

National Aeronautics and  
Space Administration



# An Overview of NASA Space Protection

**Presented to the Small Spacecraft Systems  
Virtual Institute (S3VI) by**

**Joshua.Krage@nasa.gov**

**2020-02-12**

**NASA Office of the Chief Engineer  
Space Asset Protection Program**

[www.nasa.gov](http://www.nasa.gov)

# Discussion Flow

## **This session:**

- What are we worried about?
- How is NASA responding?
- What is the NASA guidance?
  - Directives, standards, guidance
  - Common questions
- Questions from you

# Things Future Missions Should Consider

**Space is contested, congested, and competitive, and space capabilities are vulnerable to emerging threats**

**NASA missions continue to be affected by adversarial threats**

- Space systems, ground systems, support systems, physical systems, and humans are all potential victims of adversarial threats

**Integrate protection early in the conceptual and design phases**

- How do we ensure our systems are not trivially subverted?
- How do we maintain command authority over our systems?
- How do we improve the resiliency of our systems?
- How do we achieve mission success in spite of threat actor actions against our systems?

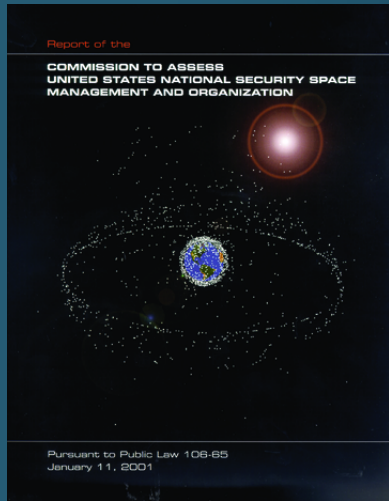
**Be informed, build a plan, integrate threat perspectives, implement protected systems, learn, iterate**

- Many NASA organizations can help, including Office of the Chief Engineer's (OCE) Space Asset Protection Program (SAPP), Office of the Chief Information Officer (OCIO), Office of Protective Services (OPS), and the Office of Safety and Mission Assurance (OSMA)

**We must protect our systems from the action of others, and protect others from our systems**

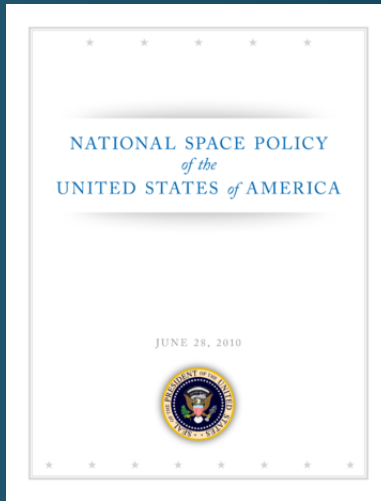
**What are we worried about?**

# Key National Documents



**2001-01-11: Commission to Assess US National Security Space Management and Organization** aka “Rumsfeld Commission”

- Space systems are vulnerable
- US is dependent on space
- Focuses mostly on DOD and the Intelligence Community
- Served as a call to action to clarify US goals in space



**2010-06-28: National Space Policy of the United States of America**

- Establishes US principles for space, including peaceful exploration, responsible actions
- US goals include cooperation, assurance and resilience, and Earth and solar observation

**Amended in 2017 to expand NASA's exploration goals to include Moon and Mars.**



**2011-01: National Security Space Strategy (Unclassified Summary)**

- Space is congested, contested, and competitive
- Improve space situational awareness and transparency
- Deter aggression in space
- Strengthen resilience

Newer documents have since been issued.



**2018-12: NASIC: Competing in Space**

**2019-02: DIA: Challenges to Security in Space**

- First public US documents describing specific counterspace threats associated with individual countries
- Overview of types of capabilities and potential effects on space systems and their support systems
- Details about counterspace capabilities available to other nations, and the perceived motivations for use



# Counterspace Continuum

## Modeling the types and means of counterspace threats

UNCLASSIFIED

### (U) Counterspace Continuum



UNCLASSIFIED

# Specific Threat Areas to Consider

## Spacecraft Command Link

- Inadvertent interference on command link frequencies
- Purposeful interference / jamming
- Purposeful probing of the receiver, unauthorized command attempts

## GPS / GNSS

- Jamming/denial of the GPS signals
- Measurement or data spoofing of GPS signals

## Cybersecurity

- Command link bypass/subversion, e.g., operations console hijack
- Re-purposed sub-systems on the space platform
- Loss of critical digital reference files, e.g., via ransomware

