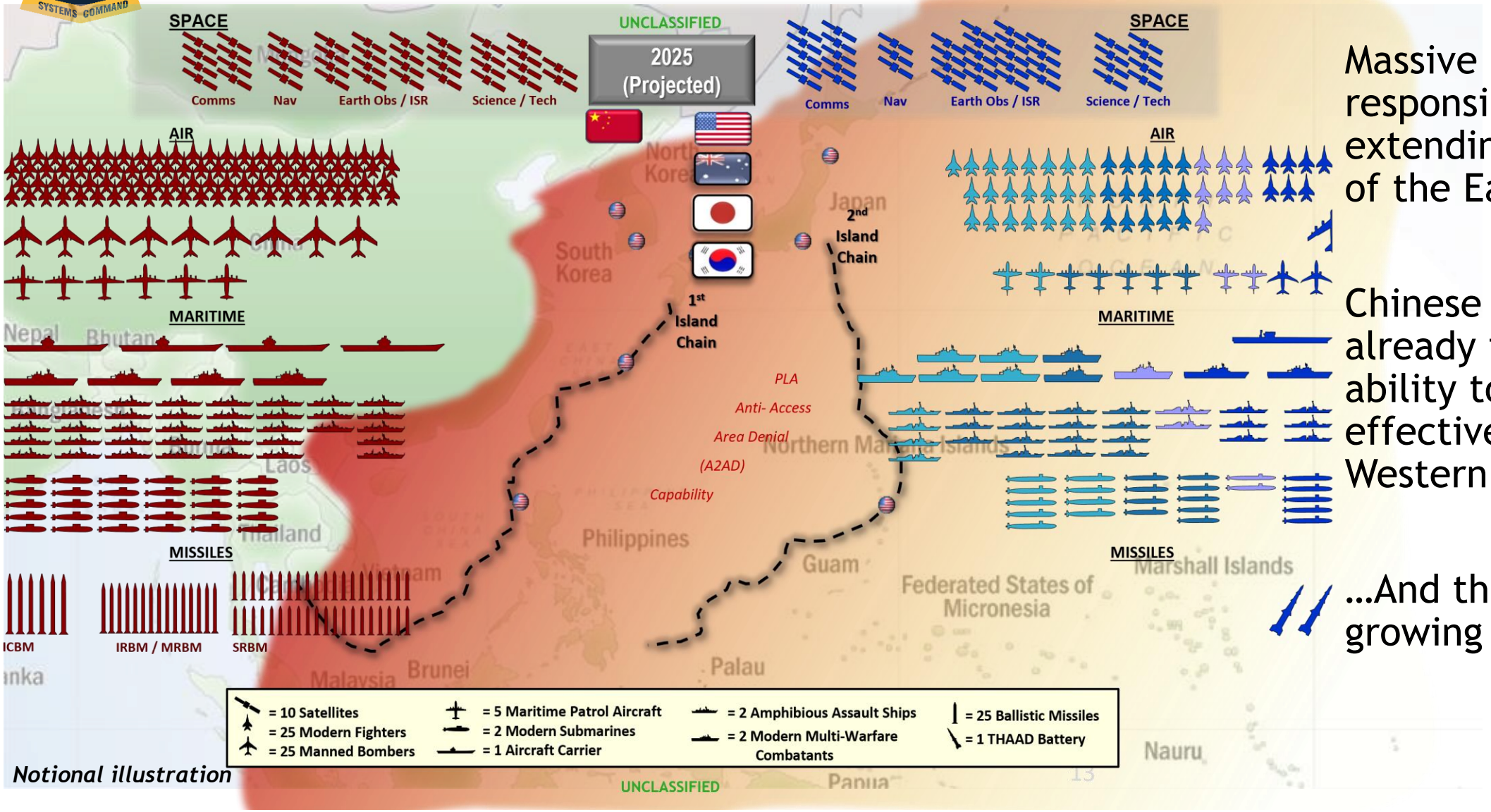
Tyranny of Distance



Massive area of responsibility extending over a third of the Earth's surface

Chinese capabilities already threaten the ability to operate effectively in the Western Pacific

Tyranny of Distance



Massive area of responsibility extending over a third of the Earth's surface

Chinese capabilities already threaten the ability to operate effectively in the Western Pacific

…And they're only growing stronger

Selected Space Capabilities

The Current Op Environment

U.S. intelligence shows that China's President Xi Jinping has instructed his country's military to "be ready by 2027" to invade Taiwan—though he may be currently harboring doubts about his ability to do so given Russia's experience in its war with Ukraine.

