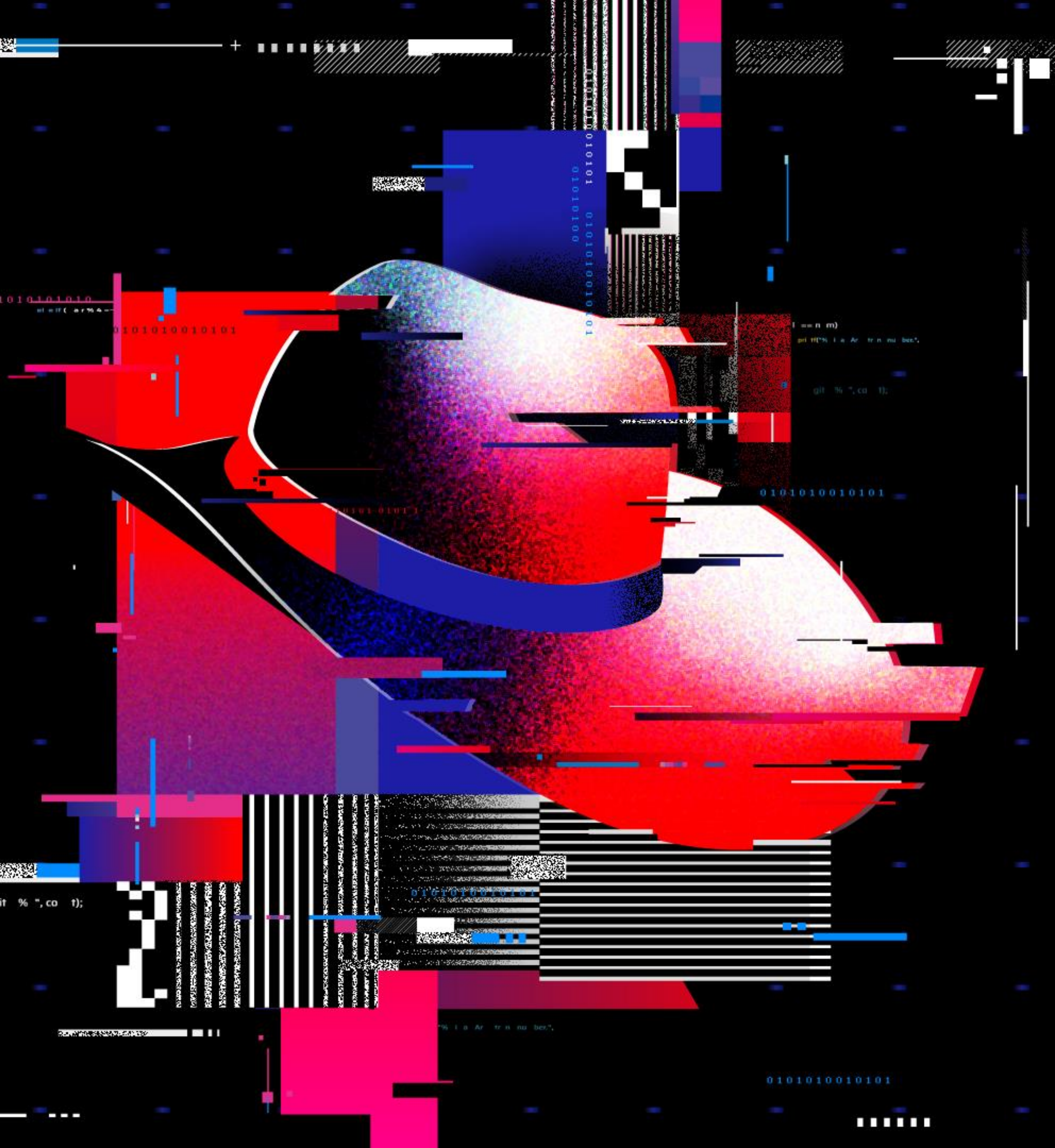
# Adventures in *Cyber* Space

## An Introduction to Satellite Cybersecurity

James Pavur



* Opinions expressed are solely my own and do not express the views or opinions of my employer

# The Ultimate High Ground

*“Control of space[...] means control of the world [...] Whoever gains that ultimate position gains control, total control, over the earth, for purposes of tyranny or for the service of freedom.”*

**Lindon B. Johnson -** January 1958

# 0

Space Wars to Date

# Roadmap

The Peace Puzzle

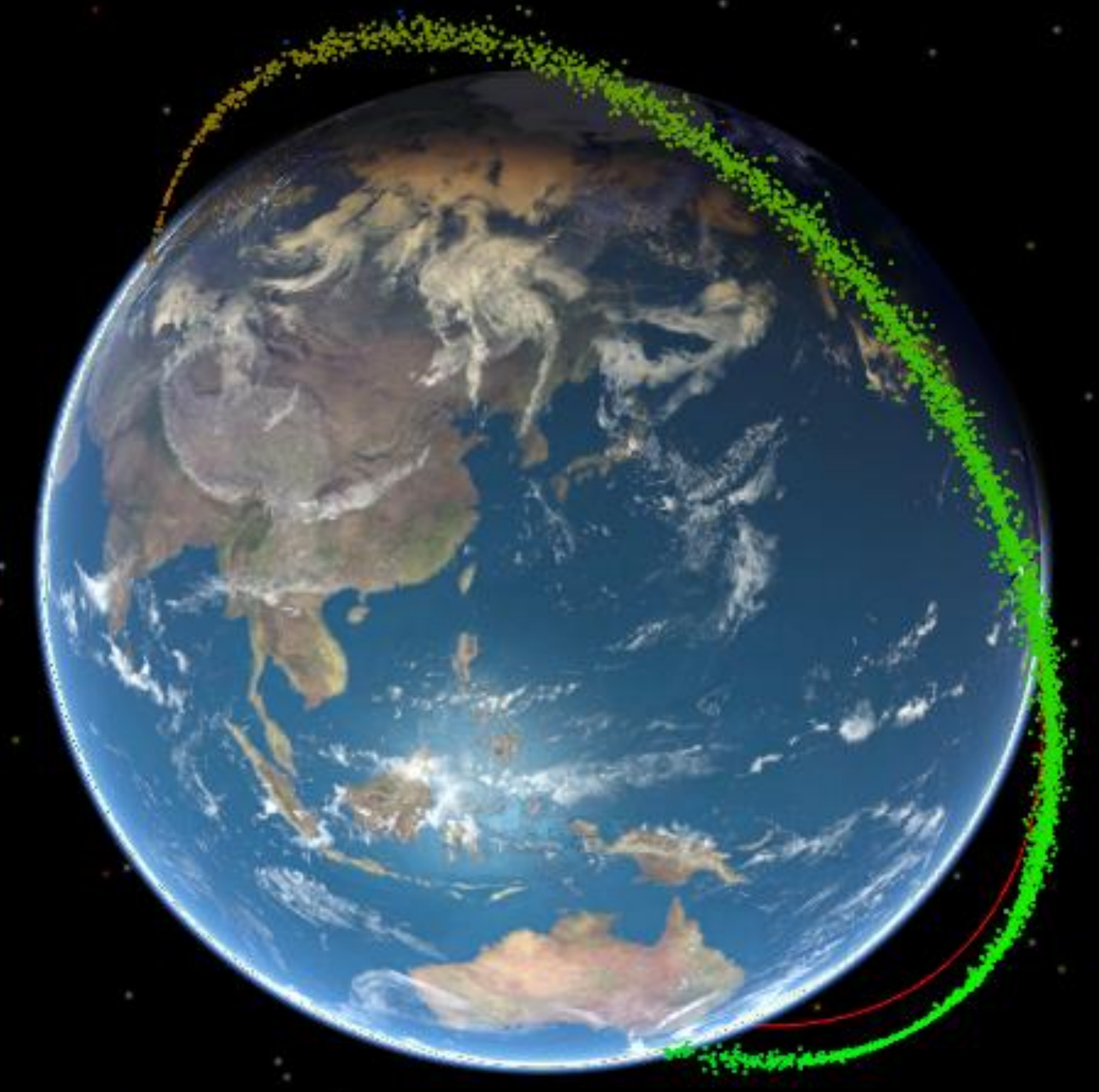
- Cyber's Impact

State-Level Case Study

- SSA Deception

Non-State Case Study

- SIGINT for Cheap



# The Cyber ASAT

## Will Space Stay Peaceful?

# Accessibility

Image : Press Information Bureau of India. http://pib.nic.in. ID: 139905

# Accessibility

*Kinetic-ASAT*

- Only 9 or 10 countries with orbital launch capabilities.

*Cyber-ASAT*

# Accessibility

*Kinetic-ASAT*

- Only 9 or 10 countries with orbital launch capabilities.

*Cyber-ASAT*

- All countries (and most non-state threats) have access to cyberspace.

# Accessibility

## *Kinetic-ASAT*

- Only 9 or 10 countries with orbital launch capabilities.
- Only 4 countries with offensive ASATs (China, US, Russia, India).

## *Cyber-ASAT*

- All countries (and most non-state threats) have access to cyberspace.

# Accessibility

## *Kinetic-ASAT*

- Only 9 or 10 countries with orbital launch capabilities.
- Only 4 countries with offensive ASATs (China, US, Russia, India).

## *Cyber-ASAT*

- All countries (and most non-state threats) have access to cyberspace.
- 100s of countries with offensive cyber-capabilities

# Accessibility

## *Kinetic-ASAT*

- Only 9 or 10 countries with orbital launch capabilities.
- Only 4 countries with offensive ASATs (China, US, Russia, India).
- Cost of meaningful capacity: $ billions.

## *Cyber-ASAT*

- All countries (and most non-state threats) have access to cyberspace.
- 100s of countries with offensive cyber-capabilities

# Accessibility

## *Kinetic-ASAT*

- Only 9 or 10 countries with orbital launch capabilities.
- Only 4 countries with offensive ASATs (China, US, Russia, India).
- Cost of meaningful capacity: $ billions.

## *Cyber-ASAT*

- All countries (and most non-state threats) have access to cyberspace.
- 100s of countries with offensive cyber-capabilities
- Cost of meaningful capacity: $ thousands.

# Norms & Deterrence

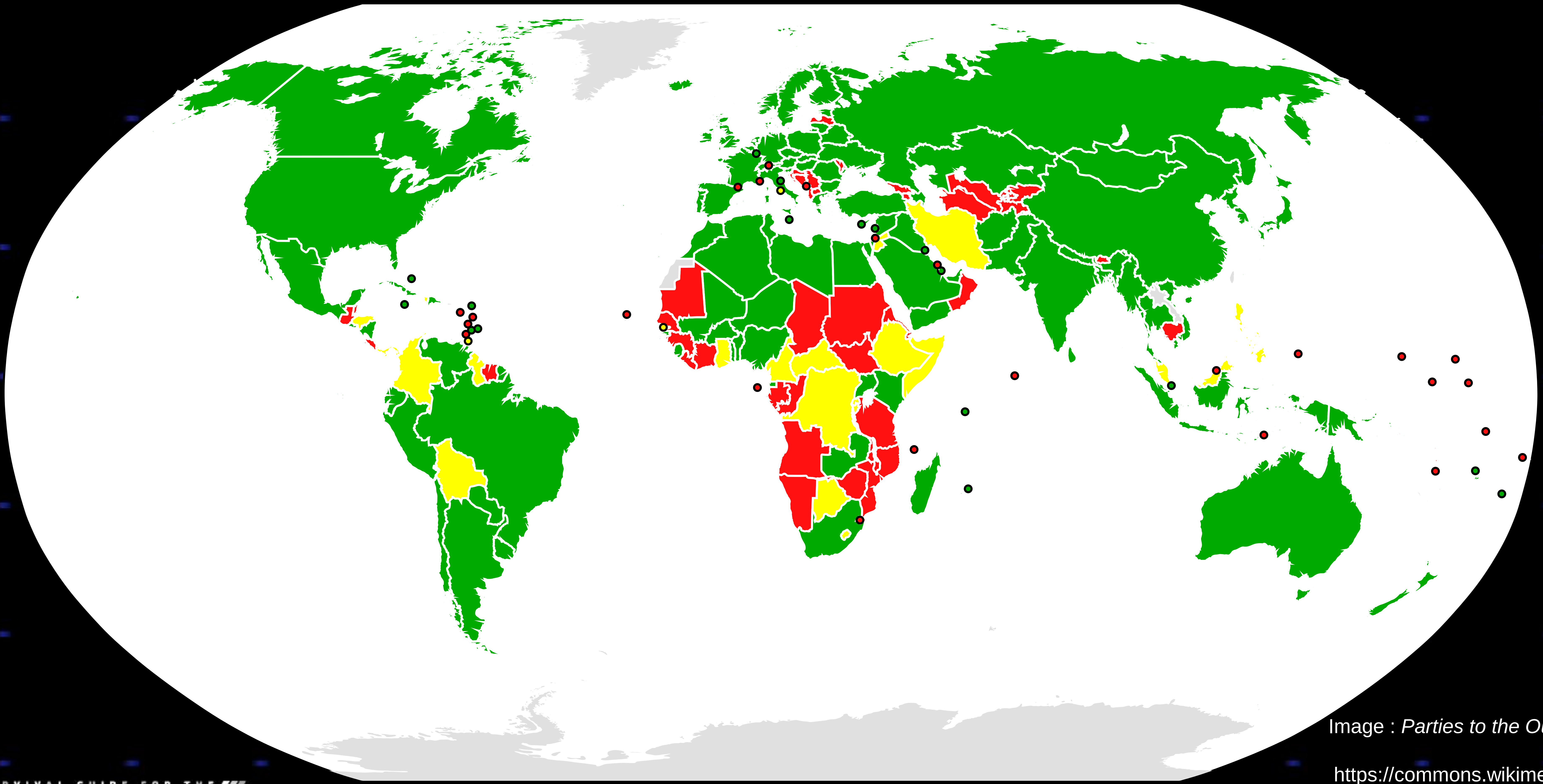


Image : *Parties to the Outer Space Treaty (CC-BY-SA-2.5)*
https://commons.wikimedia.org/wiki/File:Outer_Space_Treaty_parties.svg

# Norms & Deterrence

## *Kinetic-ASAT*

- Codified (50+ years) and widely adopted (100+ parties) legal regime.