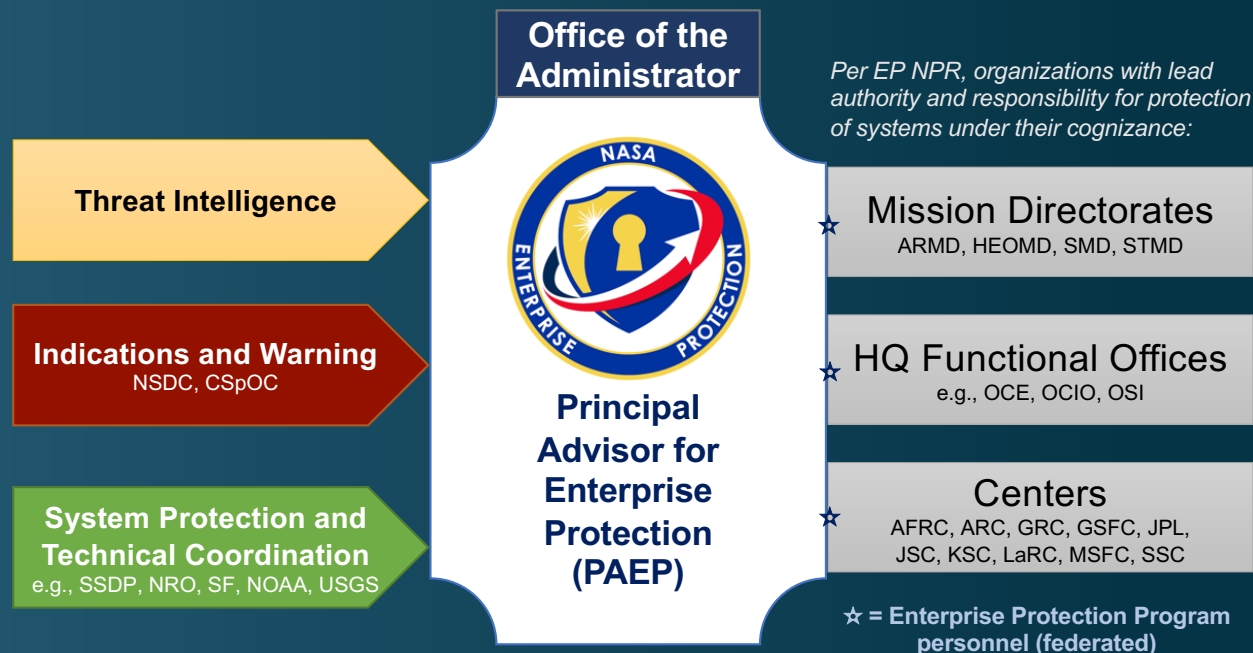
## Directed Energy

- Overload of optical sensors from excess energy

# How is NASA responding?



# What is Enterprise Protection? Overview



## Agency Strategic Objective 4.5: Ensure Enterprise Protection

“Increase the resiliency of NASA’s enterprise systems by assessing risk and implementing comprehensive, economical, and actionable solutions.”

## NPR 1058.1 NASA Enterprise Protection Program

# Office of Chief Engineer: Space Asset Protection Program

## **Space Asset Protection Program (SAPP), established in 2008**

- Deputy Chief Engineer is Technical Authority (TA) for space asset protection
- Comprised of cleared technical experts in space and ground systems, with additional expertise in unclassified and classified threats and vulnerabilities, and mitigation strategies

## **Prepares protection guidance, based on threats, vulnerabilities, and actual NASA protection-related experiences**

- Ongoing technical interchange with other government agencies
- Experiments and research projects to discover or validate vulnerabilities and mitigations

## **Provides technical support to Mission Directorate and Center protection teams**

- These teams in turn aid programs and projects to implement effective protection measures
  - Ex. HEOMD System Protection Office (SPO), GSFC, LaRC, JPL

## **Integral part of the Enterprise Protection Program**

- Near daily work with PAEP
- Leads work on unexplained interference detection and reporting in support of the US Purposeful Interference Response Team (PIRT)

# What is the NASA guidance?

# NASA Protection Guidance, Summary

## NASA Enterprise Protection Guidance

- NPR 1058.1, June 2019, NASA Enterprise Protection
  - Establishes the roles and responsibilities related to the Principal Advisor for Enterprise Protection, the Enterprise Protection Program (EPP), and the Enterprise Protection Board (EPB)