–William Burns, DCIA

Cyber Threats to Space Assets

Cyber Threats

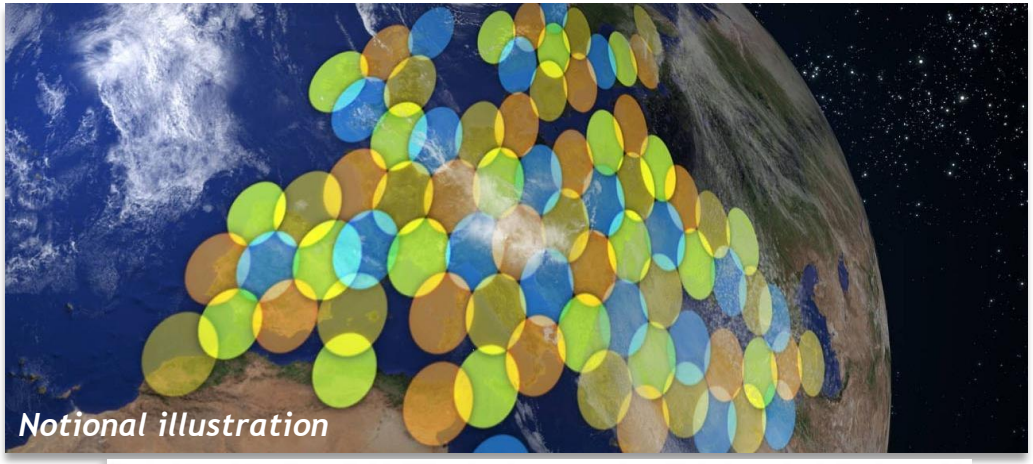
Cyber capabilities threaten *all* space segments

- Dec 2015: China stands up PLASSF
- PLA writings emphasize offensive cyberspace capabilities as a major component of “informatized” warfare
- Centralizes cyber, space, and electronic warfare capabilities

Distinction as a non-government entity does NOT provide protection from adversary ATTACK

Ukraine: Viasat

- Private satellite internet provider whose KA-SAT network offers a wide footprint across Europe
- Misconfigured subcontractor (Skylogic) VPN in ground segment gave attackers access beyond DMZ
- Transmitted wiper software to customer modems via specific spot beams that left them unable to connect to network
- Though a commercial system, KA-SAT is also used by Ukrainian armed forces and other government agencies