## *Cyber-ASAT*

# Norms & Deterrence

## *Kinetic-ASAT*

- Codified (50+ years) and widely adopted (100+ parties) legal regime.

## *Cyber-ASAT*

- No comparable international legal regime.

# Norms & Deterrence

*Kinetic-ASAT*

- Codified (50+ years) and widely adopted (100+ parties) legal regime.
- States cautious when “pushing boundaries” within regime.

*Cyber-ASAT*

- No comparable international legal regime.

# Norms & Deterrence

## *Kinetic-ASAT*

- Codified (50+ years) and widely adopted (100+ parties) legal regime.
- States cautious when "pushing boundaries" within regime.

## *Cyber-ASAT*

- No comparable international legal regime.
- States and non-state actors have large appetite for precedence-breaking.

# Norms & Deterrence

*Kinetic-ASAT*

- Codified (50+ years) and widely adopted (100+ parties) legal regime.
- States cautious when “pushing boundaries” within regime.
- Attack attribution is immediate, easy, and provable.

*Cyber-ASAT*

- No comparable international legal regime.
- States and non-state actors have large appetite for precedence-breaking.

# Norms & Deterrence

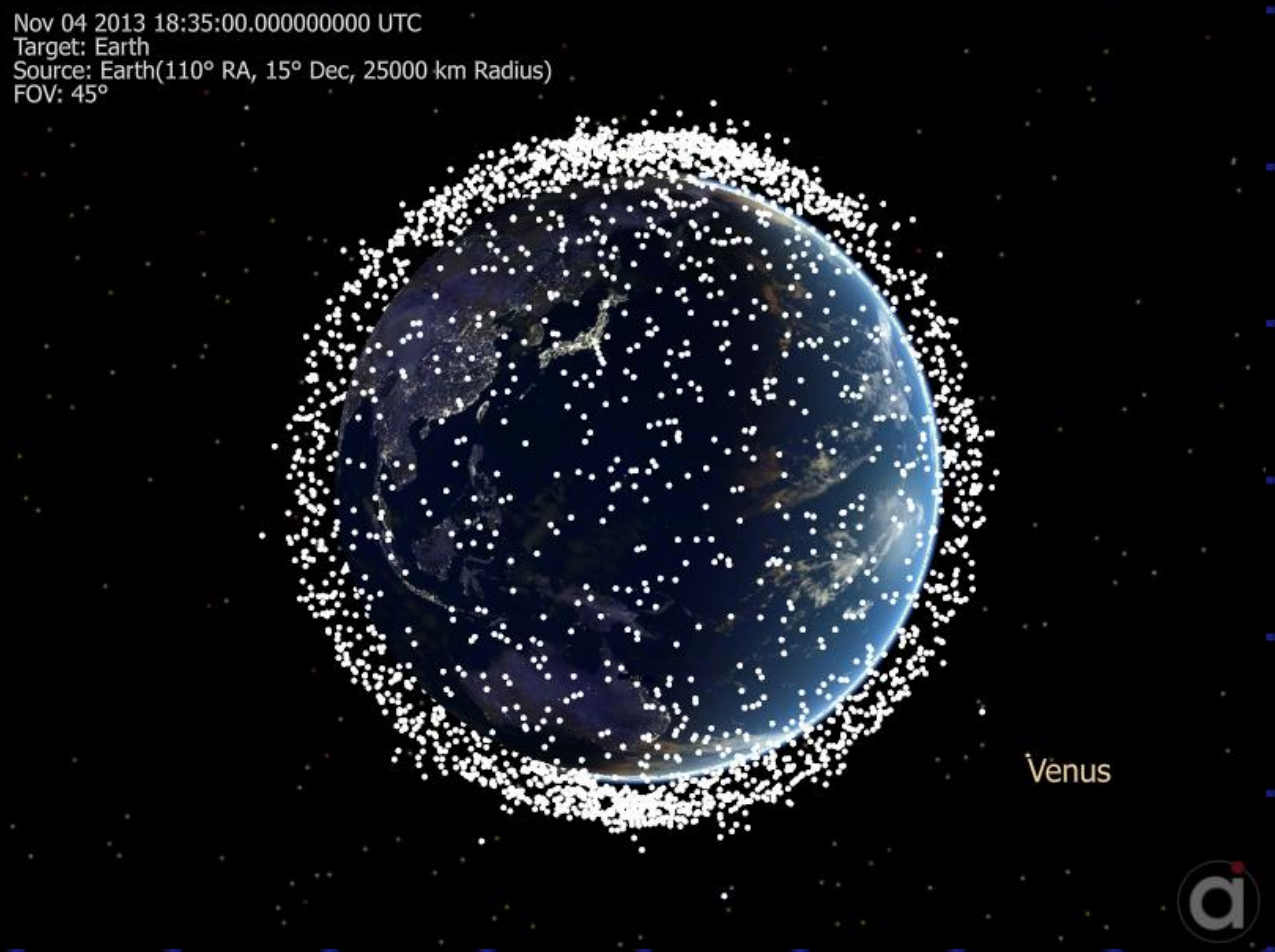
*Kinetic-ASAT*

- Codified (50+ years) and widely adopted (100+ parties) legal regime.
- States cautious when “pushing boundaries” within regime.
- Attack attribution is immediate, easy, and provable.

*Cyber-ASAT*

- No comparable international legal regime.
- States and non-state actors have large appetite for precedence-breaking.
- Attack attribution is slow, difficult, and uncertain.

# Environment



Nov 04 2013 18:35:00.000000000 UTC
Target: Earth
Source: Earth(110° RA, 15° Dec, 25000 km Radius)
FOV: 45°

# Environment

*Kinetic-ASAT*

- High risk of collateral damage from generated debris field.

*Cyber-ASAT*

# Environment

*Kinetic-ASAT*

- High risk of collateral damage from generated debris field.

*Cyber-ASAT*

- Possibility of “zero-debris” counterspace capabilities.

# Environment

## *Kinetic-ASAT*

- High risk of collateral damage from generated debris field.
- Long term (multi-decadal) consequences from cascade.

## *Cyber-ASAT*

- Possibility of "zero-debris" counterspace capabilities.

# Environment

*Kinetic-ASAT*

- High risk of collateral damage from generated debris field.
- Long term (multi-decadal) consequences from cascade.

*Cyber-ASAT*

- Possibility of “zero-debris” counterspace capabilities.
- Generally short-term and precise effects from given exploit.

# Environment

## *Kinetic-ASAT*

- High risk of collateral damage from generated debris field.
- Long term (multi-decadal) consequences from cascade.
- All feasible attackers are participants in the environment.

## *Cyber-ASAT*

- Possibility of "zero-debris" counterspace capabilities.
- Generally short-term and precise effects from given exploit.

# Environment

## *Kinetic-ASAT*

- High risk of collateral damage from generated debris field.
- Long term (multi-decadal) consequences from cascade.
- All feasible attackers are participants in the environment.

## *Cyber-ASAT*

- Possibility of “zero-debris” counterspace capabilities.
- Generally short-term and precise effects from given exploit.
- Many attackers do not have space capabilities or dependencies.

# Theory ✓

Cyber-ASAT is a threat when:

- Uses accessible technology
- Is difficult to detect/attribute
- Avoids collateral damage

# Theory ✓

Cyber-ASAT is a threat when:

- Uses accessible technology
- Is difficult to detect/attribute
- Avoids collateral damage

# Practice ?

# Case Study: SSA Deception

## Who Knows What's Out There?

# Space Situational Awareness

SSA = Data describing the state of orbit

- Includes both satellites and debris

Myriad uses

- Mission Planning
- Conjunction Analysis
- Coverage and Contact Analysis
- Research
- Intelligence / National Security