## NASA Space Protection Guidance

- NPR 7120.5, August 2012, NASA Space Flight Program and Project Management Requirements
  - Requires a project protection plan based off threat summaries
  - NPR 7120.8 projects can incorporate protection plan requirements (such as via project control plans and project tailoring)
- OCE Memo, May 2018, Space Asset Protection Requirements
  - Updates 7120.5 to reflect process changes for protection plans, adds Candidate Protection Strategies, removes some constraints such as classification requirements for plans
- AA Memo, February 2019, Direction to Protect Command Link and Other Aspects of Robotic Spacecraft
  - Establishes new requirements for robotic spacecraft, to be codified by the Chief Engineer in future policy
- Candidate Protection Strategies
  - Starting point for developing a protection plan, series of questions related to best practices to mitigate high threat and risk issues
- NASA-STD-1006: Space System Protection Standard
  - Baseline standards to improve space system protection from well understood threats

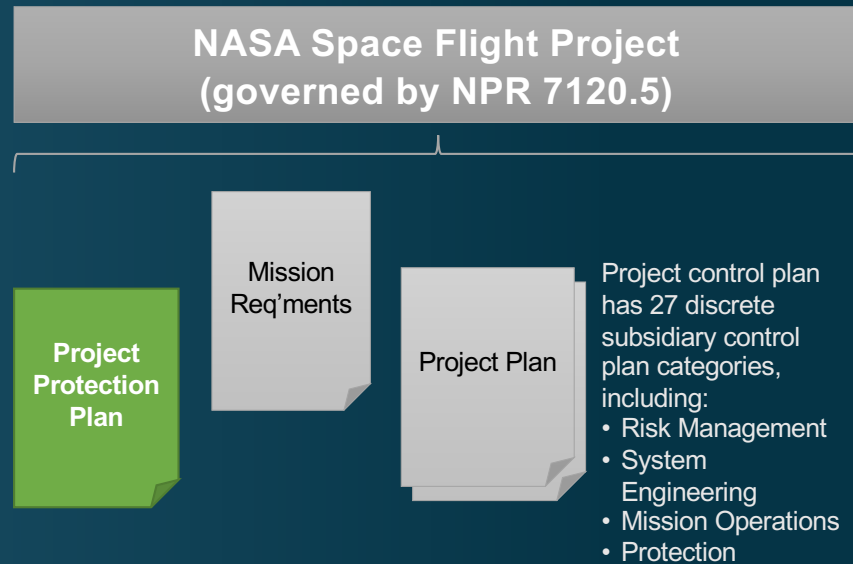
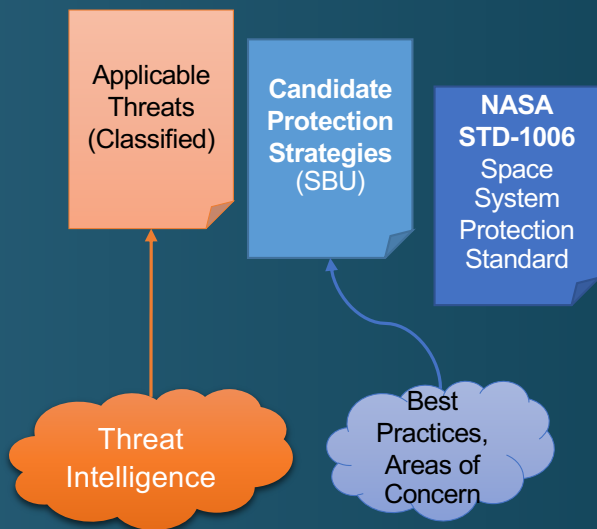
**Note also: related guidance for physical/industrial security (NPD 1600 series), and information security (NPD 2810 series)**

## NASA Engineering Network (NEN) Space Asset Protection Community of Practice site:

- <https://nen.nasa.gov/web/sap>

# Space Protection Approach

Each mission's protection profile is derived from its objectives, capabilities, applicable threats, and risk posture.



Missions leverage institutional infrastructure capabilities, such as space communications (Deep Space Network, Near Earth Network, Space Network), terrestrial communications, test chambers, and operations centers.

# Robotic Spacecraft Command Link Protection Policy Memorandum [1]

National Aeronautics and  
Space Administration  
Office of the Administrator  
Washington, DC 20546-0001



February 1, 2019

TO: Chief Engineer  
Associate Administrator for the Science Mission Directorate  
Associate Administrator for the Space Technology Mission Directorate  
Associate Administrator for the Human Exploration and Operations Mission Directorate

FROM: Associate Administrator

SUBJECT: Direction to Protect Command Link and Other Aspects of Robotic Spacecraft

Identified threats and vulnerabilities to space systems indicate that command uplinks to robotic spacecraft need to be better protected. Consequently, I am directing the protection contained in the enclosure.

I am directing the Chief Engineer to promulgate additional requirements, as appropriate, to implement the intent of this memorandum, and to incorporate these requirements into Agency governance documentation as expeditiously as possible. In case of conflict, Agency governance documentation, once released, will supersede this memorandum.

  
Stephen G. Jurczyk

Enclosure

cc:  
Associate Administrator for Aeronautics Research Mission Directorate  
Assistant Administrator for Protective Services

## Direction to Protect Command Link and Other Aspects of Robotic Spacecraft

- (1) Except for:
- Spacecraft already required to use command uplink encryption,
  - Hosted instrument payloads,
  - Class C or D spacecraft without a propulsion subsystem, and
  - Spacecraft designed to operate beyond the Moon.

All new-start or newly-solicited robotic spacecraft shall protect the command uplink with encryption compliant with the Federal Information Processing Standard (FIPS) 140-2, Cryptographic Module Validation Program.

(Rationale: Command link incidents with civil space missions have demonstrated potential impacts to safe operations.)

For robotic spacecraft already in development that would otherwise be subject to this protection, the technical, cost, and schedule impact of adding command link protection shall be analyzed by the Mission Directorate during FY 2019. Command link protection shall be added if it is determined by the Mission Directorate that mission risk is significant and documented in the Project Protection Plan.

The downlink may be encrypted, if determined appropriate by a Mission Directorate, to protect sensitive data.

- (2) For all new-start or newly-solicited robotic spacecraft, the command uplink, position, navigation, and timing (PNT) subsystems shall recognize and survive interference.

(Rationale: Recent GPS incidents with civil space missions showed that missions can unexpectedly lose GPS signals, including timing information.)

- (3) For all robotic spacecraft, information pertaining to the command uplink shall be protected at least as Sensitive But Unclassified (SBU), and in accordance with the Asset Vulnerability Protection security classification guide issued by the Office of Protective Services, August 29, 2017.

Enclosure

Please follow Mission Directorate guidance in the implementation of this policy.

# Robotic Spacecraft Command Link Protection Policy Memorandum [2]

National Aeronautics and  
Space Administration  
Office of the Administrator  
Washington, DC 20546-0001



February 1, 2019

TO: Chief Engineer  
Associate Administrator for the Science Mission Directorate  
Associate Administrator for the Space Technology Mission Directorate  
Associate Administrator for the Human Exploration and Operations Mission Directorate

FROM: Associate Administrator

SUBJECT: Direction to Protect Command Link and Other Aspects of Robotic Spacecraft

Identified threats and vulnerabilities to space systems indicate that command uplinks to robotic spacecraft need to be better protected. Consequently, I am directing the protection contained in the enclosure.

I am directing the Chief Engineer to promulgate additional requirements, as appropriate, to implement the intent of this memorandum, and to incorporate these requirements into Agency governance documentation as expeditiously as possible. In case of conflict, Agency governance documentation, once released, will supersede this memorandum.

  
Stephen G. Jurczyk

Enclosure

cc:  
Associate Administrator for Aeronautics Research Mission Directorate  
Assistant Administrator for Protective Services

Please follow Mission Directorate guidance in the implementation of this policy.

## Direction to Protect Command Link and Other Aspects of Robotic Spacecraft

- (1) Except for:
- Spacecraft already required to use command uplink encryption,
  - Hosted instrument payloads,
  - Class C or D spacecraft without a propulsion subsystem, and
  - Spacecraft designed to operate beyond the Moon.

All new-start or newly-solicited robotic spacecraft shall protect the command uplink with encryption compliant with the Federal Information Processing Standard (FIPS) 140-2, Cryptographic Module Validation Program.

(Rationale: Command link incidents with civil space missions have demonstrated potential impacts to safe operations.)

For robotic spacecraft already in development that would otherwise be subject to this protection, the technical, cost, and schedule impact of adding command link protection shall be analyzed by the Mission Directorate during FY 2019. Command link protection shall be added if it is determined by the Mission Directorate that mission risk is significant and documented in the Project Protection Plan.

The downlink may be encrypted, if determined appropriate by a Mission Directorate, to protect sensitive data.

- (2) For all new-start or newly-solicited robotic spacecraft, the command uplink, position, navigation, and timing (PNT) subsystems shall recognize and survive interference.

(Rationale: Recent GPS incidents with civil space missions showed that missions can unexpectedly lose GPS signals, including timing information.)

- (3) For all robotic spacecraft, information pertaining to the command uplink shall be protected at least as Sensitive But Unclassified (SBU), and in accordance with the Asset Vulnerability Protection security classification guide issued by the Office of Protective Services, August 29, 2017.

(1) ...

All new-start or newly-solicited robotic spacecraft shall **protect the command uplink with encryption** compliant with the FIPS 140-2...

(2) For all new-start or newly-solicited robotic spacecraft, the command uplink, position, navigation, and timing (PNT) subsystems shall **recognize and survive interference**.


(3) For all robotic spacecraft, information pertaining to the command uplink shall be protected at least as SBU...

Enclosure

# NASA Technical Standard NASA-STD-1006

## Space System Protection Standard [approved 2019-10-29]

<https://standards.nasa.gov/standard/nasa/nasa-std-1006>

 NASA TECHNICAL STANDARD Office of the NASA Chief Engineer	NOT MEASUREMENT SENSITIVE
	NASA-STD-1006
	Approved: 2019-10-29
<b>SPACE SYSTEM PROTECTION STANDARD</b>	
APPROVED FOR PUBLIC RELEASE—DISTRIBUTION IS UNLIMITED	

The standard may be incorporated into program/project requirements on a voluntary basis.

A decision on how to mandate implementation of the standard through NASA policy is pending.

### Maintain Command Authority

- Command Stack Protection: Programs/projects shall protect the command stack with encryption that meets or exceeds the FIPS 140.
- Backup Command Link Protection: If a project uses an encrypted primary command link, any backup command link shall, at minimum, use authentication.
- Command Link Critical Program/Project Information (CPI): The program/project shall protect the confidentiality of command link CPI as NASA SBU information to prevent inadvertent disclosure to unauthorized parties per NASA NID 1600.55 and NPR 2810.1.

### Ensure Positioning, Navigation, and Timing (PNT) Resilience

- PNT Interference Recognition: If project-external PNT services are required, projects shall ensure that systems are resilient to the complete loss of, or temporary interference with, external PNT services.

### Report Unexplained Interference

- Interference Reporting: Projects/Spectrum Managers/Operations Centers shall report unexplained interference to SAPP or to other designated notifying organizations.
- Interference Reporting Training: Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.



## Candidate Protection Strategies (CPS)

**Serve as a starting point for mission protection planning**

**Best practices, consider relevant threat intelligence and risk issues**

**Protection plans incorporate results of the CPS analysis, including any requisite requirement tailoring**

CPS document is NASA Sensitive But Unclassified (SBU), available:

- via the NASA Engineering Network (NEN) SAP community of practice site (in the SBU folder), or
- via request from the NASA SAPP team

### **Main Categories (# of questions)**

- 1. Engineering Focused Strategies – Space Segment (3)**
- 2. Engineering Focused Strategies – Ground Segment (2)**
- 3. Engineering Focused Strategies – All Segments (2)**
- 4. ConOps Focused Strategies (6)**
- 5. Cyber Focused Strategies – Access (3)**
- 6. Cyber Focused Strategies – System Design (3)**
- 7. Cyber Focused Strategies – Software Design (1)**

# Common Questions Regarding Command Path Encryption [1]

## What counts as “no/without propulsion?”

- At present this can be very context specific. Ultimately, the decision authority (e.g., program office) will make this decision, with appropriate technical input.

## Does “command stack” mean only the RF link to the space platform?

- The term command stack specifically includes any components, such as a terrestrial network, between the operations center and receipt/execution on the space platform.

## What are common approaches to command link encryption?

- “Bulk encryption” encrypts the entire sequence, including all header and meta-data. Often the simplest to implement. Has implications for interoperability and relay architectures.
- CCSDS Space Data Link Security Protocol. Protects frame data within a transfer frame, without protecting the space link protocol frame header or trailer. Provides interoperability, should improve support for relay architectures.

## Common Questions Regarding Command Path Encryption [2]

### What is an appropriate encryption implementation?

- FIPS 140 *Security Requirements for Cryptographic Modules* certified modules.
  - NASA has not mandated a specific required FIPS 140 level (1-4).
  - From FIPS 140 Applicability: *Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard.*
  - FIPS 140 certification covers a defined cryptographic module that provides an approved set of functions (e.g., algorithms, key management), implemented in a specific executable environment (hardware, firmware, software), following specific operations procedures, all verified by independent testing.
- Both software-only and hardware solutions are acceptable if otherwise compliant.

## Common Questions Regarding GPS / GNSS?

### **Can a space system's GNSS receiver be affected by a terrestrial source?**

- Yes! From a single source, a LEO space system may only be affected during a pass (minutes). Multiple sources can extend the duration. Effects can extend beyond LEO. Depending on design, some effects may linger.

### **What resilience options should be considered?**

- Ensure the receiver has been tested against the current interface control document / specification (e.g., IS-GPS-200 for GPS)
- Use appropriate navigation filter designs (e.g., NASA/TP-2018-219822)
- Monitor PNT telemetry, e.g., solution state, number of sources being tracked, signal integrity (if available)
- Consider higher quality sources if available (e.g., GPS Precise Positioning Service)

**Questions?**

# Backup Slides

# Protection Plan Content Breakout

## Protection Plan

- Project/mission background
- Protection-related requirements
- Susceptibilities
- Risk assessment
- NASA-STD-1006 assessment
- Candidate Protection Plans assessment

Document is normally controlled as NASA Sensitive But Unclassified (SBU).

## Appendix

- Threat applicability
- Threat summary
- Vulnerability analysis
- Detailed risk analysis
- Mitigation recommendations

Appendix contents are normally Classified due to content.

# Center for Strategic and International Studies (CSIS) Space Threat Assessment 2019 (April 2019)



The report provides a readable introduction to four categories of counterspace weapons (kinetic physical, non-kinetic physical, electronic, cyber), and then reviews the known capabilities of other nations (China, Russia, Iran, North Korea, others). The report cites a large number of public documents.

CSIS reports on existing counterspace capabilities from multiple countries that include:

**Direct ascent ASAT**

**Rendezvous and proximity operations (RPO) / co-orbital ASAT**

**Blinding/damaging of optical sensors**

**High-altitude nuclear detonation**

**RF jamming on uplink/downlink frequencies**

**GPS jamming and spoofing**

**Cyber attacks against “secure networks” and control systems**

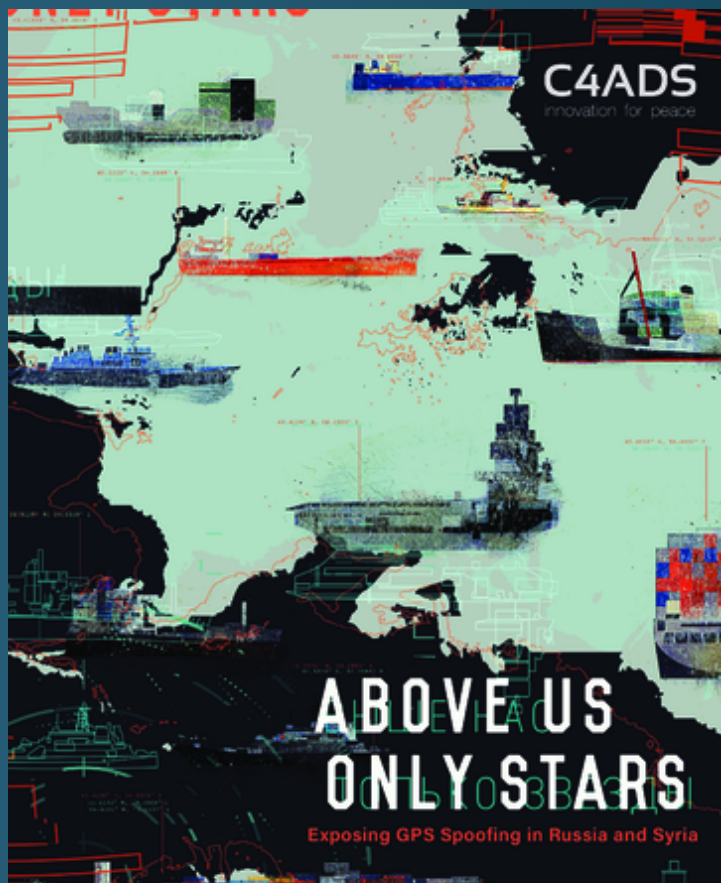
- Reference to a public report asserting cyber attackers gained access to satellite control systems

<https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf>

SPACE ASSET PROTECTION PROGRAM



## C4ADS: Above Us Only Stars (March, 2019)



<https://c4ads.org/s/Above-Us-Only-Stars.pdf>

In-depth report examining ~10k GNSS spoofing events from 2016 – 2018 across 10 locations. Attributes the sources as from the Russian Federation, and provides additional analysis and context on apparent intended uses.

The report principally focuses on GPS, not other GNSS. Some data obtained from a GPS receiver deployed on a science experiment module on the ISS.

Many maritime vessels affected by past GPS spoofing events, appearing to be positioned at an airport, similar to past reporting of spoofing in Russia.

(p. 7) Notional diagram how a GNSS spoofer might affect a maritime vessel.

(p. 10) Provides an overview of published experimental spoofing methodologies and effects.

(p. 20) Provides information on 10 discrete sites demonstrating widespread deployment of spoofing systems.

(p. 35) Cites a report suggesting one mode of operation jams L2 and L5 signals to force receivers to migrate to the L1 signal, where spoofing is performed.