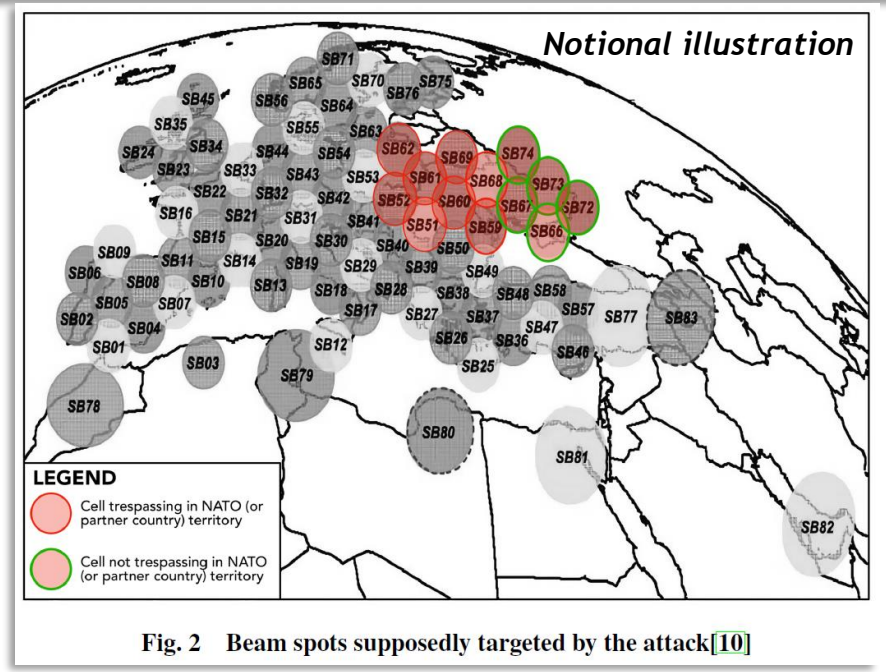


Fig. 2 Beam spots supposedly targeted by the attack[10]

Semper Supra

Research & Demonstrations

Notional illustration

Team of Chinese researchers developed a model to find security flaws in satellite constellations

- Discovered a means of accessing data from an Iridium 108 as well as recommended mitigations for it
- Liu, Bin et al, "Situational Awareness Ontology Modeling for Threat from Space Cyber Operations," *Systems Engineering and Electronics* [in Chinese], March 2022.

Thales Group hacks a demonstrator ESA nanosatellite, OPS-SAT (April 2023)

- Accessed onboard system using standard access rights; introduced malicious code via application environment
- Took control of GPS, attitude control, and onboard camera

Notional illustration

Exploit, Buy, Build

Exploit what we have, Buy what we can, Build only what we must

Dramatically reshaping SSC's approach to acquiring cutting-edge technology and capabilities

- Necessary to keep the nation's joint warfighters ahead of the threat

Employing **Exploit, Buy, Build** for programs within SSC Program Executive Officer (PEO) portfolios

- Protected Anti-Jam Tactical SATCOM (PATS): Exploiting existing infrastructure, buying commercial terminal services - Improving protection of mission capabilities
- Space Based Environmental Monitoring (SBEM): Collaborating with industry, other government agencies and allied partners – Supports providing data to the warfighter at operationally-relevant speeds
- Commercial Augmentation Services (CAS): Exploiting existing infrastructure, buying commercial antenna services to expand SCN bandwidth

Actively moving away from traditional space architectures toward Hybrid Satellite Networks (HSN)

Securing HSN

The Department of the Air Force (DAF) goal is to employ government and commercial cybersecurity capabilities to protect hybrid space architectures

- No ‘one size fits all’ solution: mission needs, system owners, and cyber risk tolerance vary across hybrid satellite architectures

DAF planning multiple solutions to provide options”

- Defensive Cyber Operations for Space (DCO-S): Defend government systems with commercial tools
  - DCO-S provides cyber defense of the space architecture, both in orbit and on the ground
- Infrastructure Asset Pre-approval (IA-Pre): Integrating commercial space providers
  - IA-Pre replaces commercial companies cybersecurity self-assessment process with assessment & authorization process to obtain Approved Products List (APL) approval
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Profile for Hybrid Satellite Networks (HSN): New cybersecurity standards written from context for use by government and/or commercial entities
  - NIST HSN provides cybersecurity guidance for stakeholders engaging in design, acquisition, and operation of hybrid satellite architectures

NIST IR 8441 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)

Karri Meldorf, MITRE

11/16/2023

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Background and Purpose: HSN Cybersecurity

- What is HSN?
  - A Hybrid Satellite Network (HSN), uses independently owned and operated terrestrial and space components to realize a space system that may provide extended global services across diverse missions and connecting points.
  - The HSN architecture typically consists of a combination of independently owned terminals, antennas, satellites, payloads, or other components that communicate across disparate networks.
  - A hosted payload is one easy example, there are many more.
- Purpose/Scope of NIST IR 8441
  - Provide practical guidance for organizations and stakeholders engaged in the design, acquisition, and operation of HSN components (such as satellite buses or payloads) in a manner consistent with the organization's risk tolerance.
  - Describe the salient cybersecurity functions that are part of the HSN and may include examples to highlight cybersecurity dependencies.