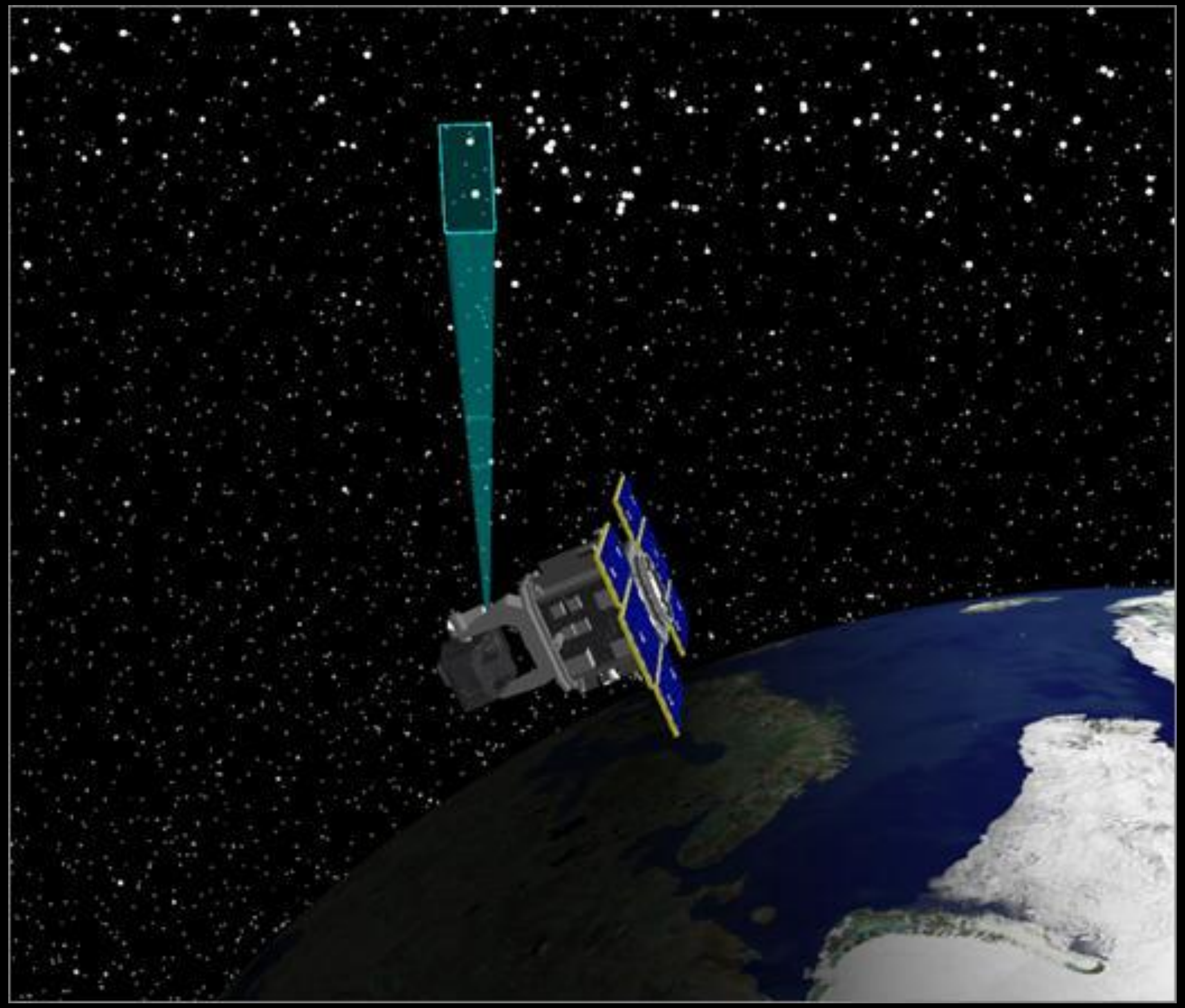
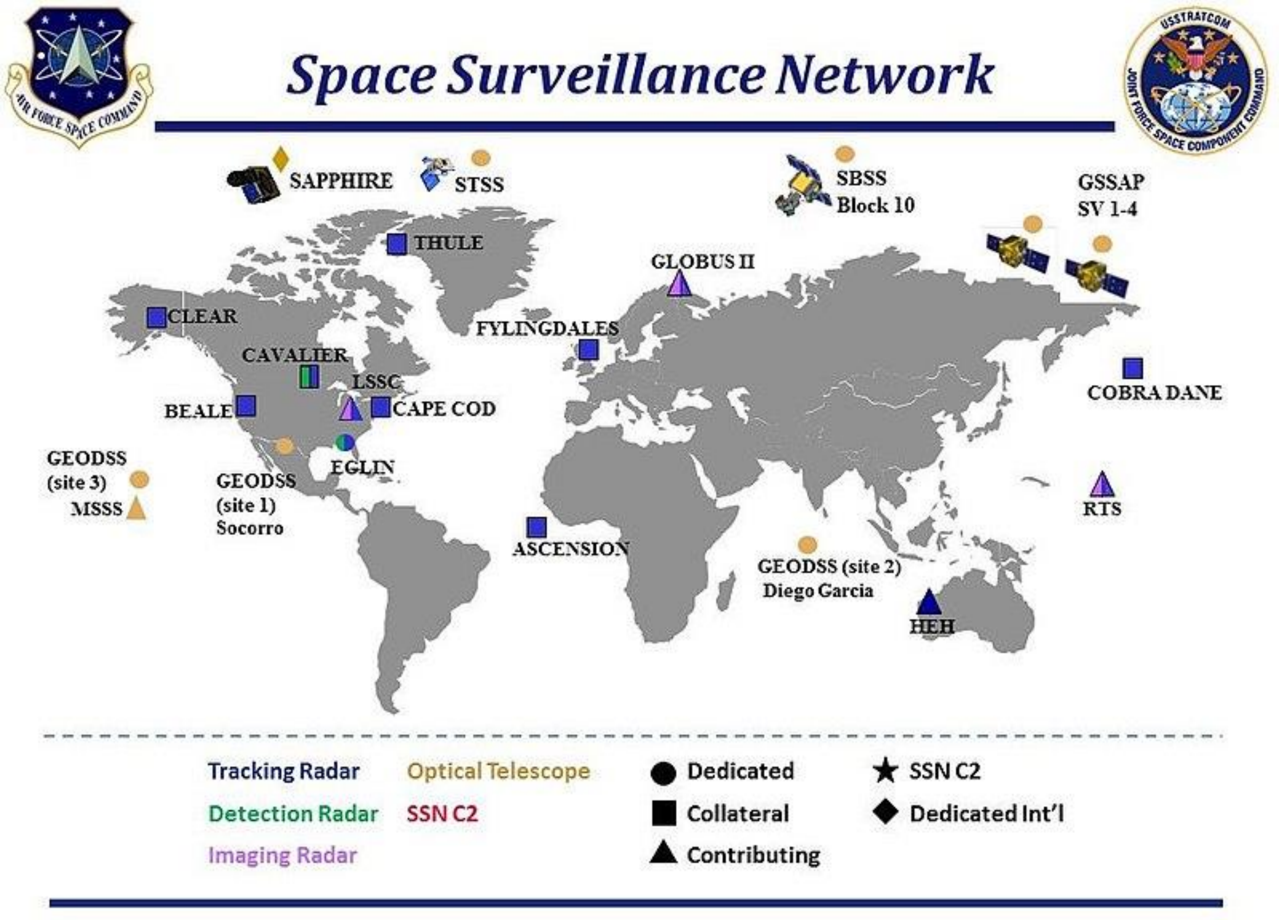
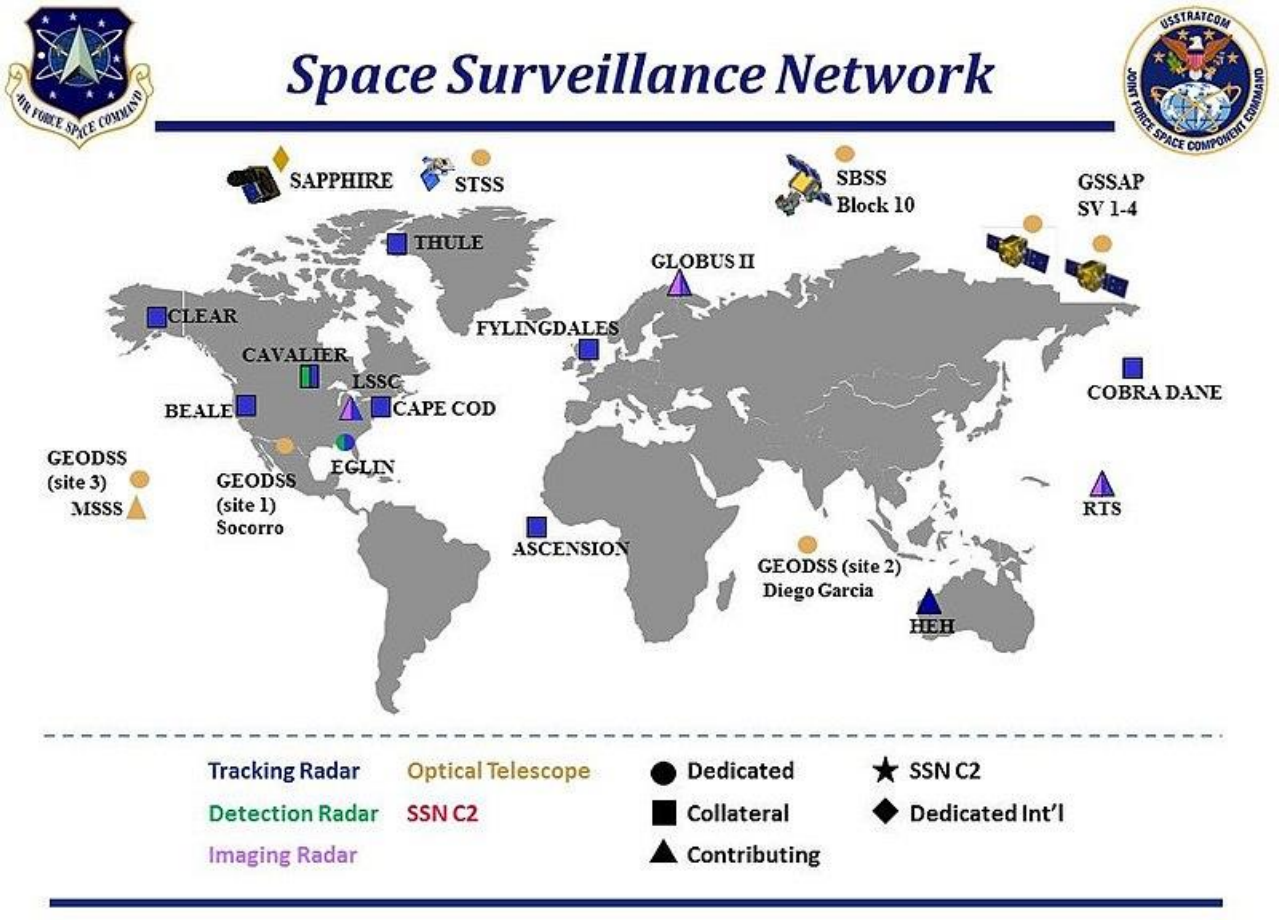


Image: AF Space Operations, US Air Force, Public Domain.

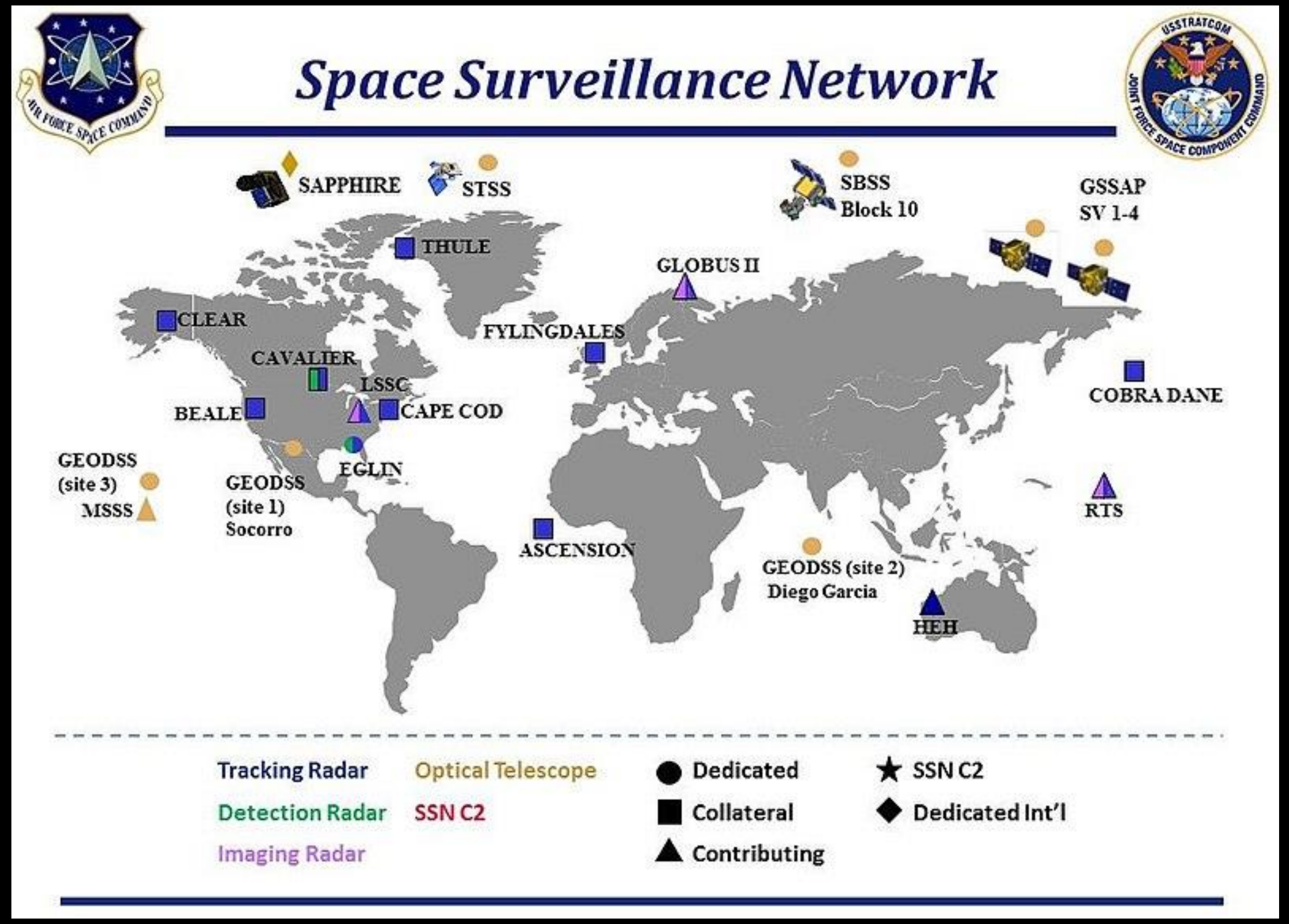
# Space Surveillance Systems



# Space Surveillance Systems

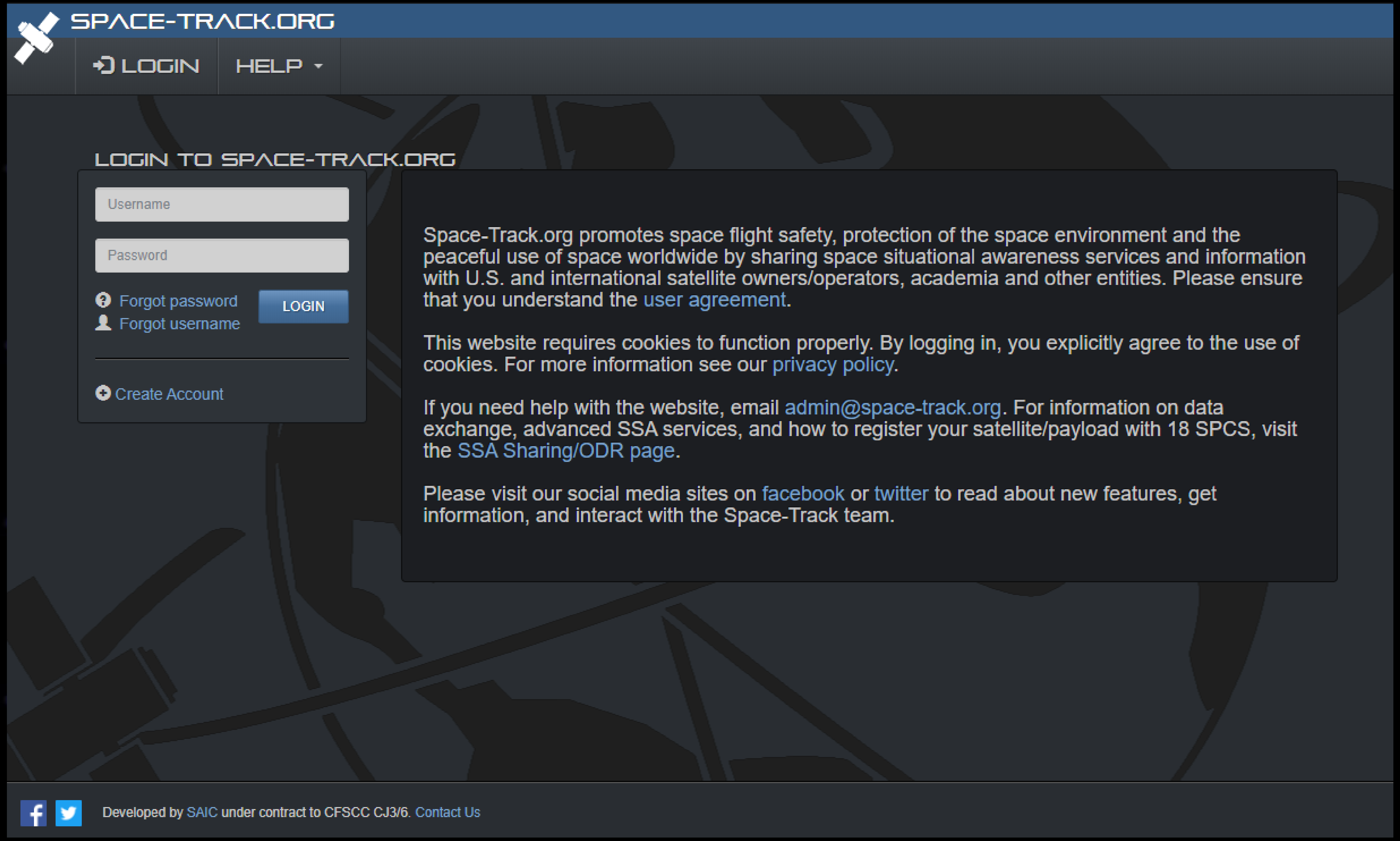


# Space Surveillance Systems



# Everyone Else

- Limited domestic capabilities in many countries
  - Notably: EU, Japan, India, Korea, Canada, Kazakhstan and Ukraine
- New commercial entrants
  - Unclear how credible coverage/capacity predictions are
- In practice: use public data shared by SSN through space-track.org



LOGIN TO SPACE-TRACK.ORG

Username

Password

Forgot password

Forgot username

LOGIN

Create Account

Space-Track.org promotes space flight safety, protection of the space environment and the peaceful use of space worldwide by sharing space situational awareness services and information with U.S. and international satellite owners/operators, academia and other entities. Please ensure that you understand the user agreement.

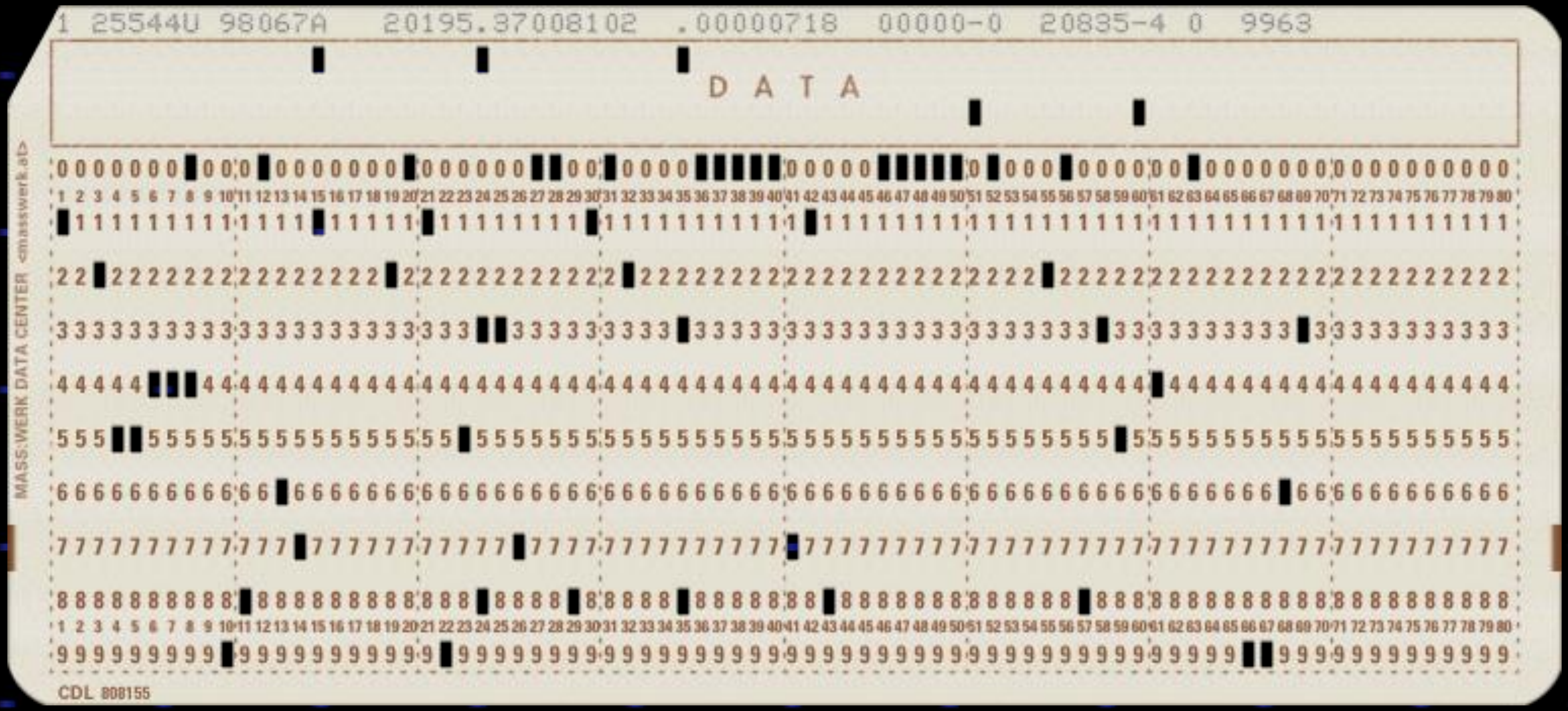
This website requires cookies to function properly. By logging in, you explicitly agree to the use of cookies. For more information see our privacy policy.

If you need help with the website, email admin@space-track.org. For information on data exchange, advanced SSA services, and how to register your satellite/payload with 18 SPCS, visit the SSA Sharing/ODR page.

Please visit our social media sites on facebook or twitter to read about new features, get information, and interact with the Space-Track team.

Developed by SAIC under contract to CFSCC CJ3/6. Contact Us

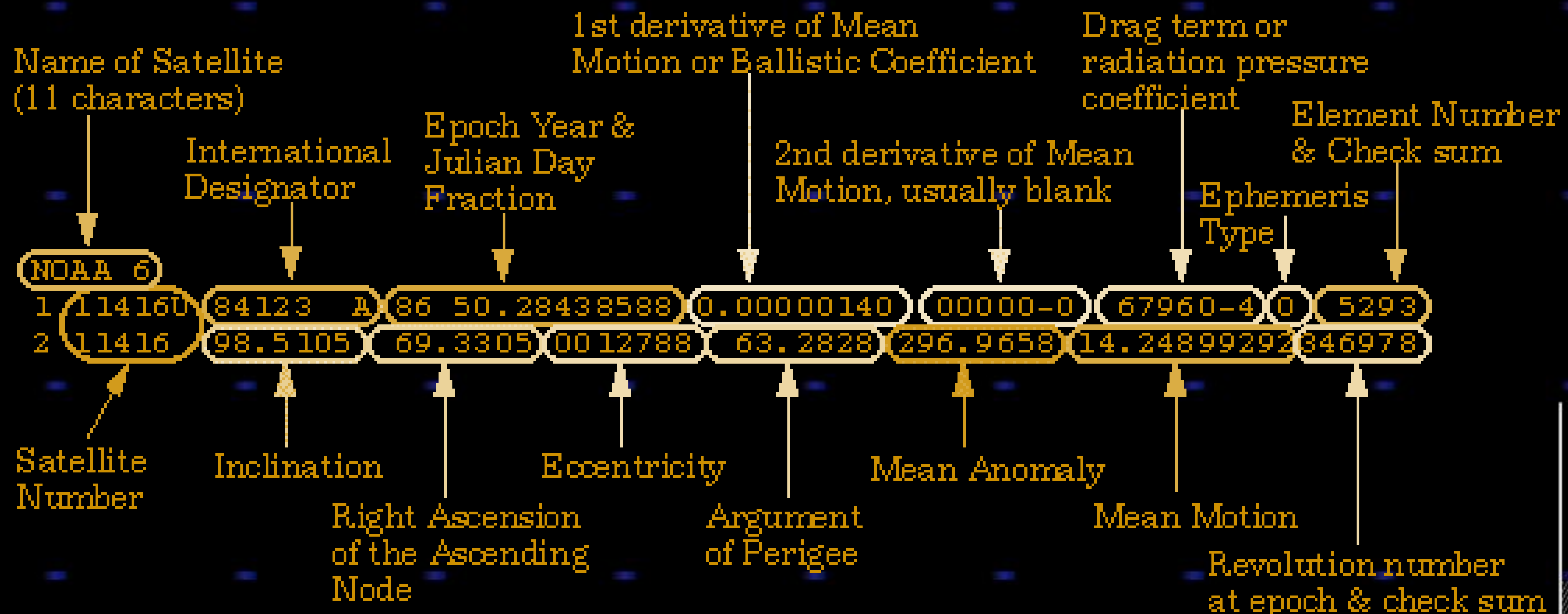
# Two Line Elements (TLE)



```
1 25544U 98067A   20195.37008102 .00000718  00000-0  20835-4 0  9963
```

# Everyone Else

- Describes key orbital elements
  - Combined with SGP4 propagator, can predict location of object in near future
- Main format shared by Space-Track.org
  - Better data available under Data Sharing Agreements


Name of Satellite (11 characters)
International Designator
Epoch Year & Julian Day Fraction
1st derivative of Mean Motion or Ballistic Coefficient
2nd derivative of Mean Motion, usually blank
Drag term or radiation pressure coefficient
Ephemeris Type
Element Number & Check sum
NOAA 6
1 11416U 84123 A 86 50.28438588 0.00000140 00000-0 67960-4 0 5293
2 11416 98.5105 69.3305 0012788 63.2828 296.9658 14.24899292346978
Satellite Number
Inclination
Right Ascension of the Ascending Node
Eccentricity
Argument of Perigee
Mean Anomaly
Mean Motion
Revolution number at epoch & check sum

# Why Target SSA?

Highly Centralized

Most Users Cannot Verify

Soft Target

Hard Effects

# Threat Actors

## Repository Owner

- It’s your data, just lie about it

## Nation State Attacker

- Compromise space surveillance sensors

## Individual/Organized Attacker

- Compromise central repository (“*Just” a Database*)

# Attacker Goals

Conceal Impending Collision

Animation: Space debris 2017 – a journey to Earth. ESA. CC BY-SA 3.0.

Fake Impending Collision

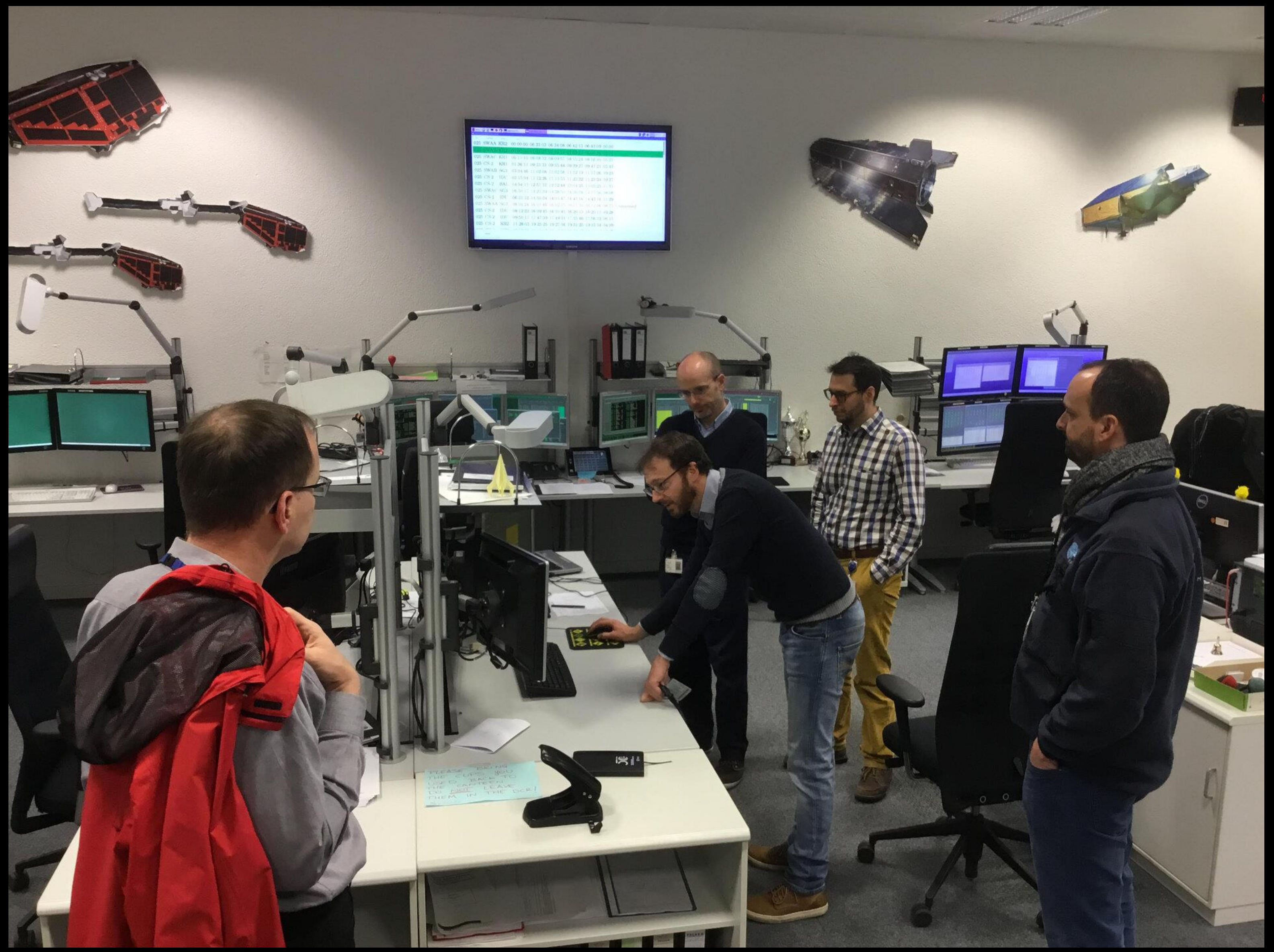


Image: Debris avoidance manoeuvre. ESA. CC BY-SA 3.0.

# Attack Assumptions

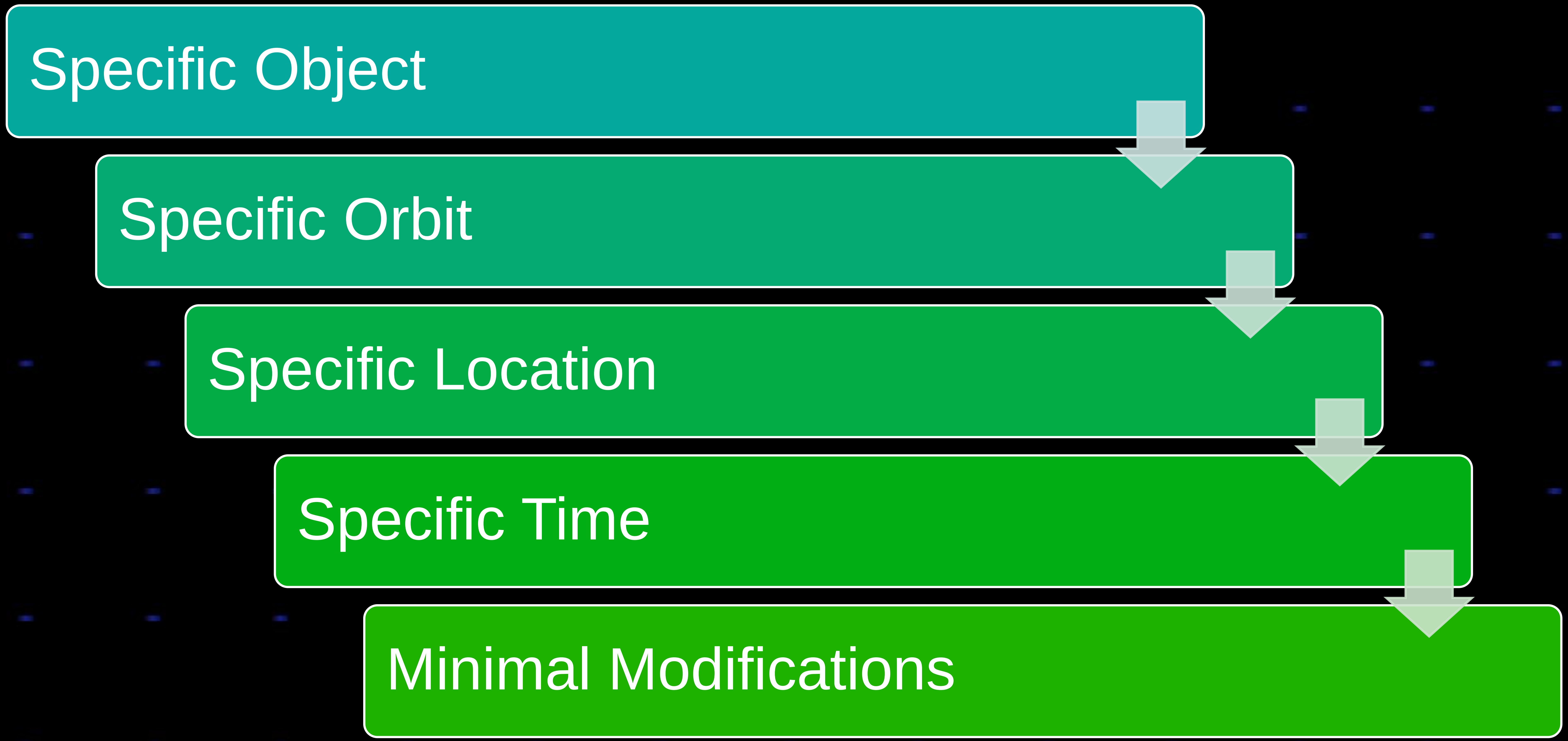
Database has been compromised

✓ TLEs used for conjunction analysis (not recommended)

✗ No additional sensing requested / granted

<1km pass = conjunction event

# Tampering Requirements



Specific Object

Specific Orbit

Specific Location

Specific Time

Minimal Modifications

eeFlyer Mission 7.5.1.53911 (Nanosecond) - candidate_finder - [Output]

ile
Options
Workspace
Window
Help
Home
Control
Output
Notes
kspace 24
sionView 51
1/5
Jul 15 2020 01:35:17.081000000
MissionView 51

atus Message: The Mission Plan executed successfully.

Status: Stopped

Run Duration: 648 s

eeFlyer Mission 7.5.1.53911 (Nanosecond) - candidate_finder - [Output]
ile
Options
Workspace
Window
Help
Home
Control
Output
Notes
kspace 24
ionView 51
1/5
MissionView 51

Jul 15 2020 01:35:17.081000000

atus Message: The Mission Plan executed successfully.

Status: Stopped

Run Duration: 648 s

eeFlyer Mission 7.5.1.53911 (Nanosecond) - candidate_finder - [Output]
ile
Options
Workspace
Window
Help
Home
Control
Output
Notes
kspace 24
sionView 51
1/5
MissionView 51

Jul 15 2020 01:35:17.081000000

atus Message: The Mission Plan executed successfully.

Status: Stopped

Run Duration: 648 s

eeFlyer Mission 7.5.1.53911 (Nanosecond) - candidate_finder - [Output]
ile
Options
Workspace
Window
Help
Home
Control
Output
Notes
kspace 24
sionView 51
1/5
MissionView 51

Jul 15 2020 01:35:17.081000000

atus Message: The Mission Plan executed successfully.

Status: Stopped

Run Duration: 648 s

FreeFlyer Mission 7.5.1.53911 (Nanosecond) - candidate_finder - [Output]
File
Options
Workspace
Window
Help
Home
Control
Output
Notes
Workspace 24
MissionView 51
1/5
Jul 15 2020 01:35:17.081000000
MissionView 51
Console
Output Properties

Status Message: The Mission Plan executed successfully.

Status: Stopped

Run Duration: 648 s

FreeFlyer Mission 7.5.1.53911 (Nanosecond) - candidate_finder - [Output]
File
Options
Workspace
Window
Help
Home
Control
Output
Notes
Workspace 24
MissionView 51
1/5
Jul 15 2020 05:36:37.0810000
Console
Console

```
9998.000000000 Objects tracked
Conjuncting with : 35806
Conjuction Time : Jul 14 2020 05:45:07.
Range at TCA :   454.754407341km
Conjuncting with : 44607
Conjuction Time : Jul 14 2020 05:51:37.
Range at TCA :   172.387343934km
Conjuncting with : 34756
Conjuction Time : Jul 14 2020 06:15:27.
Range at TCA :    29.449340883km
Conjuncting with : 41156
Conjuction Time : Jul 14 2020 09:55:37.
Range at TCA :    29.306746574km
Conjuncting with : 34554
Conjuction Time : Jul 14 2020 10:04:57.
Range at TCA :    25.630729804km
Conjuncting with : 29810
Conjuction Time : Jul 14 2020 18:27:27.
Range at TCA :    24.319405398km
Conjuncting with : 32422
Conjuction Time : Jul 14 2020 22:38:07.
Range at TCA :    22.520930216km
Conjuncting with : 30919
Conjuction Time : Jul 15 2020 00:00:57.
Range at TCA :     9.398392555km
Conjuncting with : 35647
Conjuction Time : Jul 15 2020 02:49:17.
Range at TCA :     3.845021183km
Simulation Complete
Object:  35647 Distance:   3.85 Time: 2
Object:  30919 Distance:   9.40 Time: 2
Object:  31720 Distance:  18.94 Time: 2
Object:  34672 Distance:  19.19 Time: 2
Object:  32422 Distance:  22.52 Time: 2
```

Status Message: The Mission Plan executed successfully.

Status: Stopped

Run Duration: 648

# Astrophysics = Hard, GA = Easy

**Individual**

```
1 35647U 00000AAA 20196.23387825  .00000000  00000-0  93745-4 0  9993
2 35647 074.0406 334.6387 0038654 196.2234 204.2792 14.32021286581048
```

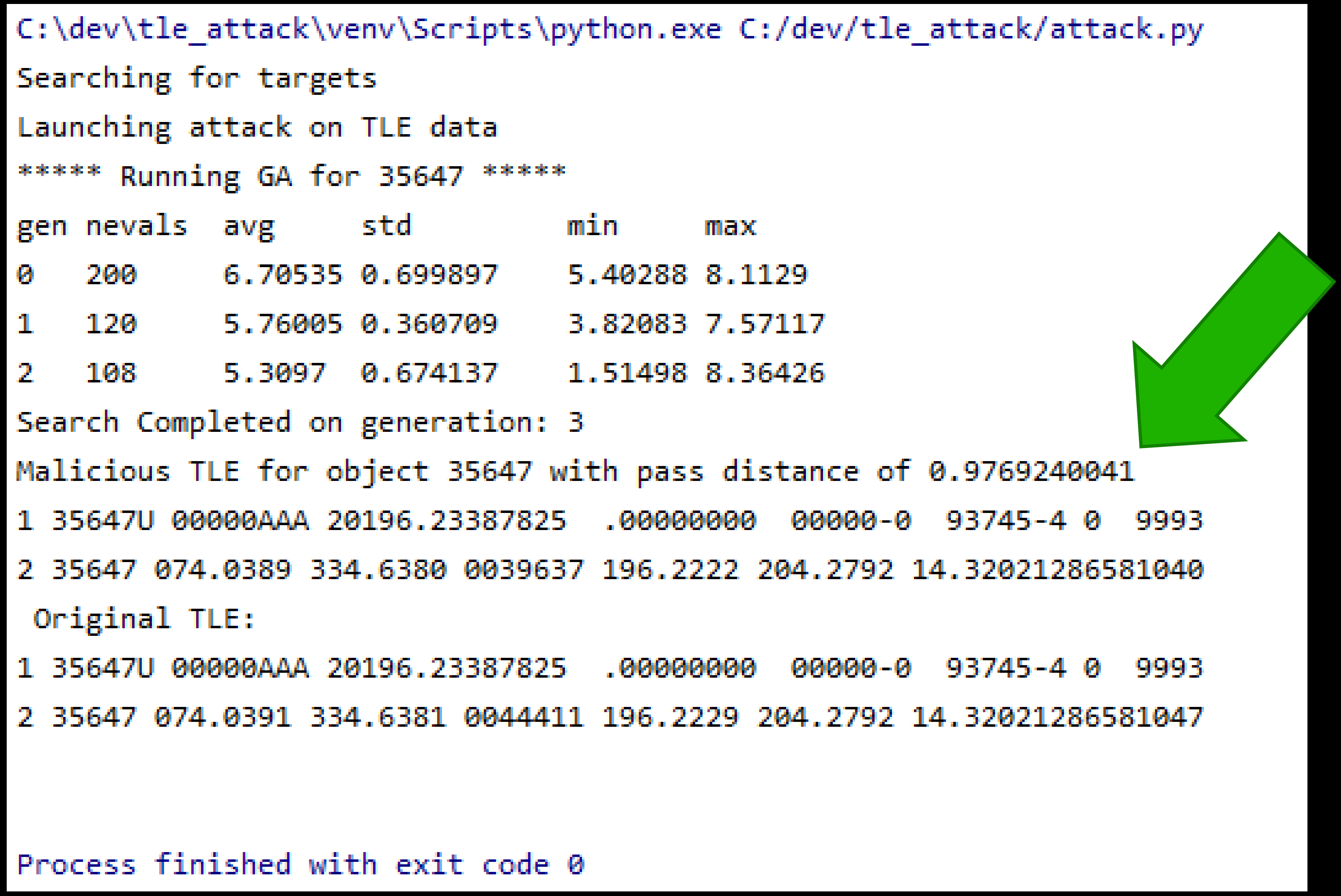
**Fitness**

Distance @ TCA ( + optional “stealth” metric)

**Stealth**

Bound @ ~10% alteration

# Genetic Algorithm Output



```
C:\dev\tle_attack\venv\Scripts\python.exe C:/dev/tle_attack/attack.py
Searching for targets
Launching attack on TLE data
***** Running GA for 35647 *****
gen nevals  avg     std         min     max
0   200     6.70535 0.699897    5.40288 8.1129
1   120     5.76005 0.360709    3.82083 7.57117
2   108     5.3097  0.674137    1.51498 8.36426
Search Completed on generation: 3
Malicious TLE for object 35647 with pass distance of 0.9769240041
1 35647U 00000AAA 20196.23387825  .00000000  00000-0  93745-4 0  9993
2 35647 074.0389 334.6380 0039637 196.2222 204.2792 14.32021286581040
 Original TLE:
1 35647U 00000AAA 20196.23387825  .00000000  00000-0  93745-4 0  9993
2 35647 074.0391 334.6381 0044411 196.2229 204.2792 14.32021286581047


Process finished with exit code 0
```

File
Options
Workspace
Window
Help
Home
Control
Output
Notes
Workspace 29
Workspace 30
Workspace 31
Workspace 32
Workspace 33
MissionView 71
MissionView 71
Mars
Neptune
IRIDIUM 106
Print
Export
All Output Properties...

Output Properties

Selected Component: MissionView 71

Viewpoint: Current: Default

View Mode: 3D View

Reference Frame: Body Fixed

Source: Earth

Source Offsets

Right Ascension: 270 deg

Declination: 20 deg

Translation: 30000 km

Field Of View: 45 deg

Target: Earth

Status Message:

Status: Running

Run Duration: 2 s

# SSA Case Takeaways

- Third-party SSA requires trust
- Abuse of this trust can be catastrophic
- External verification & state responsibility is key

# Case Study: SIGINT for Cheap

## Listening to the Sky

80
60
40
20
0
-20
-40
-60
-80
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160
Google Server
Ground Station
CargoVessel
Attacker
Comsat

80
60
40
20
0
-20
-40
-60
-80
Google Server
Ground Station
CargoVessel
Attacker
Comsat
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160

80
60
40
20
0
-20
-40
-60
-80
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160
Google Server
Ground Station
CargoVessel
Attacker
Comsat

80
60
Google Server
40
Ground Station
CargoVessel
20
Attacker
0
Comsat
-20
-40
-60
-80
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160

Google Server
Ground Station
CargoVessel
Attacker
Comsat
80
60
40
20
0
-20
-40
-60
-80
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160

GET google.com
Comsat

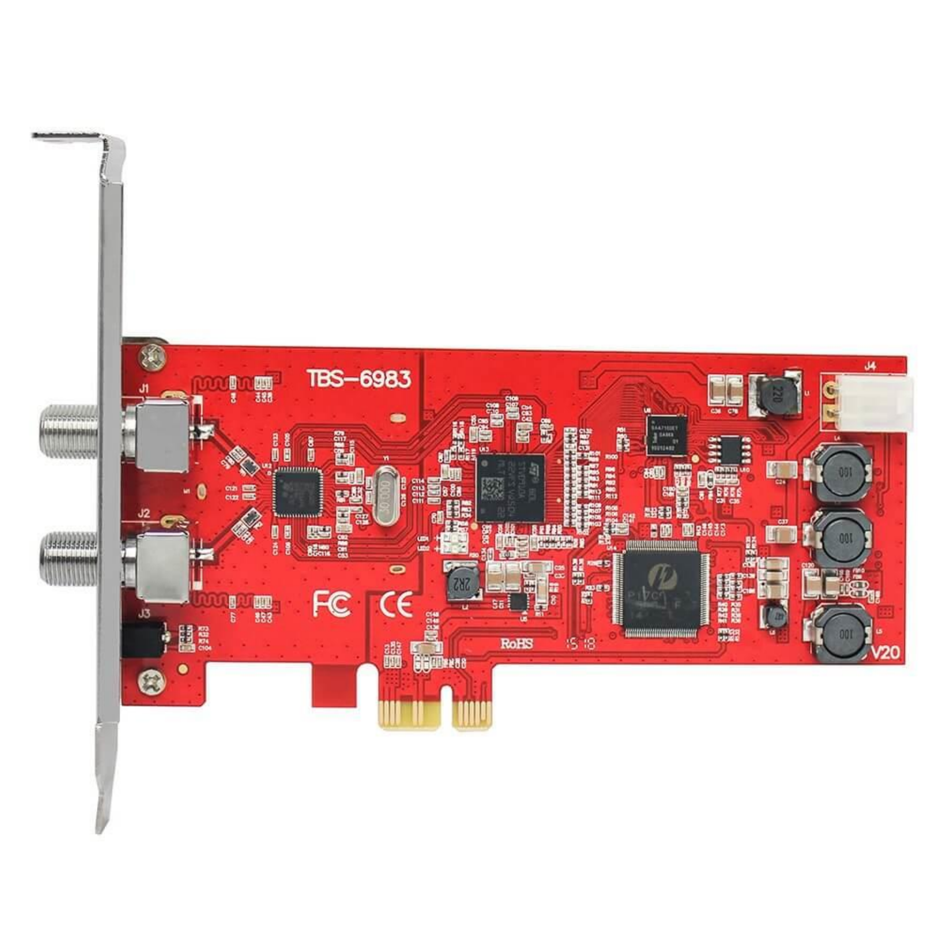
CargoVessel
Comsat

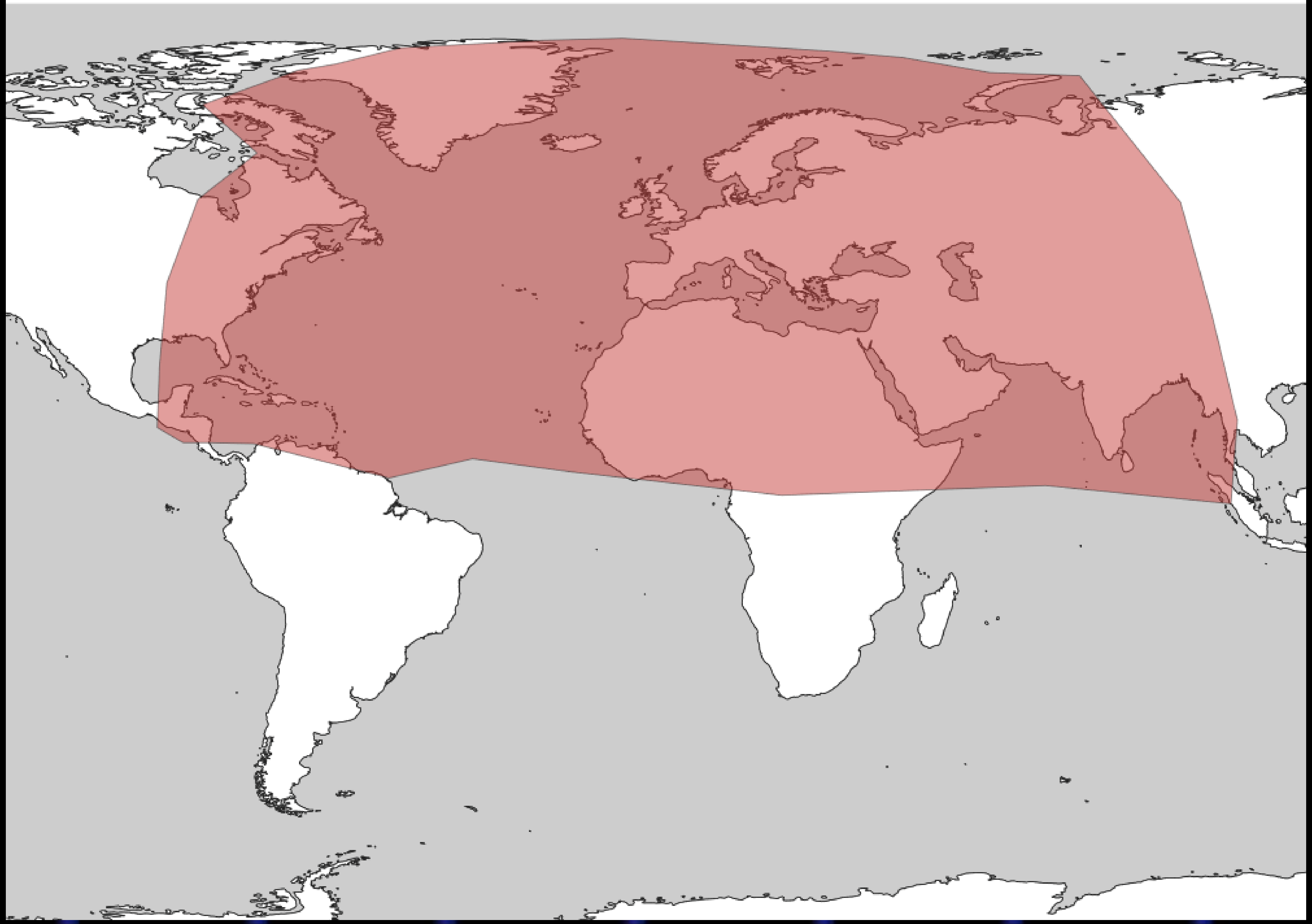
Ground Station
Comsat

Google Server
Ground Station

Comsat
Ground Station

# The Experiments





# Signal Challenges

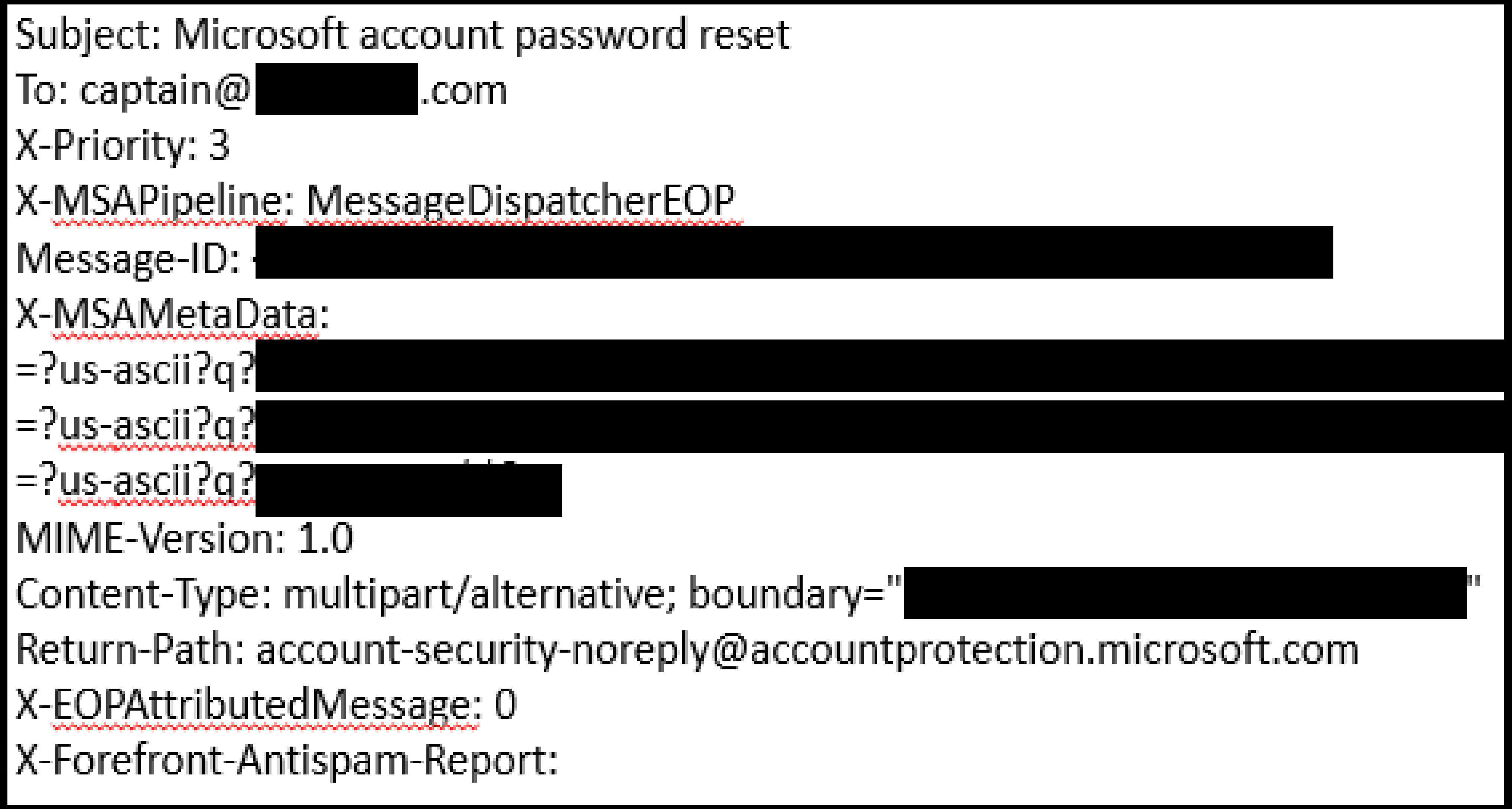
- Proper Equipment = Expensive
- Our Equipment -> Signal Errors
  - Complex modulations
  - Proprietary protocol modifications
- Solution: GSExtract
  - github.com/ssloxford/gsextract
  - Focus on the “easy” bits
  - Brute force is cheap
  - Accuracy not that important

# What’s Inside?

- $ 9 FORTUNE GLOBAL 500 MEMBERS
- ✈ 6 OF 10 LARGEST AIRLINES
- ⚓ ~40% MARITIME CARGO MARKET
- 🏛 GOVERNMENTAL AGENCIES
- 👥 YOU?

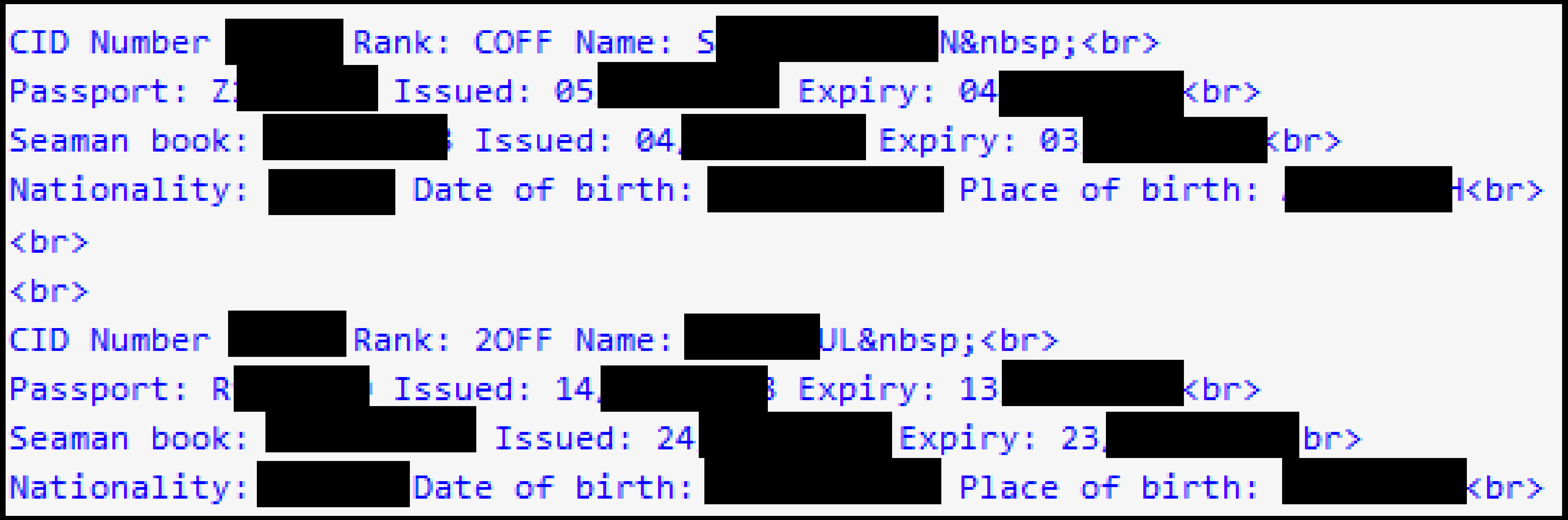
# Privacy

## Email Communications



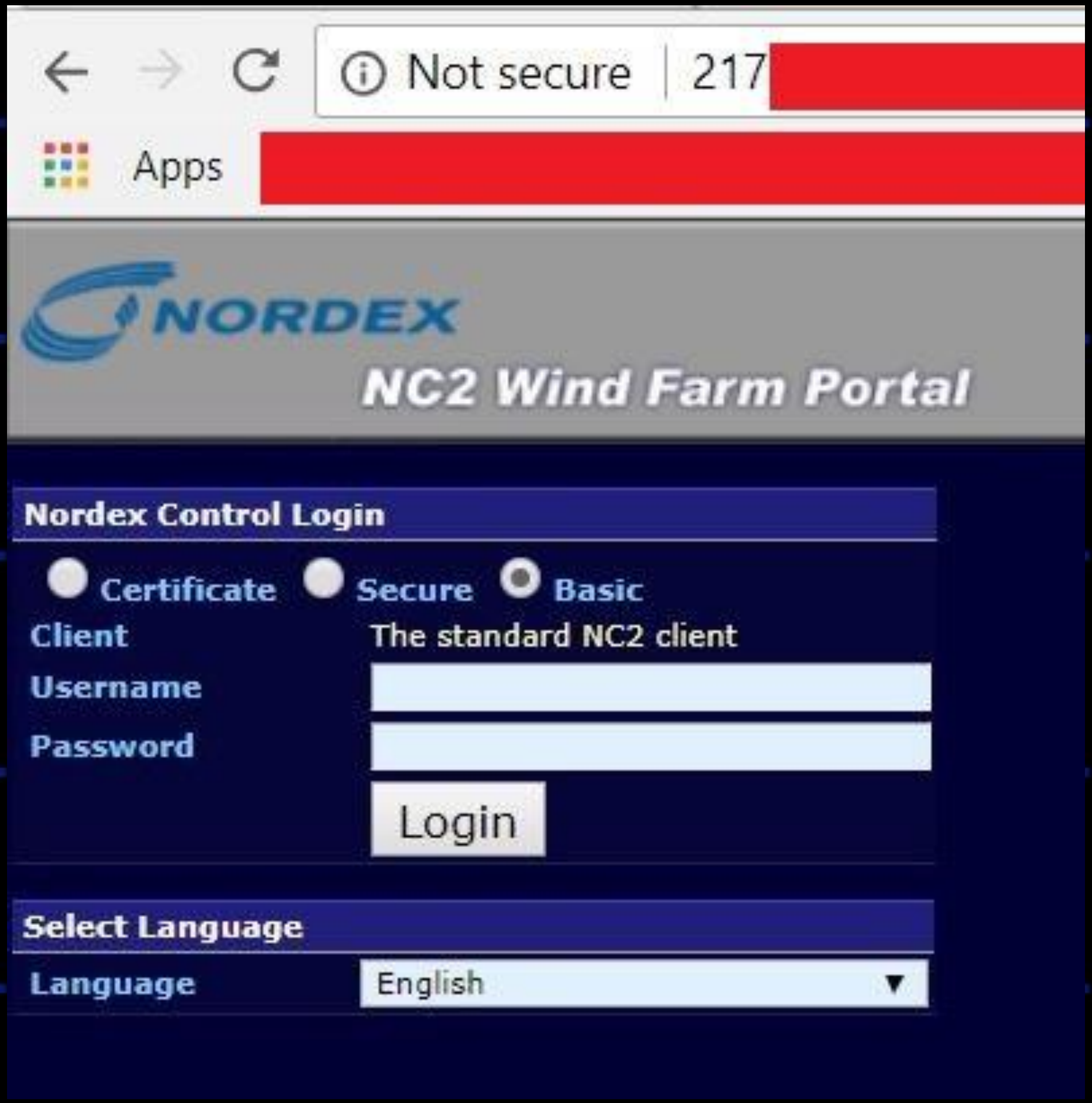
```
Subject: Microsoft account password reset
To: captain@[redacted].com
X-Priority: 3
X-MSAPipeline: MessageDispatcherEOP
Message-ID: [redacted]
X-MSAMetaData:
=?us-ascii?q?[redacted]
=?us-ascii?q?[redacted]
=?us-ascii?q?[redacted]
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="[redacted]"
Return-Path: account-security-noreply@accountprotection.microsoft.com
X-EOPAttributedMessage: 0
X-Forefront-Antispam-Report:
```

## Crew Passport Data



```
CID Number [redacted] Rank: COFF Name: S[redacted]N&nbsp;<br>
Passport: Z[redacted] Issued: 05[redacted] Expiry: 04[redacted]<br>
Seaman book: [redacted] Issued: 04[redacted] Expiry: 03[redacted]<br>
Nationality: [redacted] Date of birth: [redacted] Place of birth: [redacted]<br>
<br>
<br>
CID Number [redacted] Rank: 2OFF Name: [redacted]UL&nbsp;<br>
Passport: R[redacted] Issued: 14[redacted] Expiry: 13[redacted]<br>
Seaman book: [redacted] Issued: 24[redacted] Expiry: 23[redacted]br>
Nationality: [redacted]Date of birth: [redacted] Place of birth: [redacted]<br>
```

# IOT & Maritime



ⓘ Not secure | 217[redacted]

Apps [redacted]

NORDEX

NC2 Wind Farm Portal

**Nordex Control Login**

○ Certificate ○ Secure ● Basic

Client: The standard NC2 client

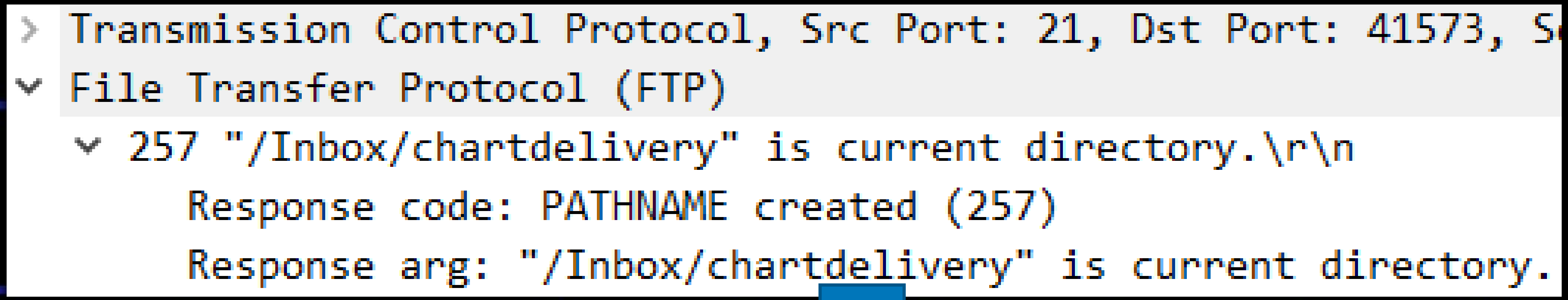
Username:

Password:

Login

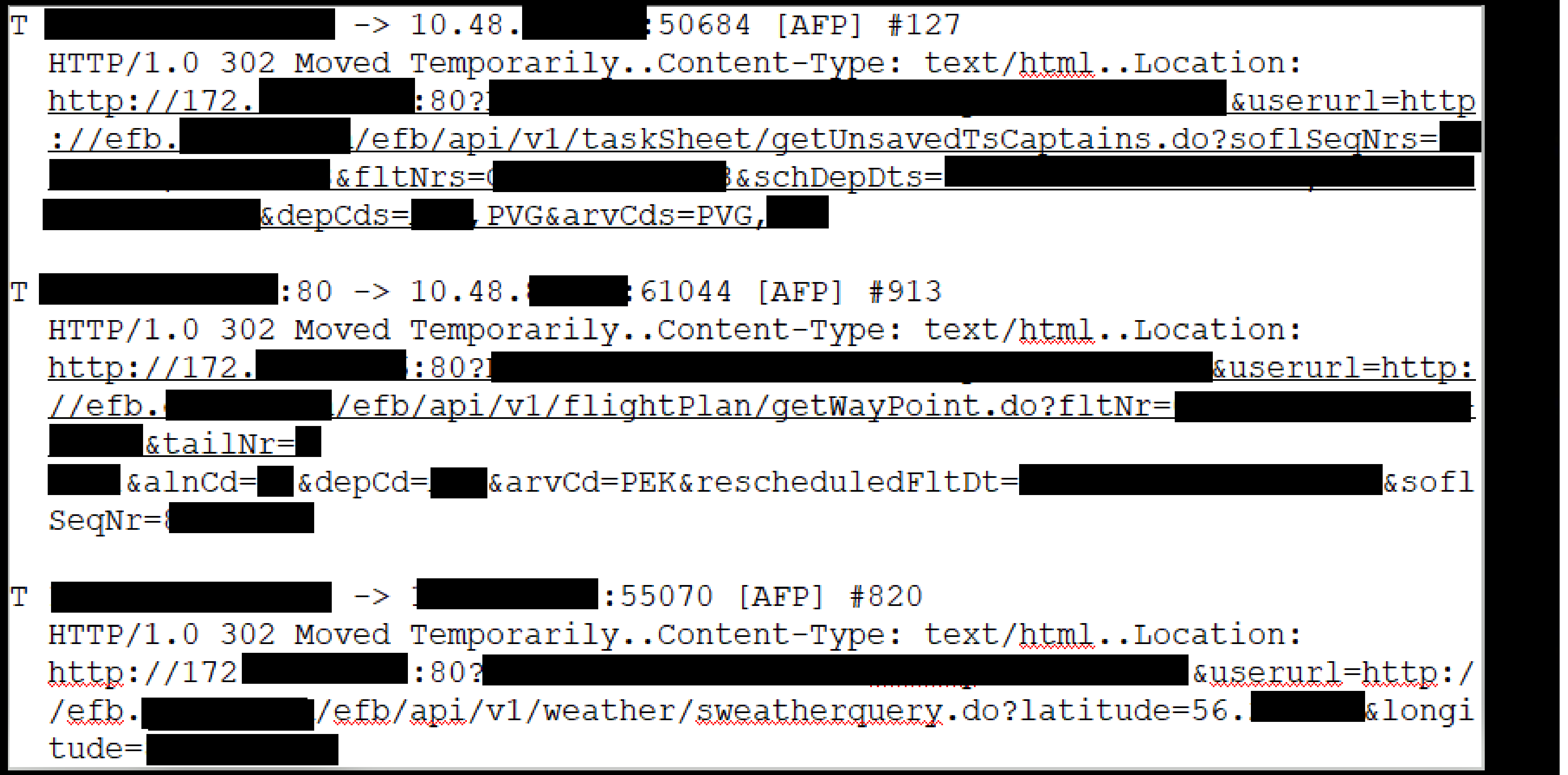
**Select Language**

Language: English ▼

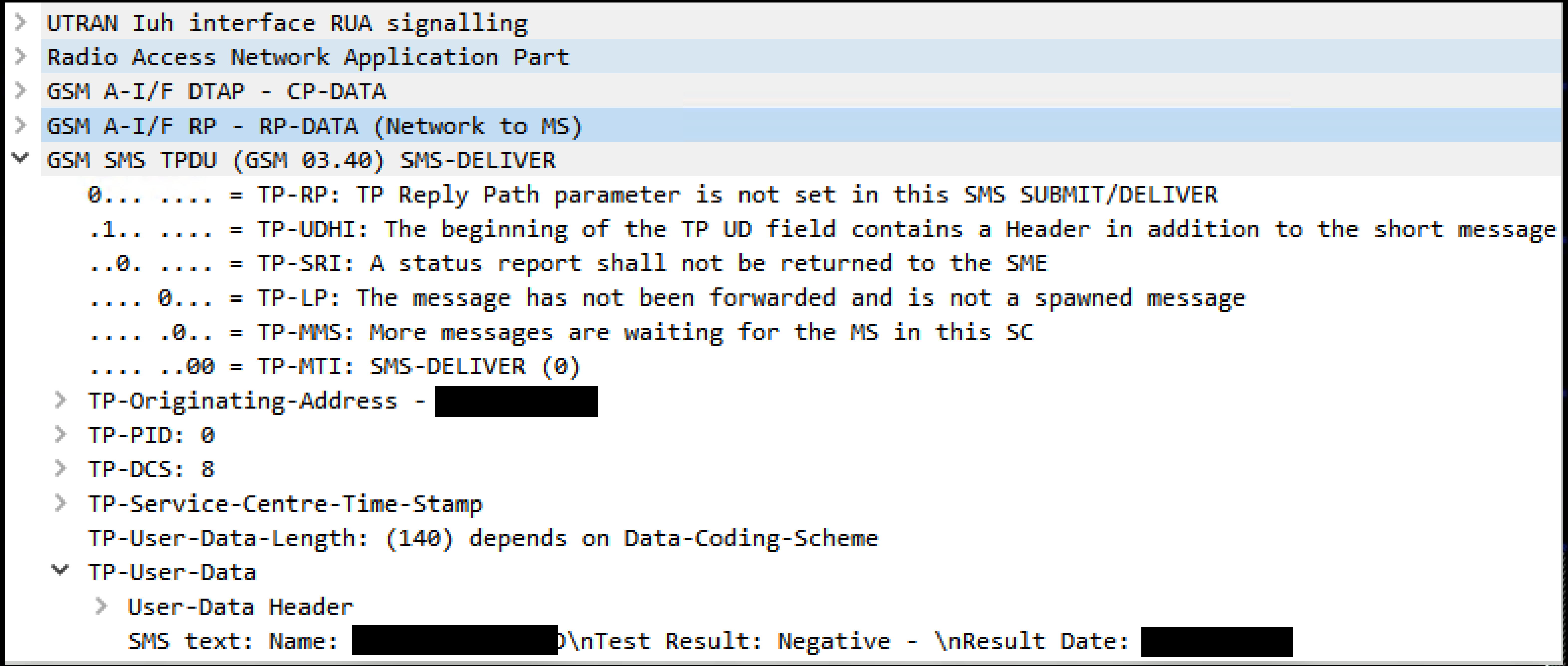


```
> Transmission Control Protocol, Src Port: 21, Dst Port: 41573, Se
v File Transfer Protocol (FTP)
  v 257 "/Inbox/chartdelivery" is current directory.\r\n
      Response code: PATHNAME created (257)
      Response arg: "/Inbox/chartdelivery" is current directory.
```

# Aviation



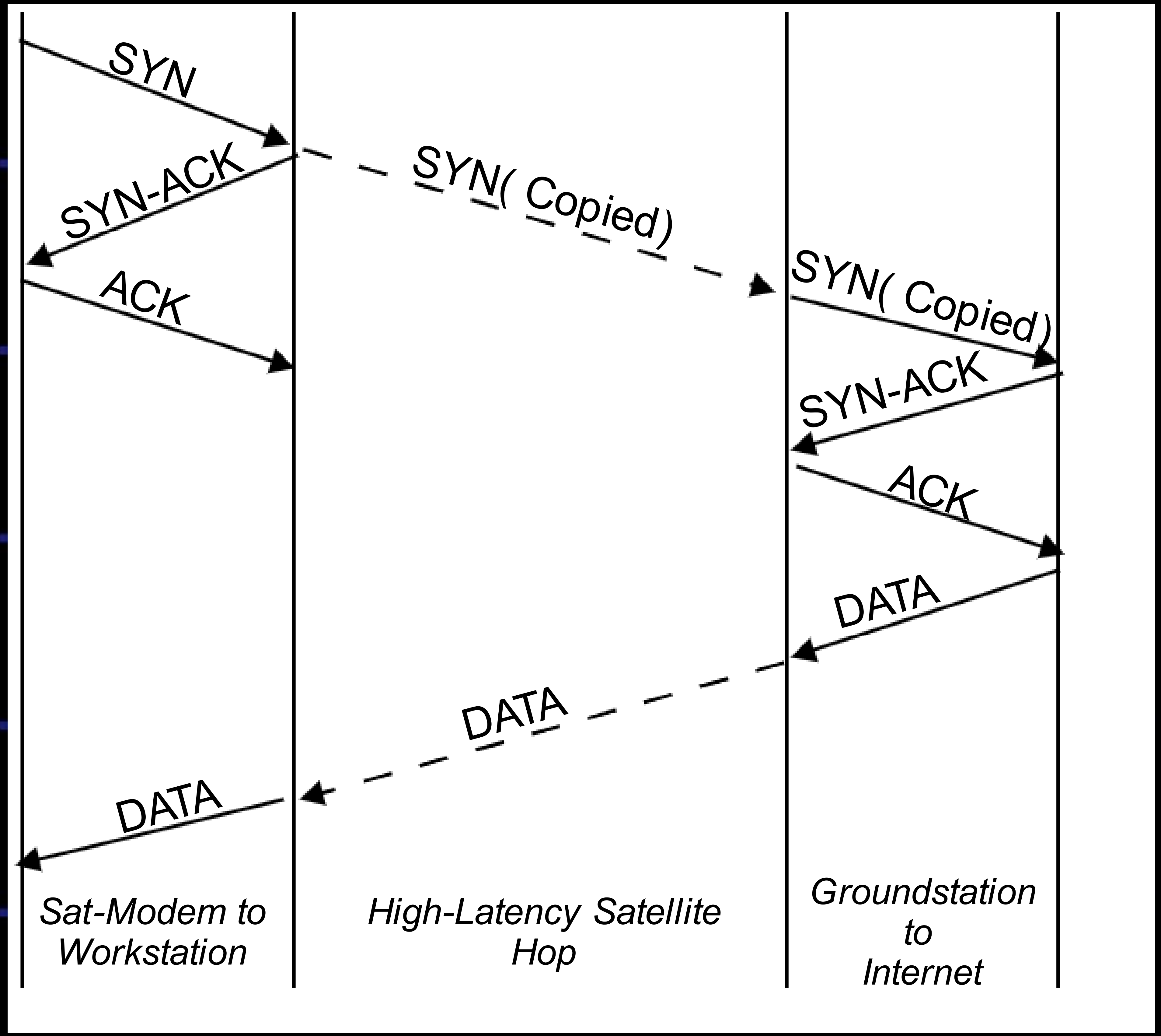
```
T [redacted] -> 10.48.[redacted]:50684 [AFP] #127
  HTTP/1.0 302 Moved Temporarily..Content-Type: text/html..Location:
  http://172.[redacted]:80?[redacted]&userurl=http
  ://efb.[redacted]/efb/api/v1/taskSheet/getUnsavedTsCaptains.do?soflSeqNrs=[redacted]
  [redacted]&fltNrs=[redacted]&schDepDts=[redacted]
 [redacted]&depCds=[redacted],PVG&arvCds=PVG,[redacted]

T [redacted]:80 -> 10.48.[redacted]:61044 [AFP] #913
  HTTP/1.0 302 Moved Temporarily..Content-Type: text/html..Location:
  http://172.[redacted]:80?[redacted]&userurl=http:
  //efb.[redacted]/efb/api/v1/flightPlan/getWayPoint.do?fltNr=[redacted]
  [redacted]&tailNr=[redacted]
  [redacted]&alnCd=[redacted]&depCd=[redacted]&arvCd=PEK&rescheduledFltDt=[redacted]&sofl
  SeqNr=[redacted]

T [redacted] -> [redacted]:55070 [AFP] #820
  HTTP/1.0 302 Moved Temporarily..Content-Type: text/html..Location:
  http://172[redacted]:80?[redacted]&userurl=http:/
  /efb.[redacted]/efb/api/v1/weather/sweatherquery.do?latitude=56.[redacted]&longi
  tude=[redacted]
```



```
> UTRAN Iuh interface RUA signalling
> Radio Access Network Application Part
> GSM A-I/F DTAP - CP-DATA
> GSM A-I/F RP - RP-DATA (Network to MS)
v GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .1.. .... = TP-UDHI: The beginning of the TP UD field contains a Header in addition to the short message
    ..0. .... = TP-SRI: A status report shall not be returned to the SME
    .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
    .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  > TP-Originating-Address - [redacted]
  > TP-PID: 0
  > TP-DCS: 8
  > TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (140) depends on Data-Coding-Scheme
  v TP-User-Data
    > User-Data Header
      SMS text: Name: [redacted])\nTest Result: Negative - \nResult Date: [redacted]
```

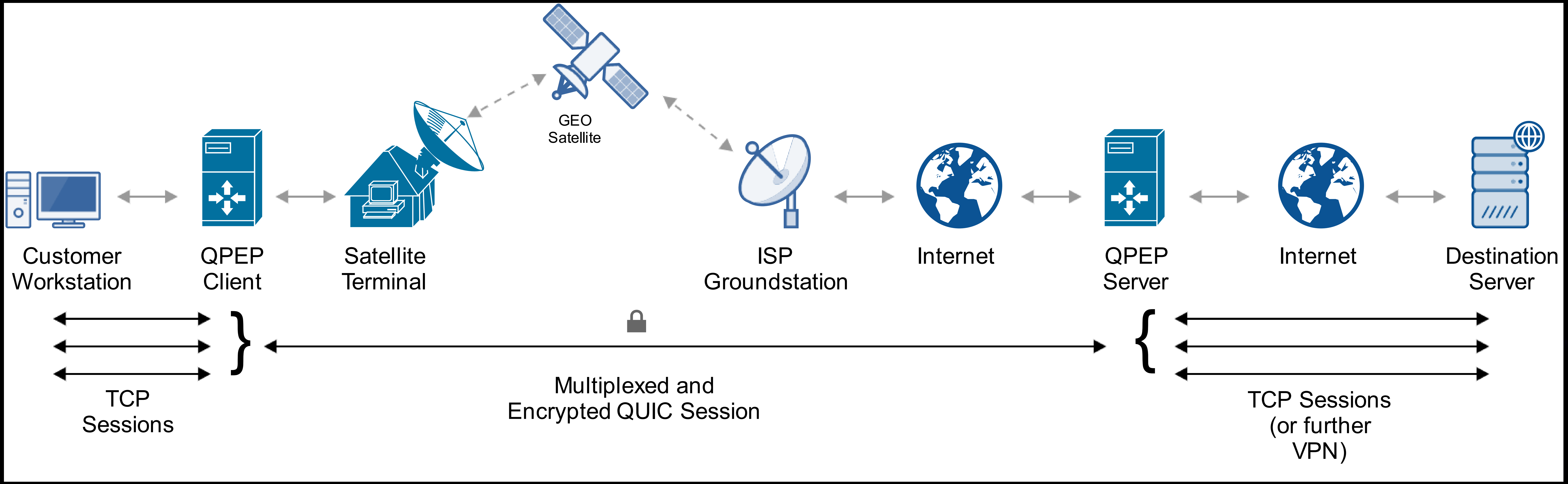
# Why Does this Happen?

- Space is far and round-trip times (RTT) to GEO are long
- TCP especially troublesome because of the 3-way handshake
- ISP = Benevolent "attacker" snooping on your traffic
  - But they can't do this if you use a VPN



HITCON PEACE 2022 SURVIVAL GUIDE FOR THE CYBER WAR

# Mitigation: QPEP



Contribute / Try It Out: https://github.com/ssloxford/qpep

# Eavesdropping Takeways

$ Threat Models Change

Passive Attacks -> Active Effects

Physicality Can Drive Security Consequences

# Concluding Thoughts

# Themes for Space Security

Physicality

Interdisciplinarity

Adaptability

**Questions/Thoughts?:**
james@pavursec.com

@jamespavur