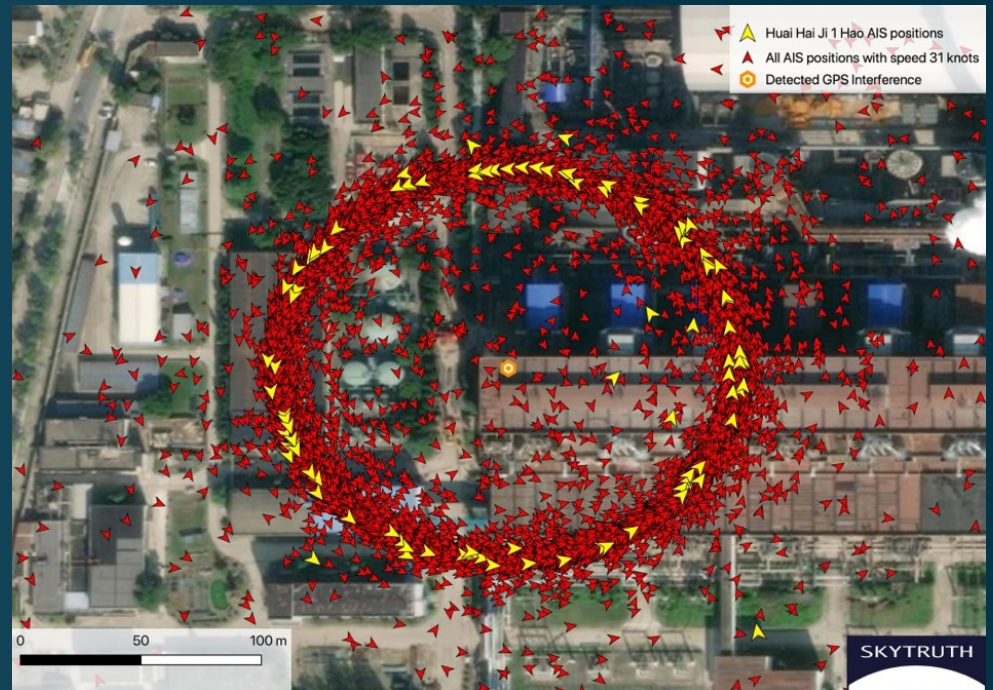
# Additional C4ADS Collaborations regarding GNSS Spoofing

## MIT Technology Review: Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai

- <https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/>  
[Mark Harris, November 15, 2019]
- Describes multiple instances of GPS spoofing in China where the spoofed signals move in a circle around a dedicated point

## SkyTruth.org: Systematic GPS Manipulation Occuring at Chinese Oil Terminals and Government Installations

- <https://skytruth.org/2019/12/systematic-gps-manipulation-occurring-at-chinese-oil-terminals-and-government-installations/>  
[Bjorn Bergman, December 12, 2019]
- Provides more precise information and locations of the GPS spoofing circles in China



# Defense Intelligence Agency (DIA): Challenges to Security In Space (February 2019)



**In-depth summary of key space topics, capabilities, and associated threats, including weapons systems**

- Captures DIA's perspective of other nations' perspective on space, including: Strategy, Doctrine, and Intent; Key Space and Counterspace Organizations; and Space and Counterspace Capabilities

**The report notes that:**

**Chinese and Russian military doctrines indicate they view space as important to modern warfare and counterspace capabilities as a means to reduce U.S. and allied military effectiveness.**

**Both countries have developed robust and capable space services, including space-based intelligence, surveillance and reconnaissance.**

**China and Russia are making improvements to existing systems including space launch vehicles and satellite navigation constellations.**

**These capabilities provide their militaries with the ability to command and control their forces worldwide with enhanced situational awareness, enabling them to monitor, track and target U.S. and allied forces.**

**Chinese and Russian space surveillance networks are capable of searching, tracking and characterizing satellites in all earth orbits. This capability supports both space operations and counterspace systems.**

**Both states are developing jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities and ground-based antisatellite missiles that can achieve a range of reversible to non-reversible effects.**

[https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space\\_Threat\\_V14\\_020119\\_sm.pdf](https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf)

SPACE ASSET PROTECTION PROGRAM



# National Air and Space Intelligence Center (NASIC): Competing in Space (December 2018)



“This publication identifies developing trends in the space domain, details growing challenges posed by foreign space assets, characterizes threats to U.S. and allied use of space, and presents an outlook for the evolution of these trends.”

## Summary trends:

- Space is Contested, Congested, and Competitive
- Space-Based Capabilities are Vulnerable
- Space is Increasingly Militarized
- International Norms Remain Elusive
- Technology Proliferation Driving the Increase in Competitive Space Actors

## Threat categories for “denying space” include:

- Space Situational Awareness
- Cyber and Electronic Threats
- Anti-satellite Missiles and Directed-Energy Weapons
- Space-Based Weapons

<https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF>

# Center for Strategic and International Studies (CSIS) Space Threat Assessment 2018 (April 2018)



The report provides a readable introduction to four categories of counterspace weapons (kinetic physical, non-kinetic physical, electronic, cyber), and then reviews the known capabilities of other nations (China, Russia, Iran, North Korea, others). The report cites a large number of public documents.

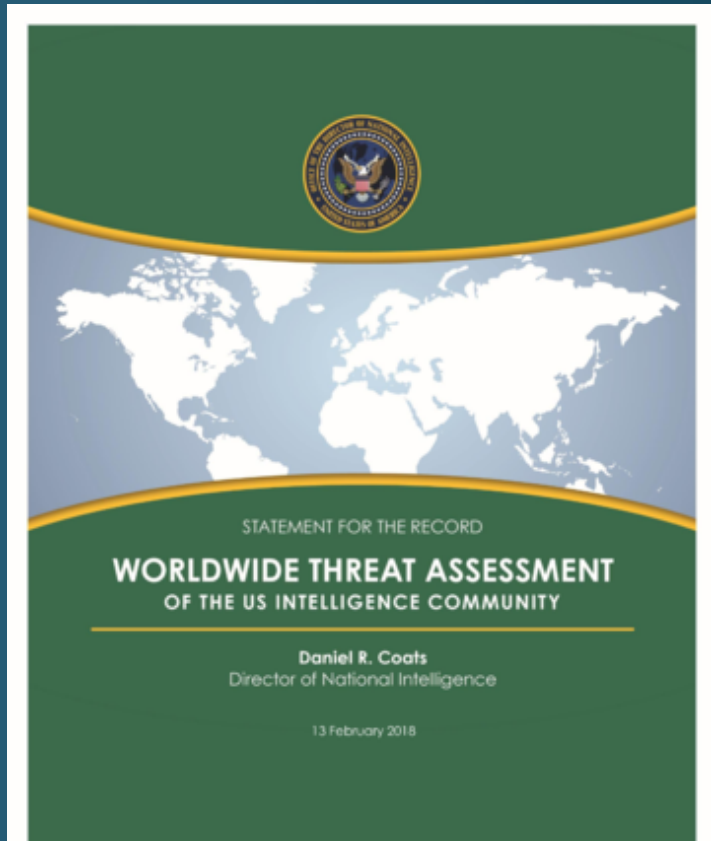
## Some passages related to NASA, NOAA, and USGS:

- (p. 8) “In 2008, a Chinese spacecraft deployed a miniature imaging satellite, the BX-1, that positioned itself in orbit around its mother spacecraft. After the successful deployment of the BX-1 and establishment of close orbit around the larger spacecraft, reports speculate that the BX-1 then maneuvered to intercept the **International Space Station (ISS)**, passing within 45 km of the station without providing prior notification.”
- (p. 11) [box: 2014 NOAA Satellite Hack] “In September 2014, Chinese hackers attacked **National Oceanographic and Atmospheric Administration (NOAA)** satellite information and weather systems. These critical systems are used by the U.S. military and other U.S. government agencies. The attack forced NOAA to take down the system and stop transmitting satellite images to the National Weather Service for two days before the organization was able to seal off the vital data.”
- (p. 11) “China has already been implicated or suspected in several cyberattacks against U.S. satellites. In October 2007 and again in July 2008, cyberattacks believed to originate in China targeted a remote sensing satellite operated by the **U.S. Geological Survey** called **Landsat-7**. Each attack caused 12 or more minutes of interference with ground station communications, but attackers did not gain control over the satellite. In June and October of 2008, hackers also believed to be from China attacked **NASA’s Terra Earth observation satellite**. In these attacks, the hackers ‘achieved all steps required to command the satellite but did not issue commands.’”

• NOTE: The source documents do not attribute the attacks to China.

<https://www.csis.org/analysis/space-threat-assessment-2018>

# DNI: Worldwide Threat Assessment of the US Intelligence Community (February 2018)



**Summary coverage of threats across a broad set of threat areas, including “cyber”, emerging and disruptive technology, and space and counterspace**

## **Space and Counterspace threat**

- Multiple nations pursuing increased and expanded access to space-based services and capabilities
- Multiple nations pursuing antisatellite (ASAT) weapons, both destructive and nondestructive
  - Destructive capabilities reaching initial operating capacity in the next few years (as of 2018)
- Potential for US space systems (military, civil, or commercial) to be attacked in a conflict

<https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>