Components of HSN

The scope of the HSN profile focuses on physical and virtual interfaces such as:

- Antenna fields
- Virtual Machine-based command formatter
- Software-defined elements hosted on a cloud
- Bus
- Payloads
- User terminals
- Intermediate ground nodes
- Intersatellite cross links for purposes such as linking to a payload hosted on another satellite, higher resolution, greater communication bandwidth, path redundancy, etc.

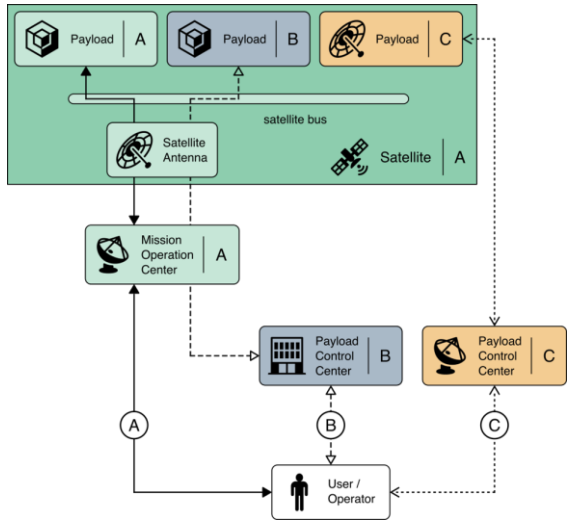
HSN intended use and architectures

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

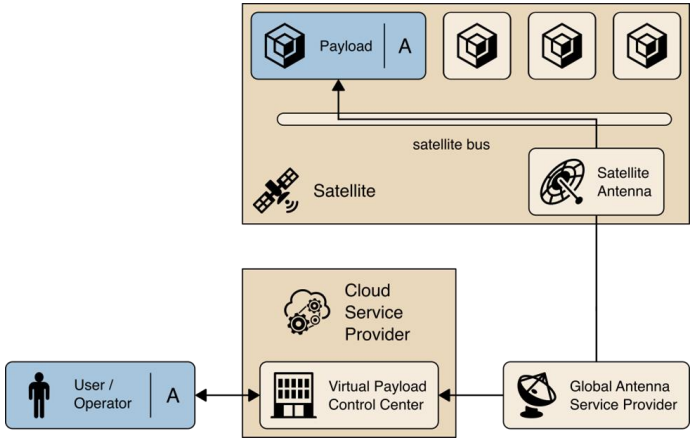
HSN profile is intended to:

- Facilitate integration
- Consistently assess and communicate the cybersecurity posture
- Provide a comprehensive framework to facilitate risk management decisions
- Facilitate consistent assessments of cyber-risk

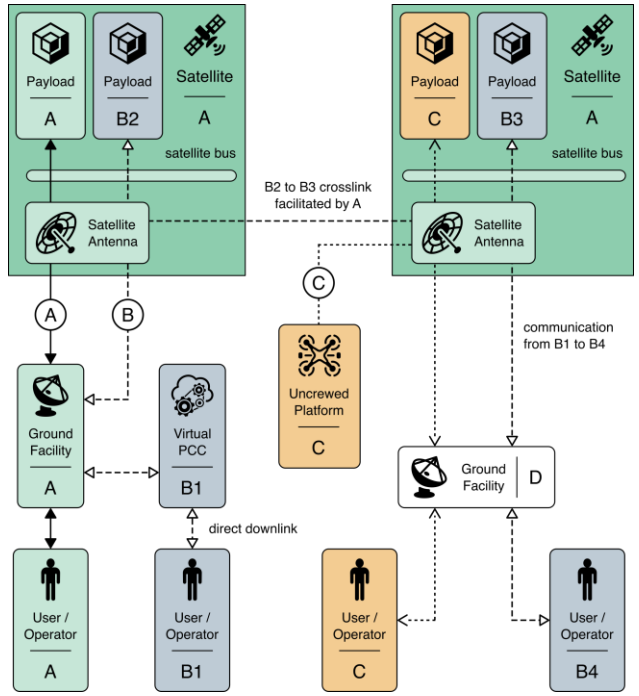
The HSN Profile is voluntary and does not issue regulations, define mandatory practices, provide a checklist for compliance, nor does it carry statutory authority. It is intended to be a foundational set of guidelines.



Simple HSN Architecture



HSN with virtualized components



More complex HSN architecture

HSN Profile Audience

Intended for those involved in managing, developing, implementing, and monitoring the HSN cybersecurity including:

- Procurement officials responsible for the acquisition of HSN services
- Public and private organizations that provide HSN services
- Managers responsible for the use of HSN services
- Risk managers, cybersecurity professionals, and others with a role in cybersecurity risk management for systems that provide or interface with HSN services
- Mission and business process owners responsible for achieving operational outcomes dependent on HSN services
- Researchers and analysts who study the unique cybersecurity needs of HSN services
- Cybersecurity architects who integrate cybersecurity into the product designs for space vehicle segments and ground segments.

Profile Intended Use

- Operational considerations
  - What methods can be used to detect potential events of concern?
  - What methods can be used to respond to those detected events?
  - What methods can be employed for post-event recovery?
- Mission considerations
  - What services are mission-critical?
  - What systems and data/assets are vulnerable?
  - What recovery/fail-over strategies can be employed?
  - What measures are available to determine the effectiveness of security controls?
- Engineering considerations
  - What are the capabilities of the system?
  - What are the capabilities of potential adversaries to the system?
  - Which system attributes are adjustable post-deployment, and which are immutable?
- External considerations
  - What external systems and data are critical?
  - What are the impacts of degraded or failed external services?

Example of HSN CSF Profile

Subcategory	Applicability to HSNs	Informative References
ID.AM-1: Physical Devices and systems within the organization are inventoried.	Focus on the interfaces of the physical devices that interact with external organizations. Successful interfaces will depend on a working knowledge of physical systems owned vs leased by external organizations as well as any constraints, performance requirements, and tolerances. Collaboration with external organizations is necessary to execute a physical inventory that spans organization locations and ownership. Be aware that in the HSN ecosystem, there are limits on the ability to execute a physical inventory (relative to an internal inventory).	**NIST SP 800-53r5** CM-8, PM-5 **3GPP TS 32.690** **3GPP TS 36.305**

Distinctions between CSF and HSN Profile

- Cybersecurity Framework (CSF)
  - Defines Functions, Categories, Subcategories pertaining to cybersecurity
  - The CSF facilitates comprehensive cybersecurity assessments
- CSF HSN Profile - NIST IR 8441
  - Evaluates the CSF in the context of the HSN cyber ecosystem
  - NIST IR 8441 is a foundation for cybersecurity practitioners to assess their HSN
- “Customize” NIST IR 8441
  - Evaluates the HSN in the context of a specific organization/project
  - Is an assessment of the organization’s cybersecurity posture

Implementing the HSN Profile

- Cybersecurity Framework (CSF)
  - Created for the Critical Infrastructure, but may be used by any organization
  - Provides *guidance* for a holistic *assessment* of their cybersecurity posture
- CSF Profile - NIST IR 8441
  - Focuses on the “what” to assess, not the “how” to implement
  - Provides guidance on “what to *consider”,* not “what to *implement*”
- “Customize” NIST IR 8441
  - Evaluates how well an implementation addresses a subcategory
    - Evaluated from the assessor’s perspective
    - Implementations of the subcategories influence and build upon other subcategories
  - Provides an assessment that can be used to support risk management.

Application of the Hybrid Satellite Network Cybersecurity Framework Profile

NIST TN 2272 - An Example Implementation of NIST IR 8441

John Wiltberger, MITRE

11/16/2023

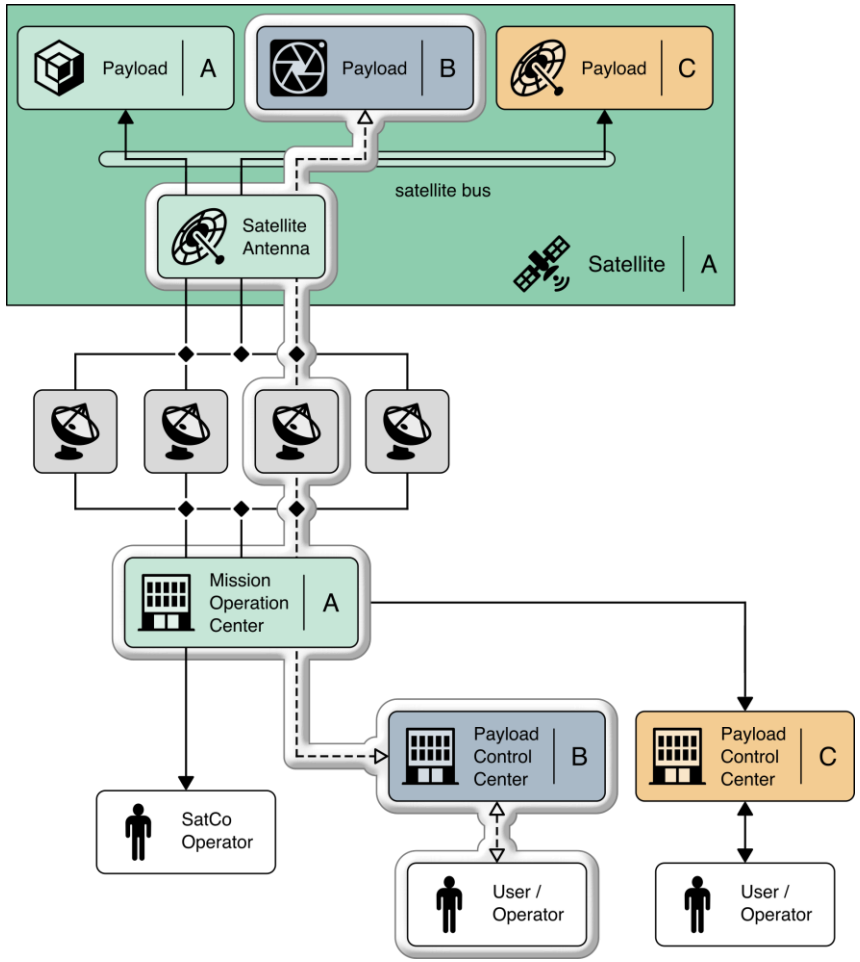
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Document Overview

- Demonstrate an implementation of CSF Profile - NIST IR 8441
- Scenario-based mission and business case
- Analyze CSF for HSN Functions and Categories in the context of the scenario
- Showcase considerations both internally and for contracts
- Validate actions through operational examples

Overview of Reference Scenario

- SaveForests
  - Mission objectives
    - Assess and protect forests using overhead imagery data
    - Provide analysis to stakeholders on various forest issues
    - Become a trusted source of accurate forest data and information
  - HSN components and architecture
- SatCo
  - Contracted to provide hardware and support
  - Utilize MOC, Ground Services, and Satellite bus
- Other Entities
  - Providing hardware for payload
  - Co-located payloads



SatCo Satellite System Overview

Example Assessment

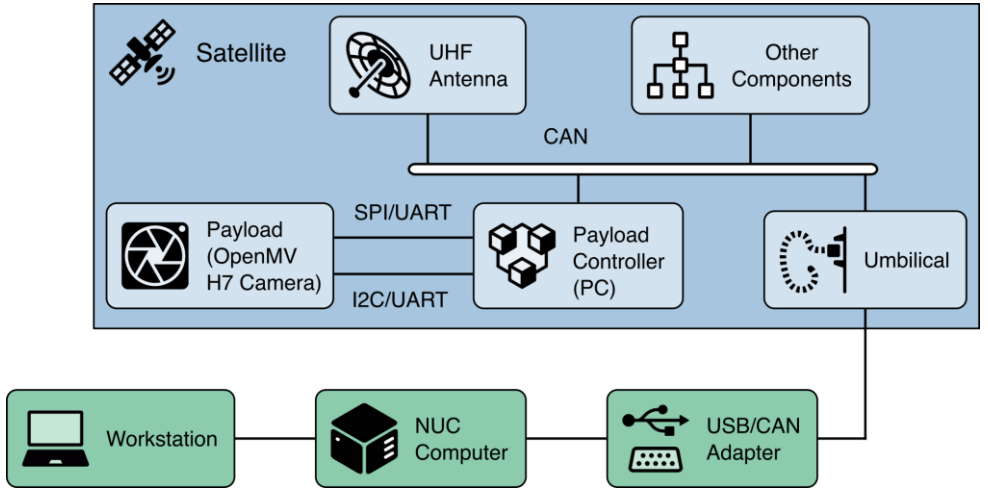
- Key findings from the assessment of SaveForests' current cybersecurity posture
- Use of NIST IR 8441 to create a custom profile for SaveForests' HSN environment
- Analysis of the current cybersecurity posture leading to testing of additional cybersecurity measures in a lab

Subcategory	SaveForests
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	**Payload owner Organization:** Interactions with the payload are strictly limited to a subset of SaveForests personnel who are authorized to command the satellite. The SatCo MOC authenticates with the PCC. Access to the PCC is strictly managed by SaveForests. The telemetry and mission data are downlinked to the MOC and then transported directly to PCC. SaveForests implements role-based access control to the mission and telemetry data stored on-premises at PCC.
	Partner Organizations: SatCo: SatCo issues and manages credentials and access to the MOC.

Subcategory	SaveForests
DE.AE-5: Incident alert thresholds are established	**Payload owner Organization:** SaveForests set thresholds for the payload to include a loss of telemetry data for a period greater than 45 minutes, a failure to acknowledge two or more consecutive commands, and a deviation of the camera orientation from the last acknowledged position.
	Partner Organizations: SatCo: Incident alert thresholds that impact the payloads established by SatCo are communicated with SaveForests.

Commercial Space Cyber Resiliency Lab (CSCRL)

- Demonstrate real world example
- Three Operational Examples
  - Hosted Payload Fault
  - Hosted Payload File Modification
  - Payload Encryption
- Test procedures and results for each operational example



Commercial Space Cyber Resiliency Lab (CSCRL)

Example #1 – Hosted Payload Fault

- Fault code displayed; potential system fault or cyber intrusion
- Fault transmitted and recorded in shared database
- Signal analyzed for fault type and resolution
- Forensic analysis to differentiate equipment issues and cyber intrusions
- Procedures for operational anomalies and cyber intrusions developed

Example #2 – Payload File Modification

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Corrupted image file; determine if anomaly or cyber intrusion
- Assess camera software/scripts for modifications
- External security device performs assessment
- Device compares internal storage with original reference
- Check code syntax, character counts, file size
- If modified, replace with original software copy

Example #3 – Payload Encryption

- Data potentially visible to other operators
- Camera encrypts data for exclusive access
- Captured image encrypted and sent to ground station
- Full encryption prevents monitoring/viewing
- Demonstrates secure image transmission feasibility

Implementation Summary

- Tailored perspectives clarify entity's standing
- CSF subcategories mitigate risk, support management plans
- CSF Profile for HSN applicable across scenarios
- Organizations can integrate, retrofit, secure HSN ecosystems

Questions?

Thank you for joining!

Team Email: spacecyber_nccoe@nist.gov

https://www.nccoe.nist.gov/cybersecurity-space-domain

nccoe.nist.gov

@NISTCyber

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE