black hat USA 2020

AUGUST 5-6, 2020

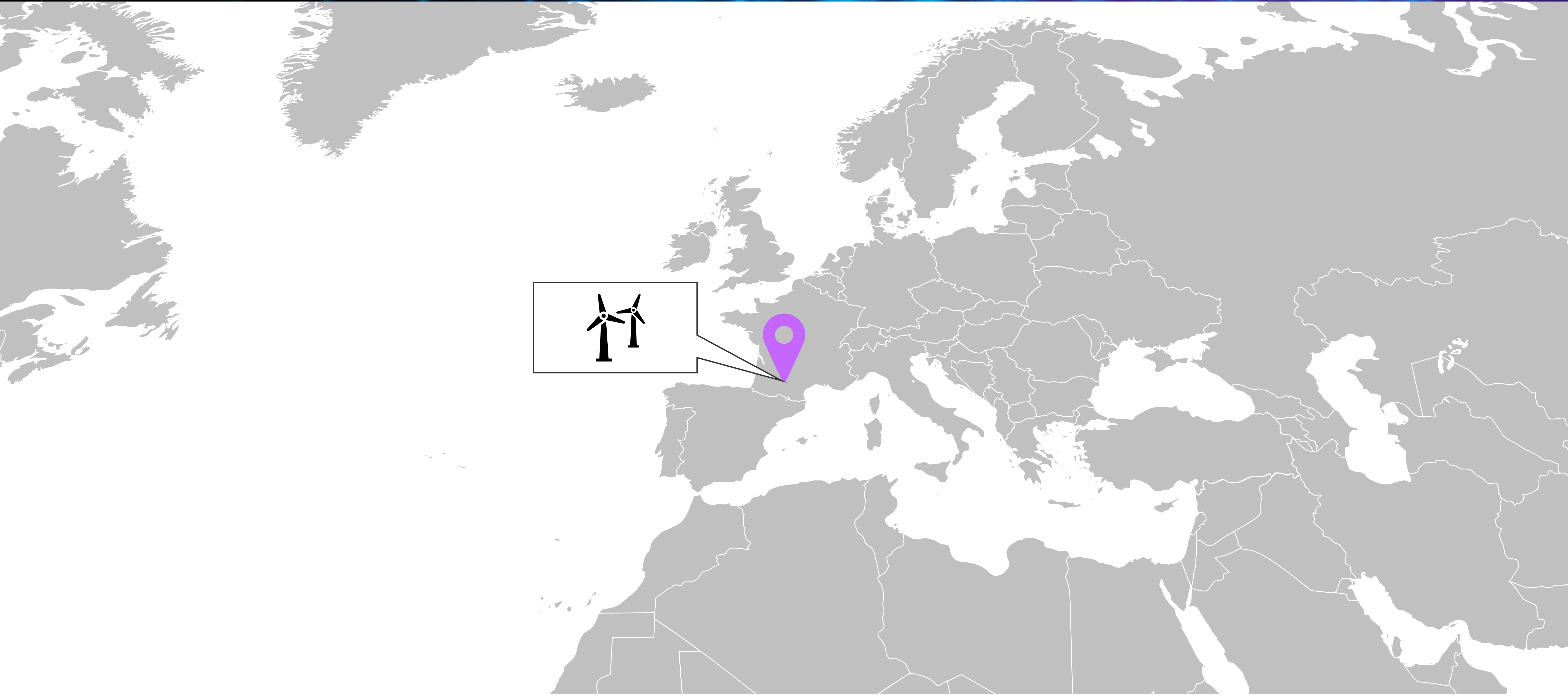
BRIEFINGS

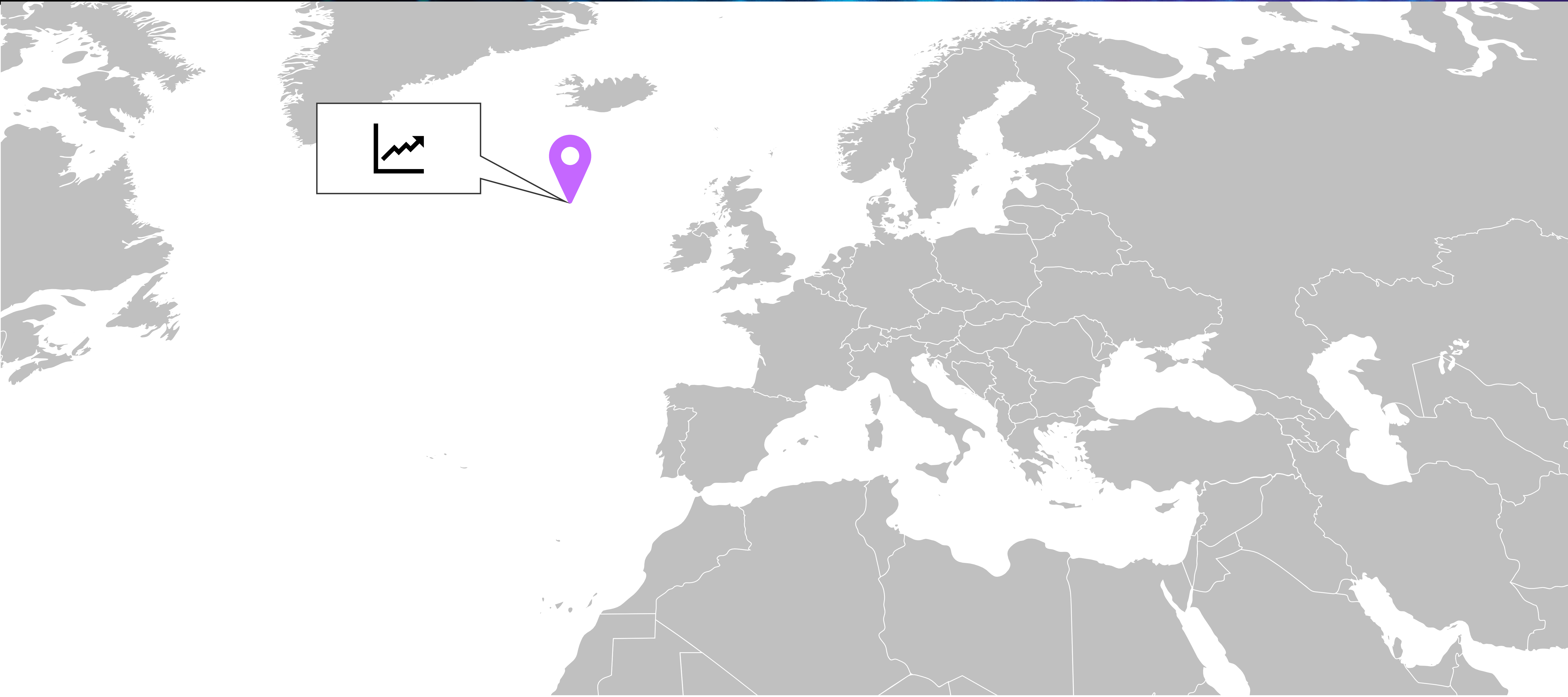
Whispers Among the Stars

Perpetrating (and Preventing) Satellite Eavesdropping Attacks

James Pavur, DPhil Student

Oxford University, Department of Computer Science





Bio / Contributors

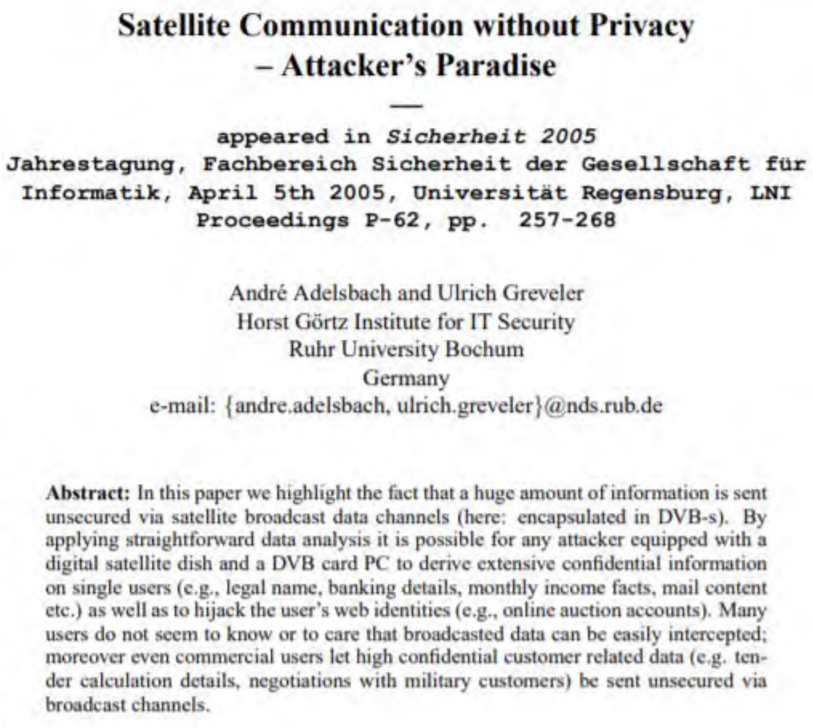
- PhD Student @ Oxford University, Systems Security Lab
  - Title of (blank) *thesis_draft.tex* file: *Securing New Space: On Satellite Cybersecurity*
- Don’t Work Alone…
  - Daniel Moser, armasuisse / ETH Zürich
  - Martin Strohmeier, armasuisse / Oxford University
  - Vincent Lenders, armasuisse
  - Ivan Martinovic, Oxford University

CYD CYBER DEFENCE CAMPUS

RHODES TRUST

CENTRE FOR DOCTORAL TRAINING in CYBER SECURITY

Lessons from the Past



Satellite Communication without Privacy – Attacker's Paradise

—

appeared in *Sicherheit 2005*
Jahrestagung, Fachbereich Sicherheit der Gesellschaft für Informatik, April 5th 2005, Universität Regensburg, LNI Proceedings P-62, pp. 257-268

André Adelsbach and Ulrich Greveler
Horst Görtz Institute for IT Security
Ruhr University Bochum
Germany
e-mail: {andre.adelsbach, ulrich.greveler}@nds.rub.de

Abstract: In this paper we highlight the fact that a huge amount of information is sent unsecured via satellite broadcast data channels (here: encapsulated in DVB-s). By applying straightforward data analysis it is possible for any attacker equipped with a digital satellite dish and a DVB card PC to derive extensive confidential information on single users (e.g., legal name, banking details, monthly income facts, mail content etc.) as well as to hijack the user's web identities (e.g., online auction accounts). Many users do not seem to know or to care that broadcasted data can be easily intercepted; moreover even commercial users let high confidential customer related data (e.g. tender calculation details, negotiations with military customers) be sent unsecured via broadcast channels.

Ruhr-University Bochum, 2005

$atellite Hacking for Fun & Pr0fit!

Adam Laurie
adam@algroup.co.uk

http://rfidiot.org

Black Hat DC, 2009

S21sec

Leonardo Nve Egea
lnve@s21sec.com

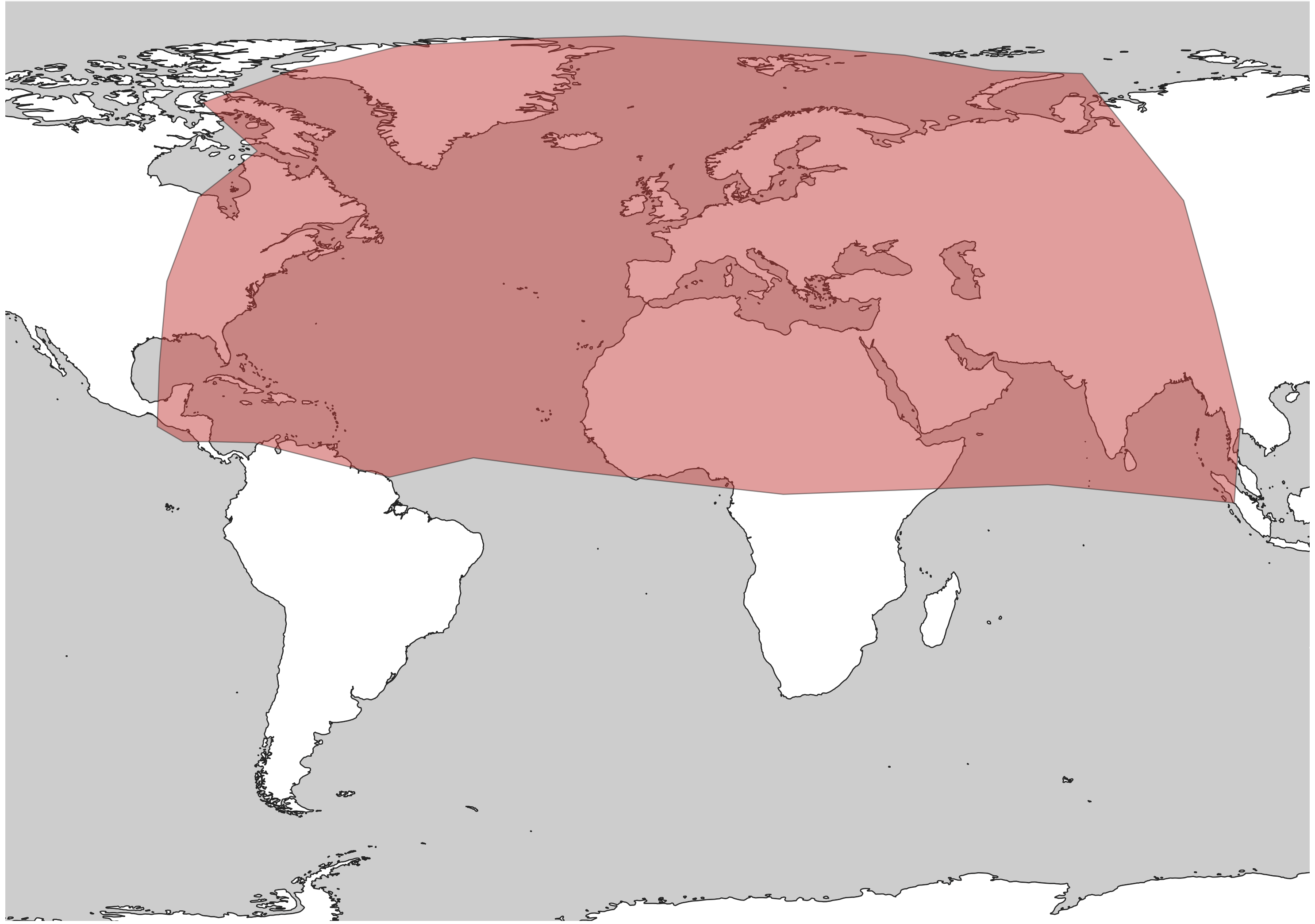
Playing in a Satellite environment 1.2

Black Hat DC, 2010

3 Domain-Focused Experiments

18 GEO Satellites

Coverage Area ~100 million km^2

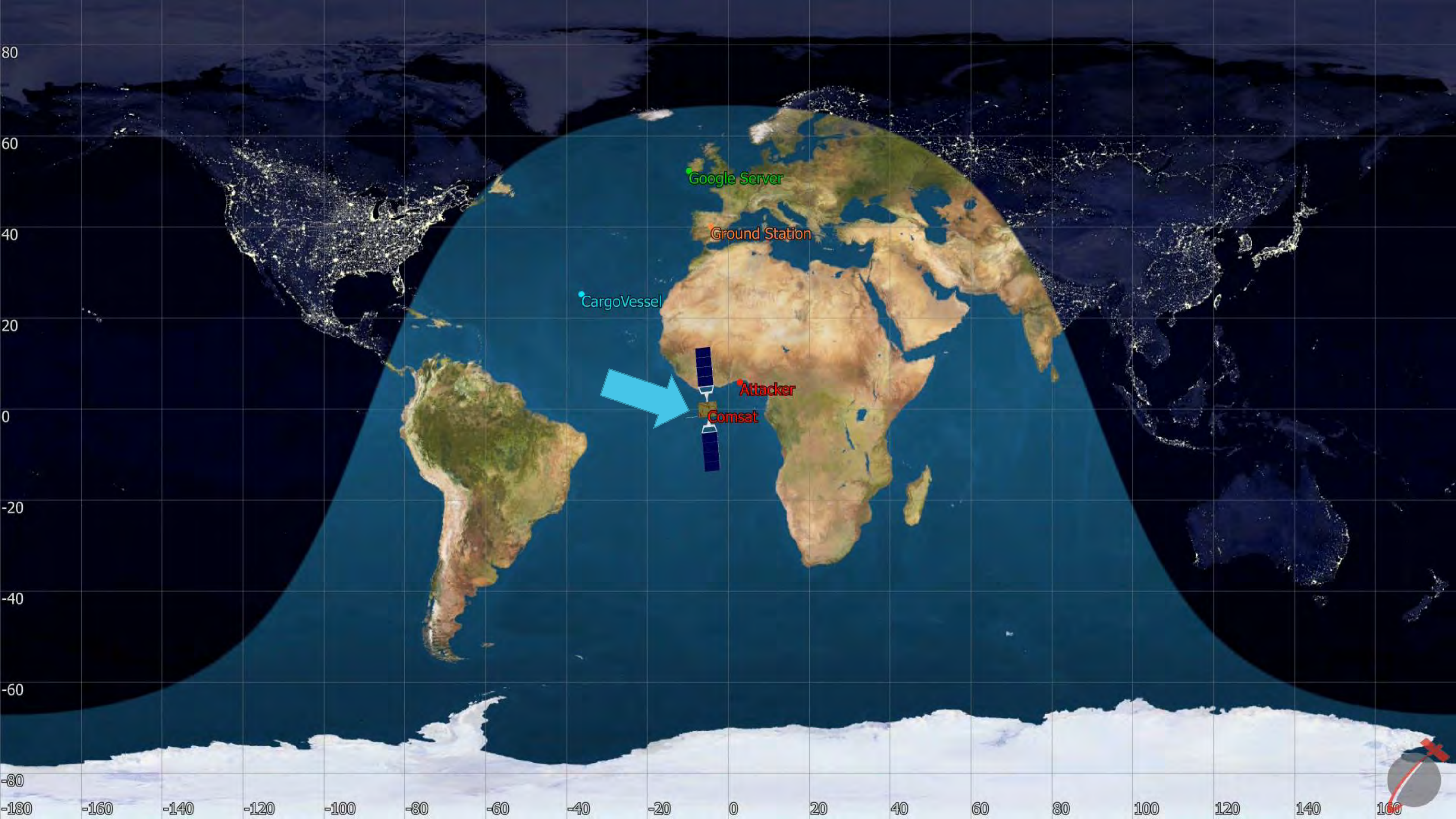


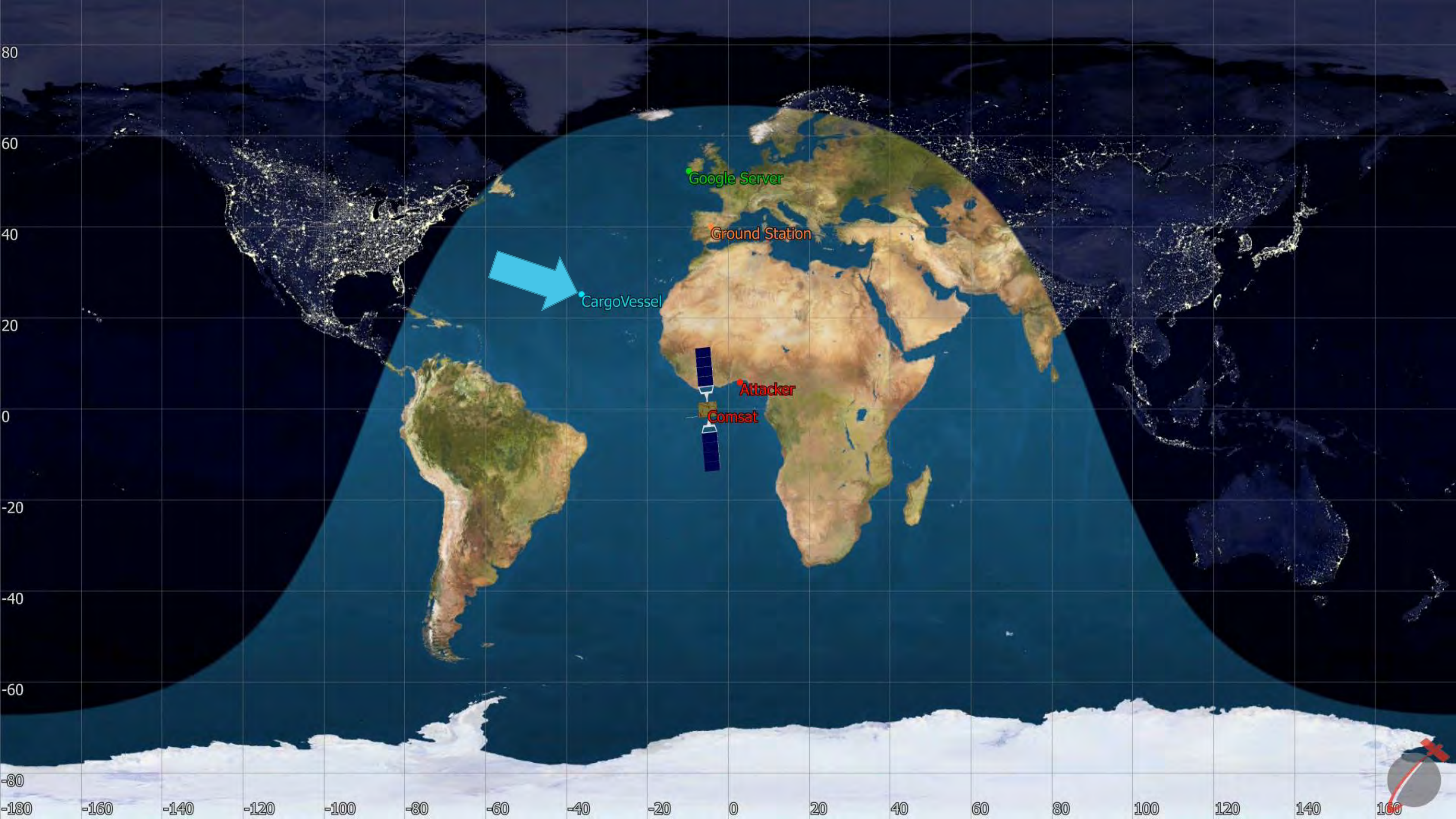
Whose Data?

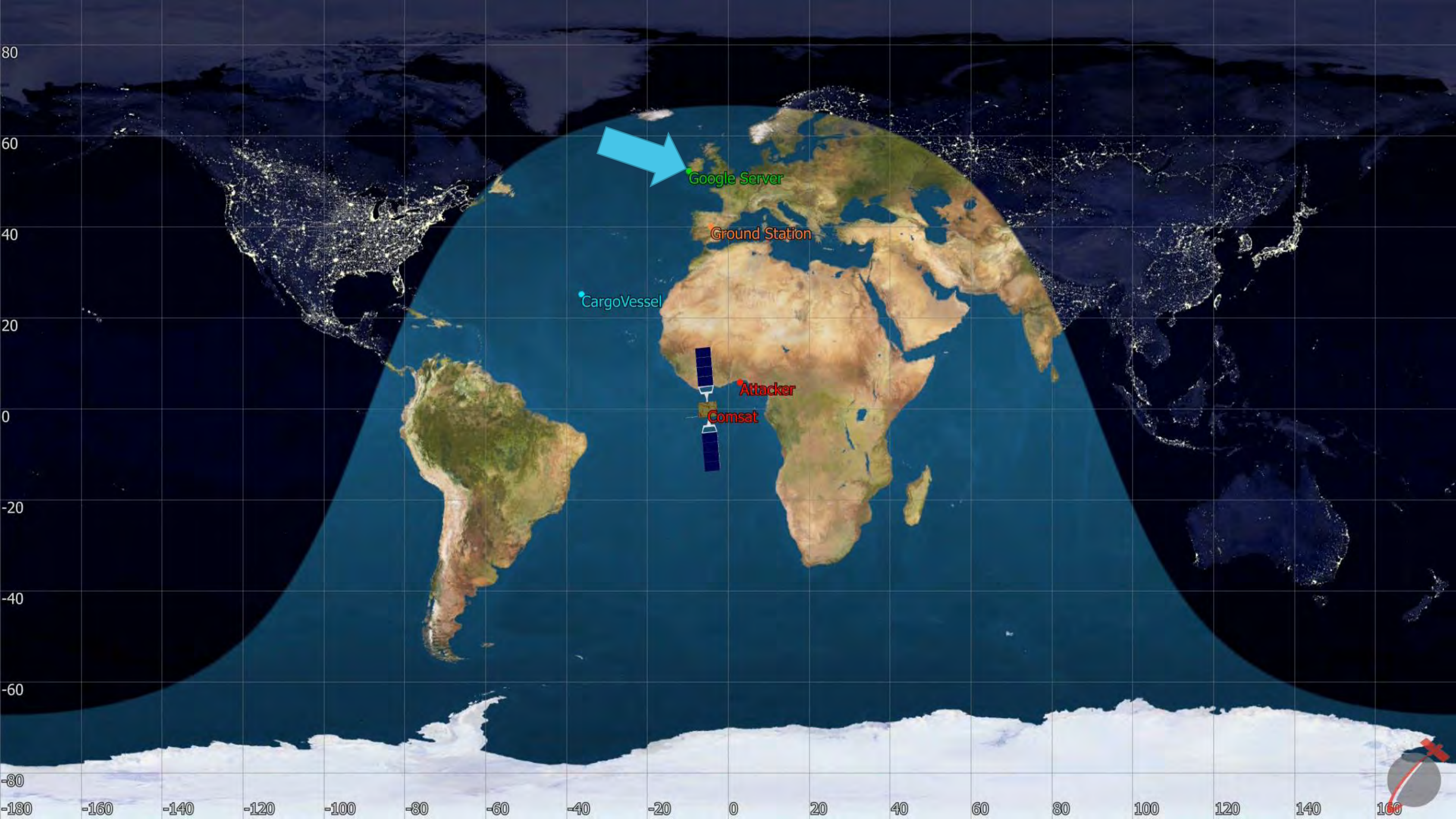
$	✈	⚓	🏛	👥
9 FORTUNE GLOBAL 500 MEMBERS	6 OF 10 LARGEST AIRLINES	~40% MARITIME CARGO MARKET	GOVERNMENTAL AGENCIES	YOU?

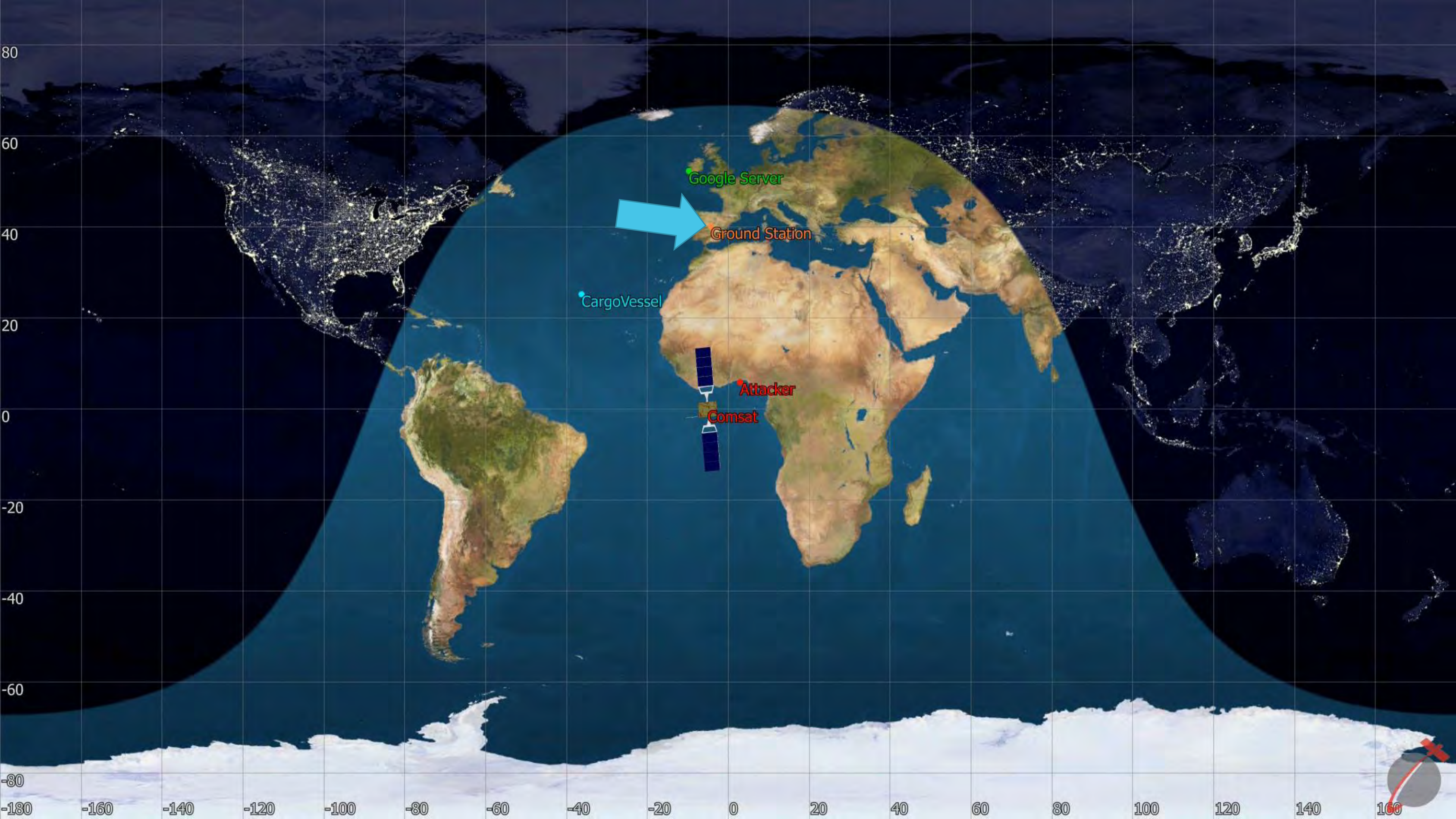
3-Minute SATCOM Crash Course

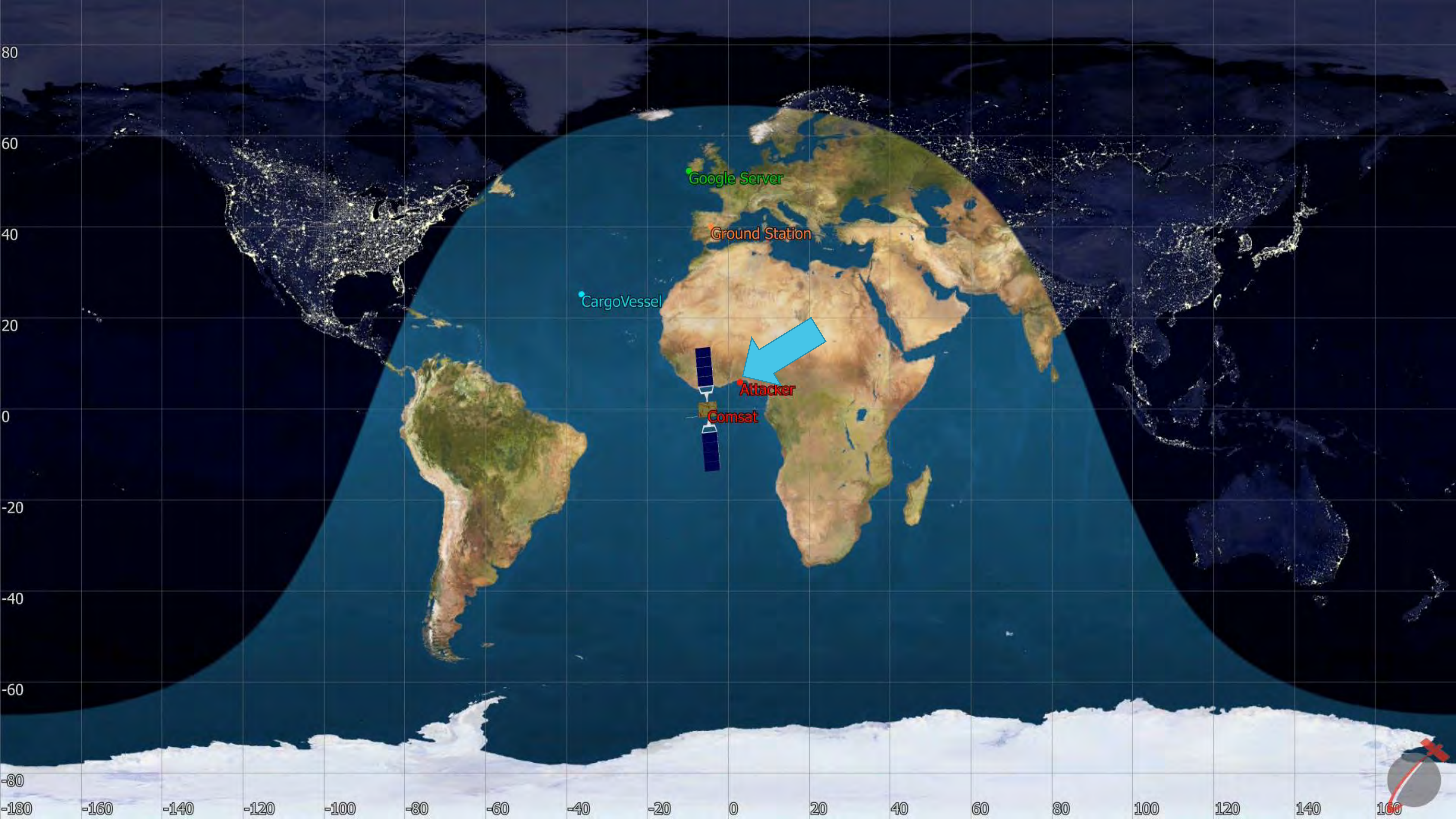
Photo: *Three Crew Members Capture Intelsat VI*, NASA, 1992, Public Domain


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


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

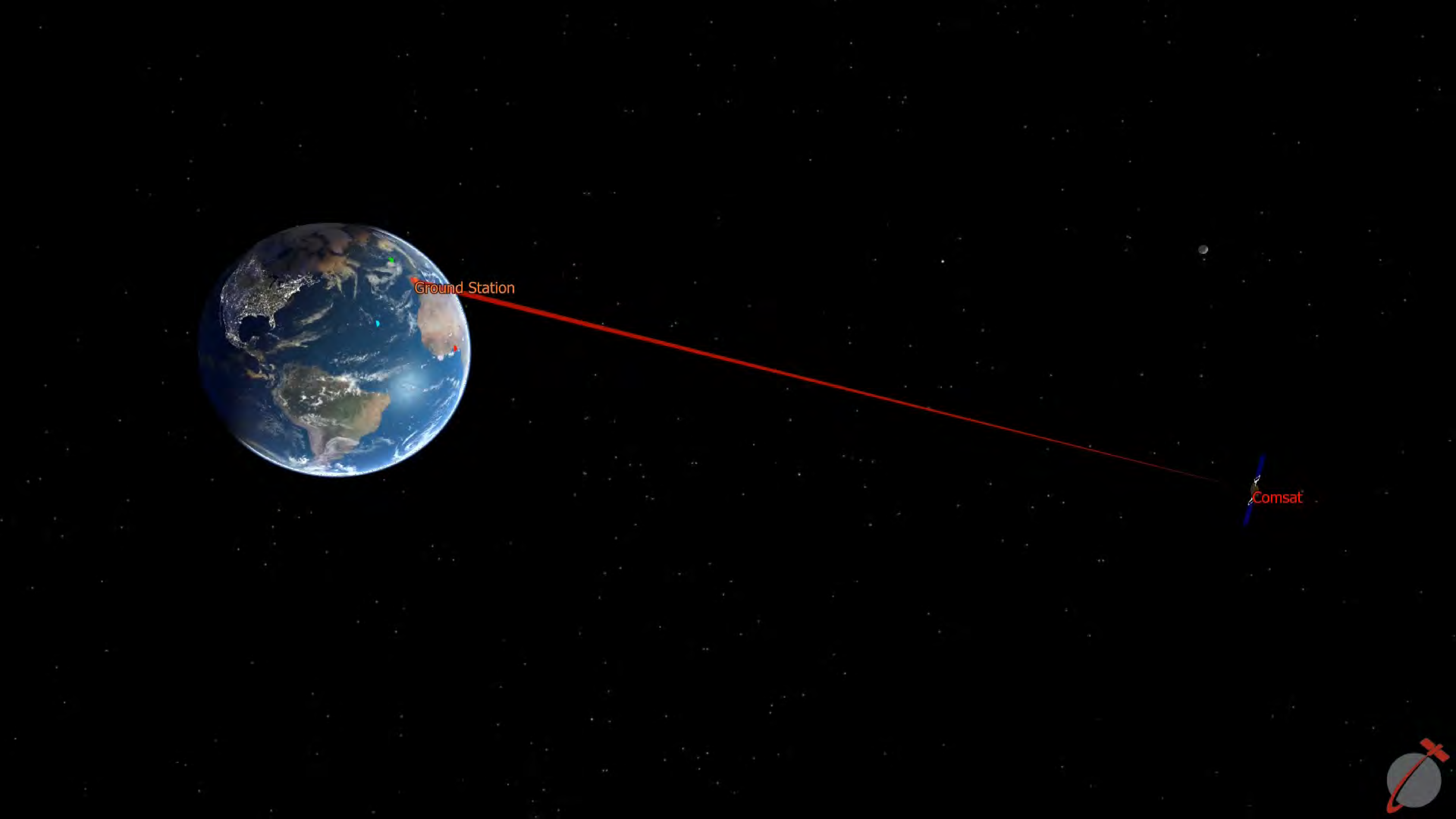

Google Server
Ground Station
CargoVessel
Attacker
Comsat
80
60
40
20
0
-20
-40
-60
-80
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160


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


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

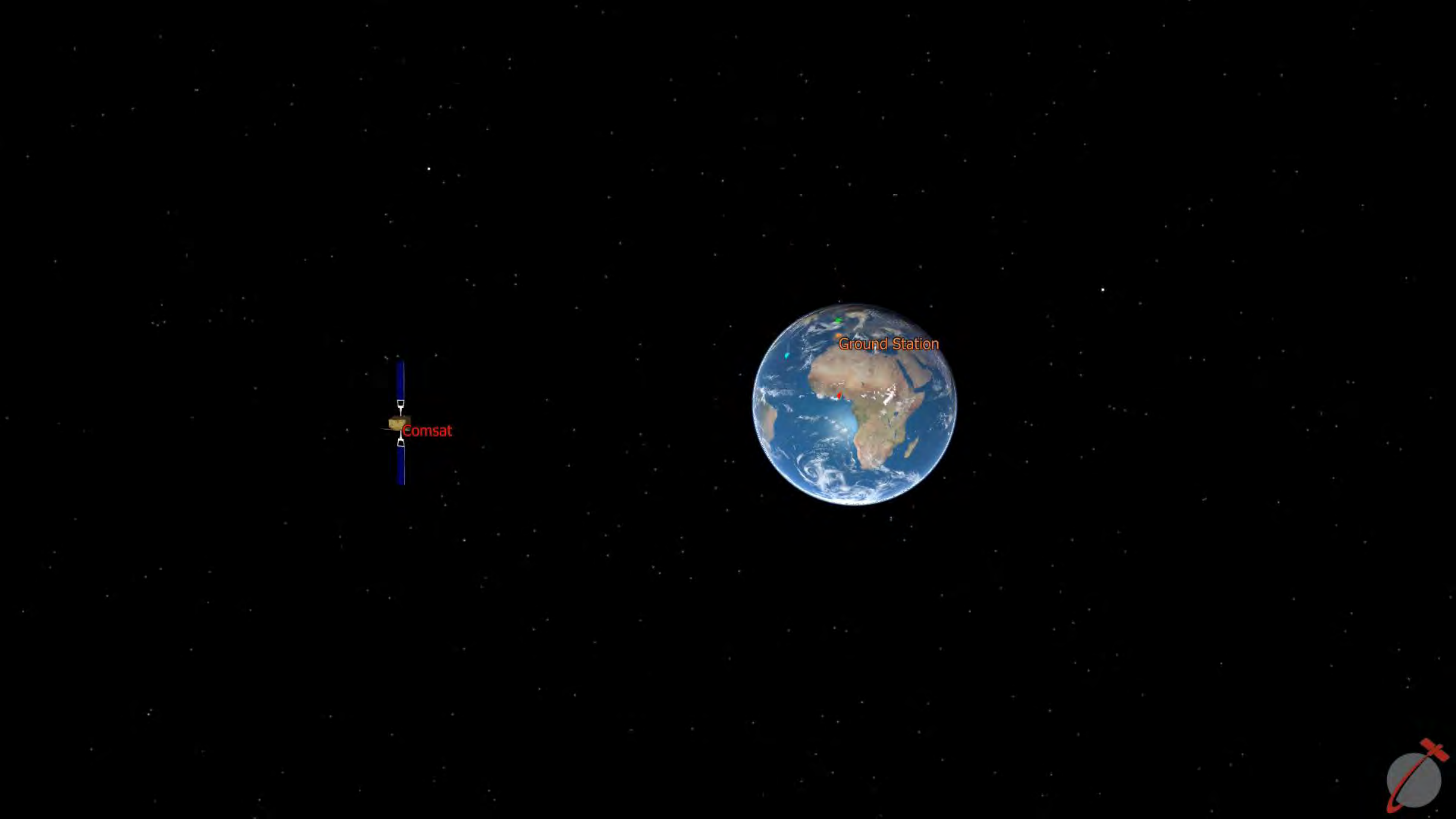
GET google.com
Comsat

CargoVessel
Comsat



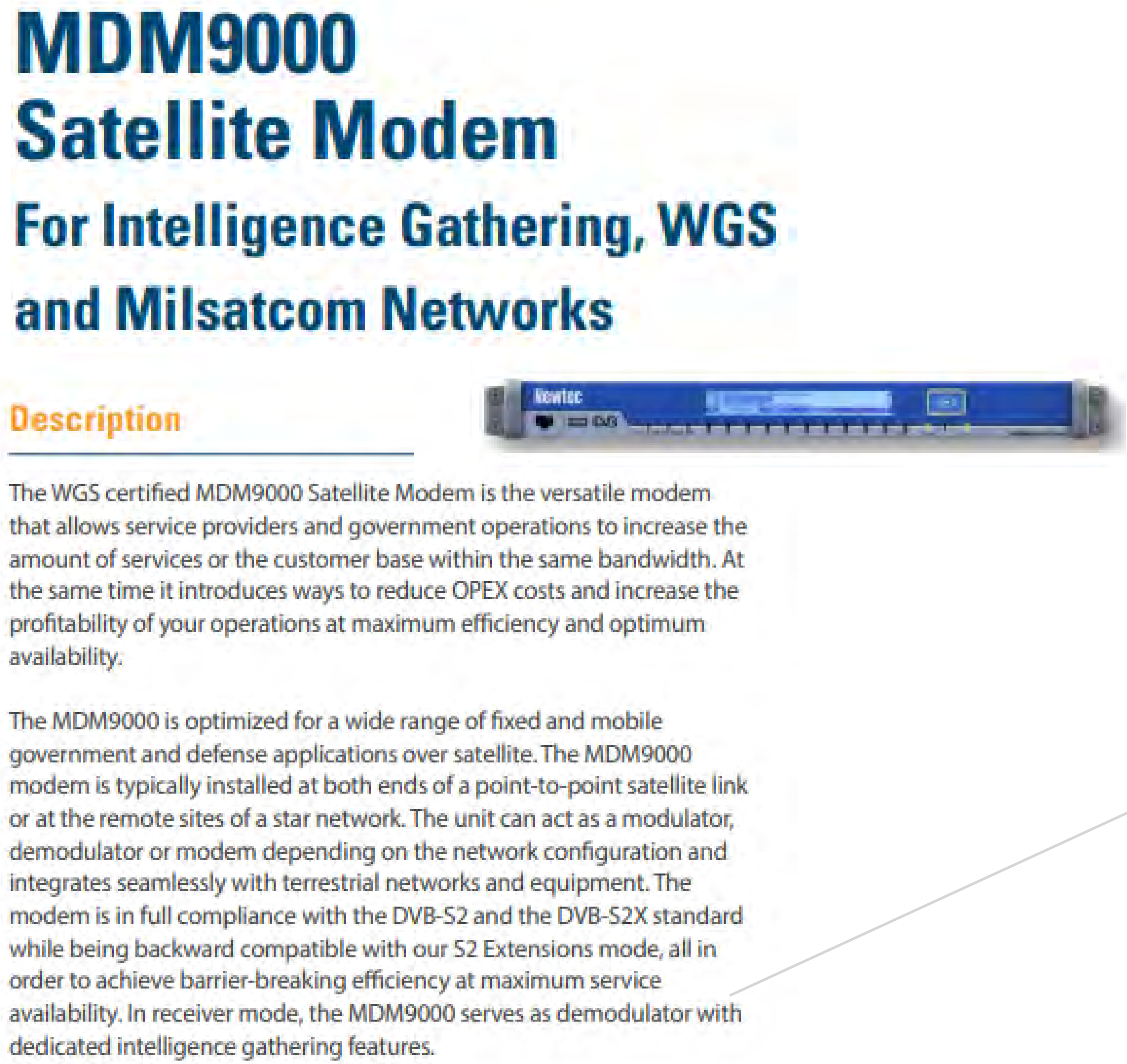
Ground Station
Comsat

Google Server
Ground Station


Comsat
Ground Station

Threat Model

Nation-State Actor Tech



MDM9000
Satellite Modem
For Intelligence Gathering, WGS and Milsatcom Networks

Description

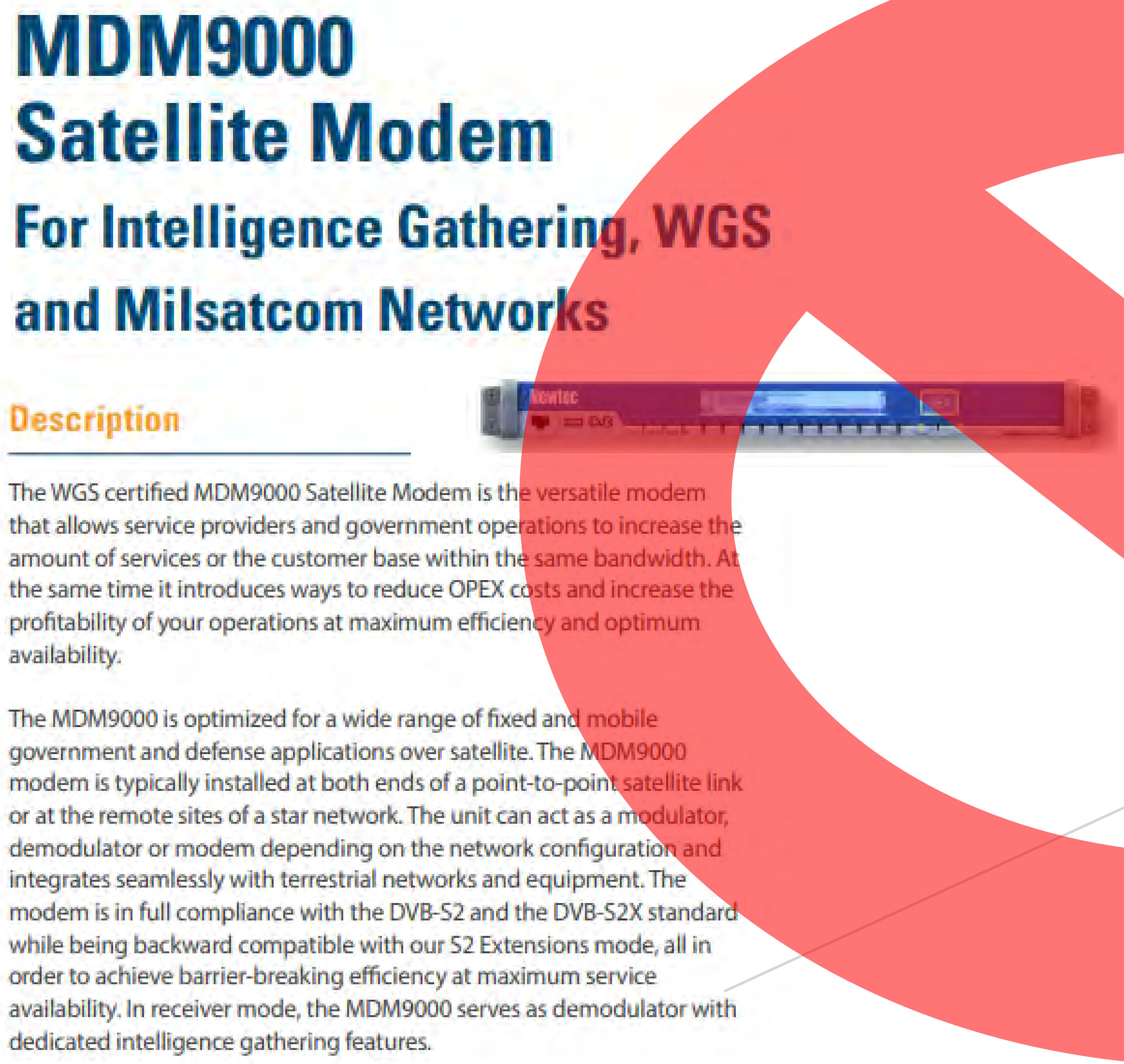
The WGS certified MDM9000 Satellite Modem is the versatile modem that allows service providers and government operations to increase the amount of services or the customer base within the same bandwidth. At the same time it introduces ways to reduce OPEX costs and increase the profitability of your operations at maximum efficiency and optimum availability.

The MDM9000 is optimized for a wide range of fixed and mobile government and defense applications over satellite. The MDM9000 modem is typically installed at both ends of a point-to-point satellite link or at the remote sites of a star network. The unit can act as a modulator, demodulator or modem depending on the network configuration and integrates seamlessly with terrestrial networks and equipment. The modem is in full compliance with the DVB-S2 and the DVB-S2X standard while being backward compatible with our S2 Extensions mode, all in order to achieve barrier-breaking efficiency at maximum service availability. In receiver mode, the MDM9000 serves as demodulator with dedicated intelligence gathering features.

In receiver mode, the MDM9000 serves as demodulator with dedicated intelligence gathering features.

Photo: *Het grondstation van de NSO*, Wutsje, July 2012, Wikimedia Commons, CC BY-SA 3.0

Nation-State Actor Tech



MDM9000
Satellite Modem
For Intelligence Gathering, WGS and Milsatcom Networks

Description

The WGS certified MDM9000 Satellite Modem is the versatile modem that allows service providers and government operations to increase the amount of services or the customer base within the same bandwidth. At the same time it introduces ways to reduce OPEX costs and increase the profitability of your operations at maximum efficiency and optimum availability.

The MDM9000 is optimized for a wide range of fixed and mobile government and defense applications over satellite. The MDM9000 modem is typically installed at both ends of a point-to-point satellite link or at the remote sites of a star network. The unit can act as a modulator, demodulator or modem depending on the network configuration and integrates seamlessly with terrestrial networks and equipment. The modem is in full compliance with the DVB-S2 and the DVB-S2X standard while being backward compatible with our S2 Extensions mode, all in order to achieve barrier-breaking efficiency at maximum service availability. In receiver mode, the MDM9000 serves as demodulator with dedicated intelligence gathering features.

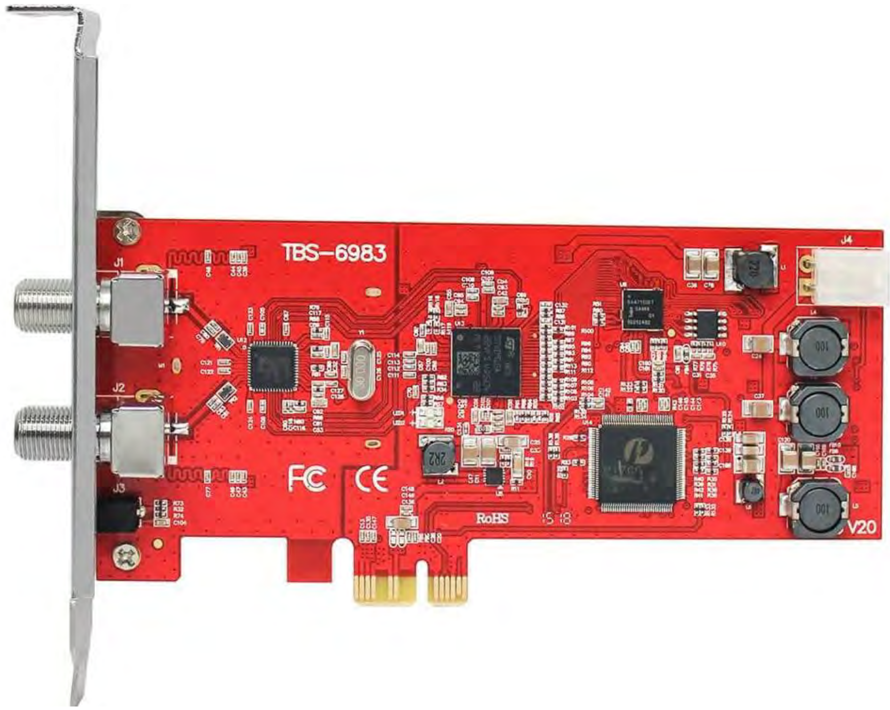
In receiver mode, the MDM9000 serves as demodulator with dedicated intelligence gathering features.

Photo: *Het grondstation van de NSO*, Wutsje, July 2012, Wikimedia Commons, CC BY-SA 3.0

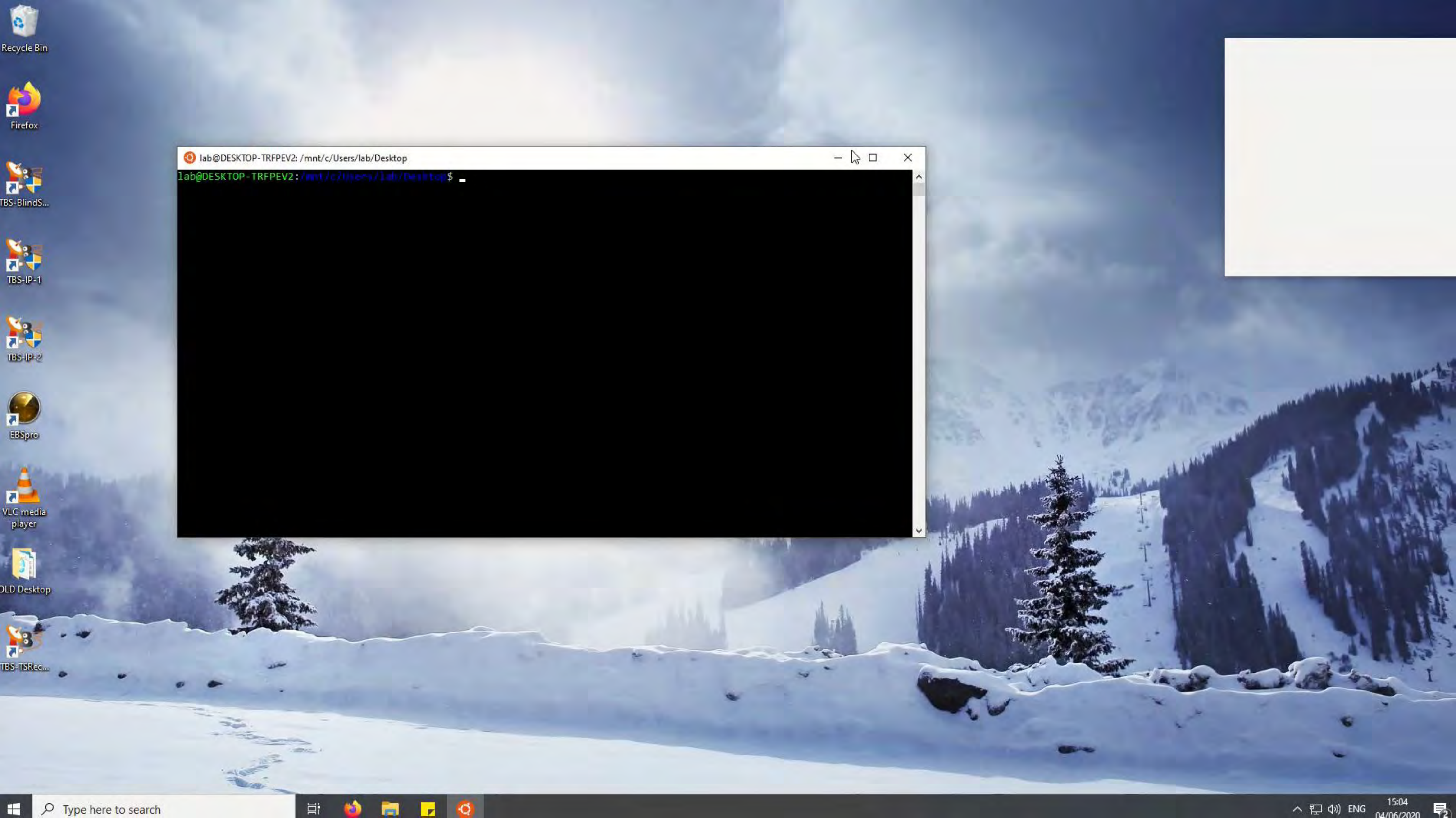
$300 of TV Equipment

Selfsat H30D ~$90 (or any old satellite dish + LNB off Craigslist)

+



TBS-6983/6903 ~$200-$300 (or comparable PCIE DVB-S tuner, ideally with APSK support)



lab@DESKTOP-TRFPEV2: /mnt/c/Users/lab/Desktop

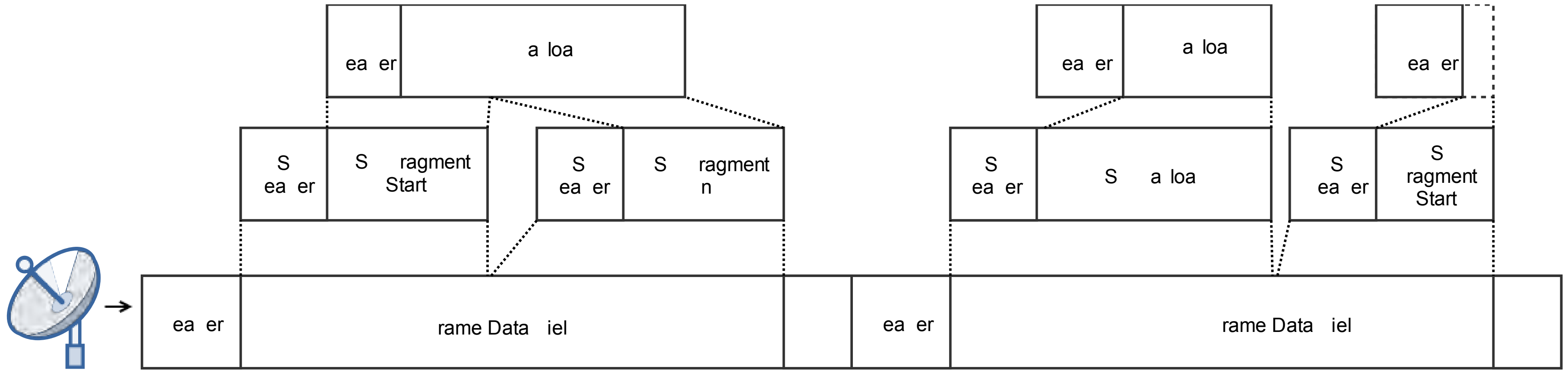
```
lab@DESKTOP-TRFPEV2:/mnt/c/Users/lab/Desktop$ _
```

MPEG-TS + MPE/ULE

- Legacy (but still popular) standard
  - Sort of a hacked together combination of protocols built for other purposes
- Tools exist for parsing
  - dvbsnoop, tsduck, TSReader
- Primary focus of related work from 2000-2010

GSE (Generic Stream Encapsulation)

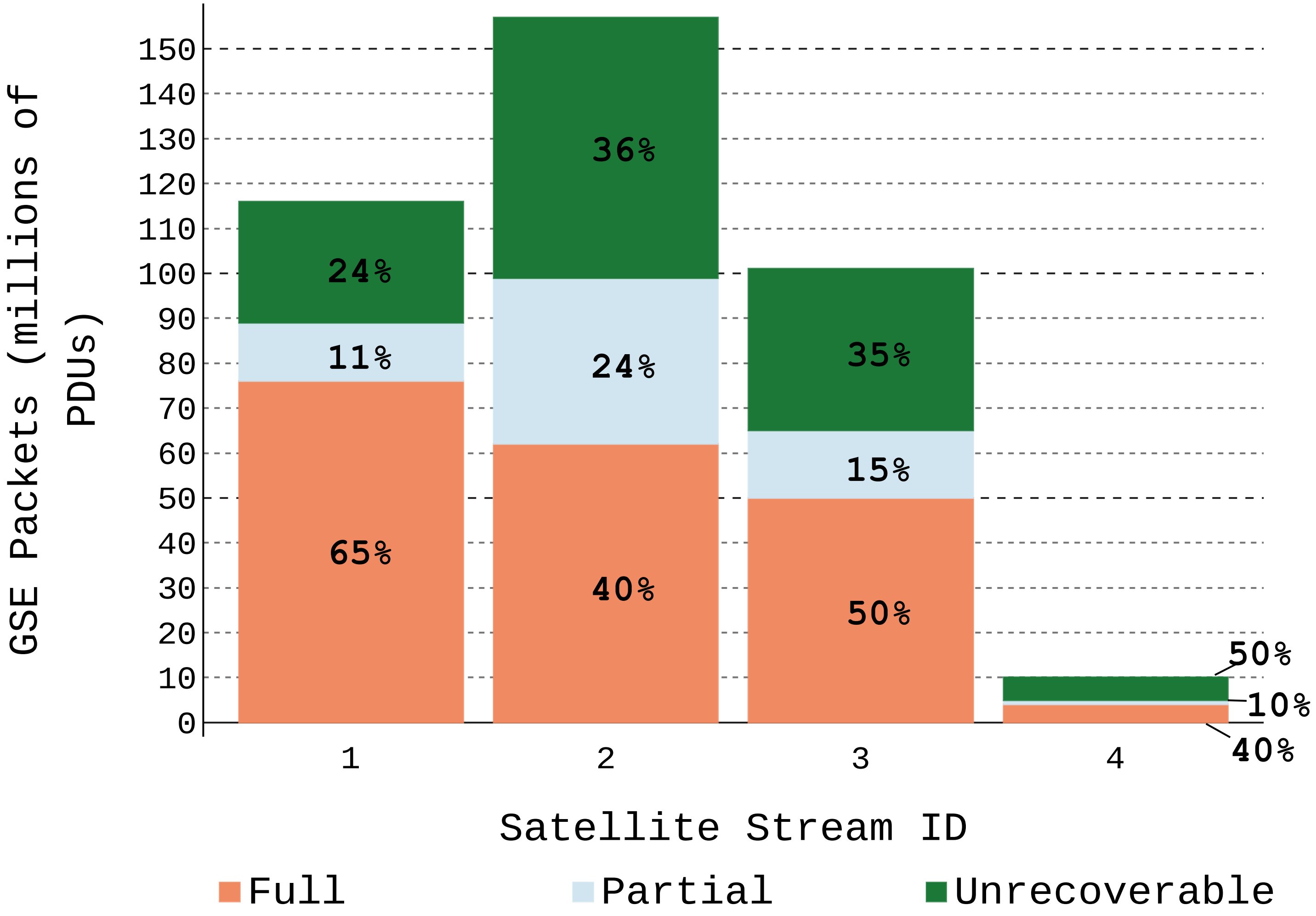
- More modern, popular among enterprise “VSAT” customers
- In practice, networks assume equipment in the $25k-$100k range

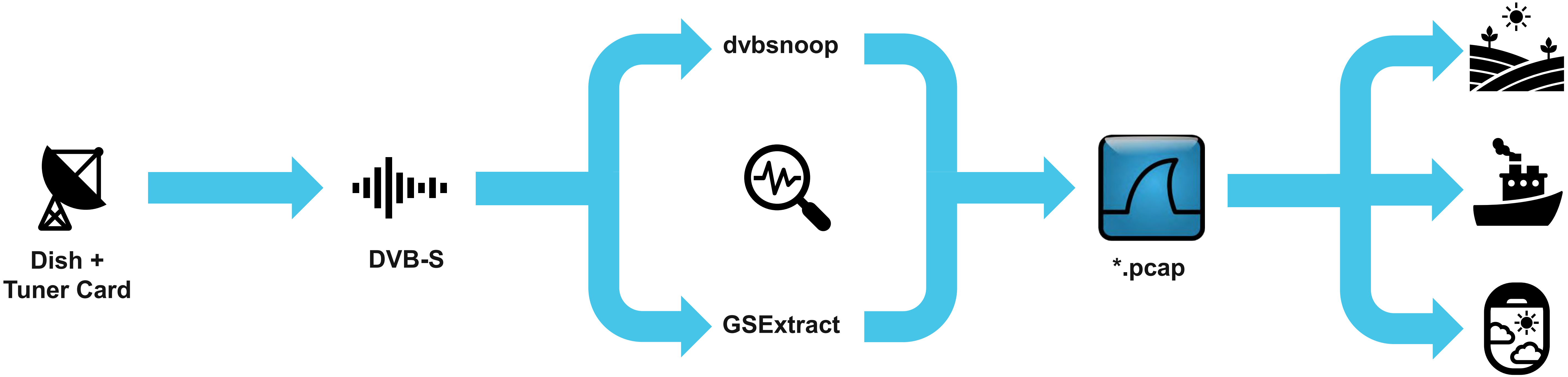


GSExtract

- Custom tool to forensically reconstruct bad recordings
  - Applies simple rules to find IP headers / place fragments
  - https://doi.ieeecomputersociety.org/10.1109/SP40000.2020.00056
- Public Release?
  - https://github.com/ssloxford

Packet Recovery Rate Using GSExtract



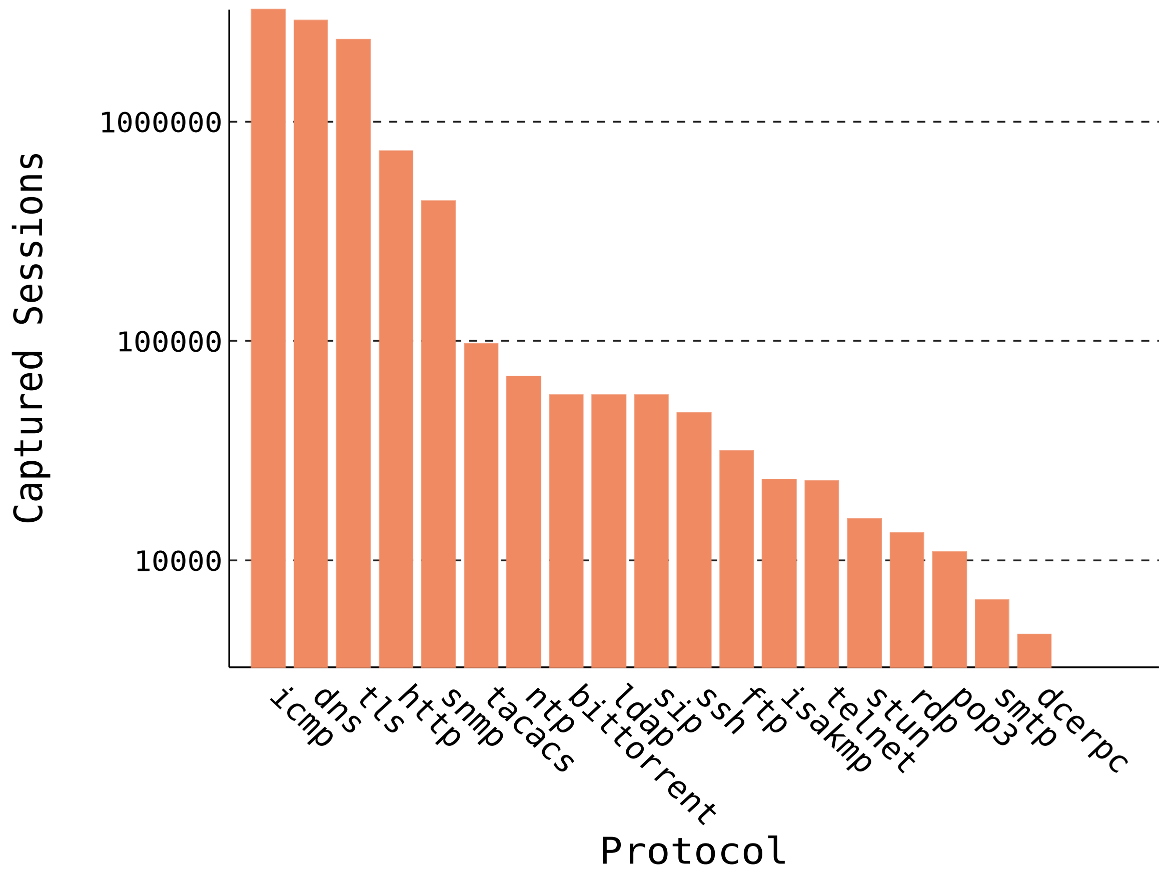

Dish +
Tuner Card
DVB-S
dvbsnoop
GSExtract
*.pcap

General Findings

NO DEFAULT ENCRYPTION

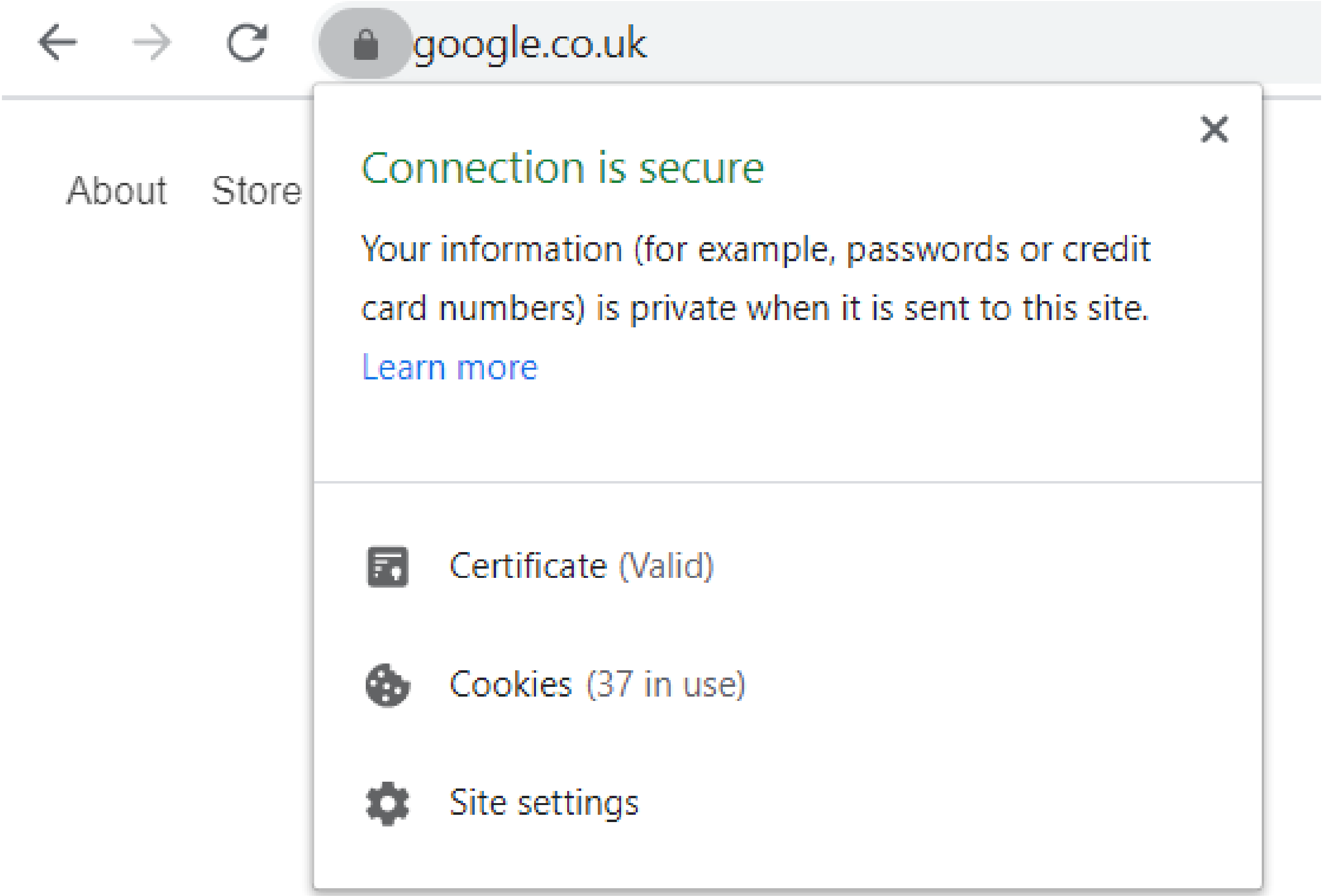
ISP-ESQUE VANTAGE POINT

BREACH THE PERIMETER



Terrestrial

TLS == Privacy?

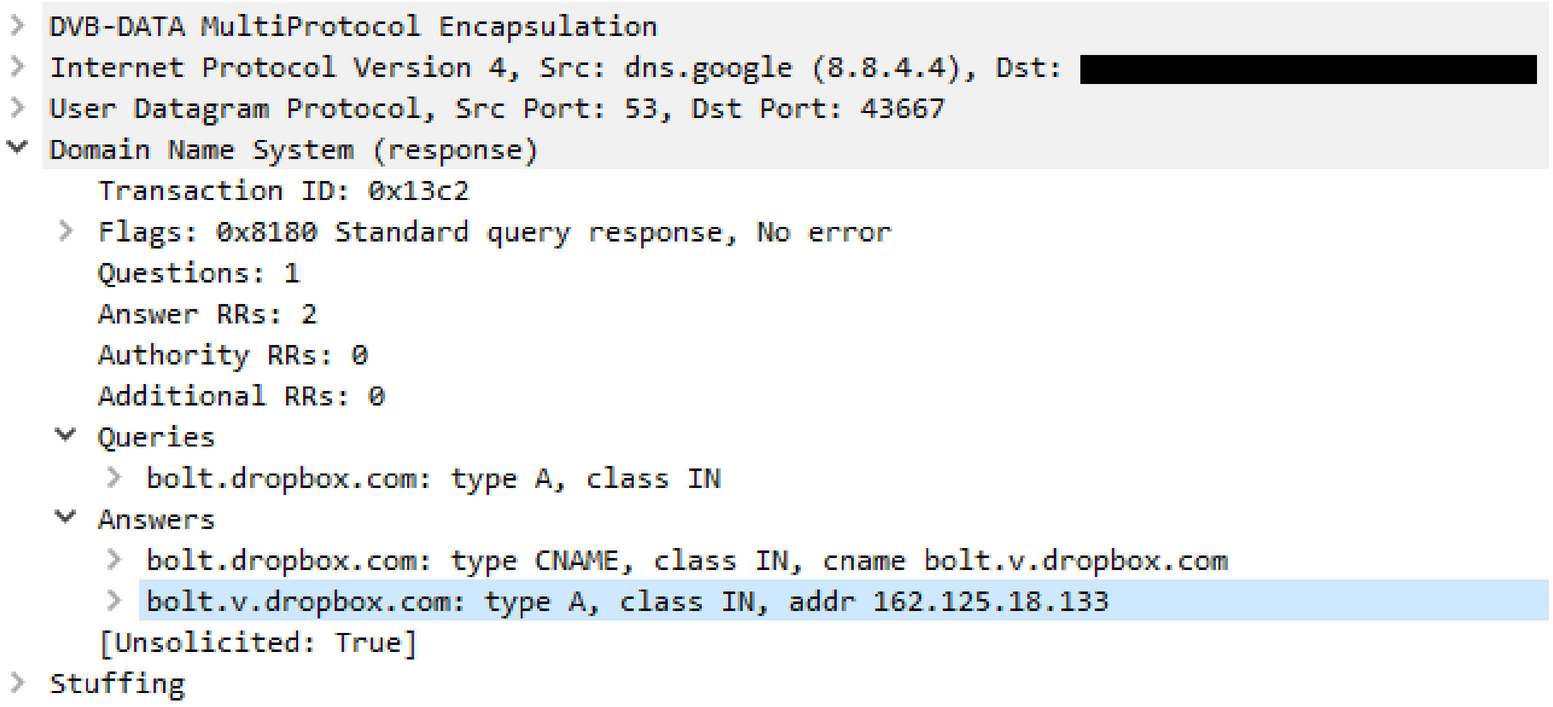


google.co.uk

Connection is secure

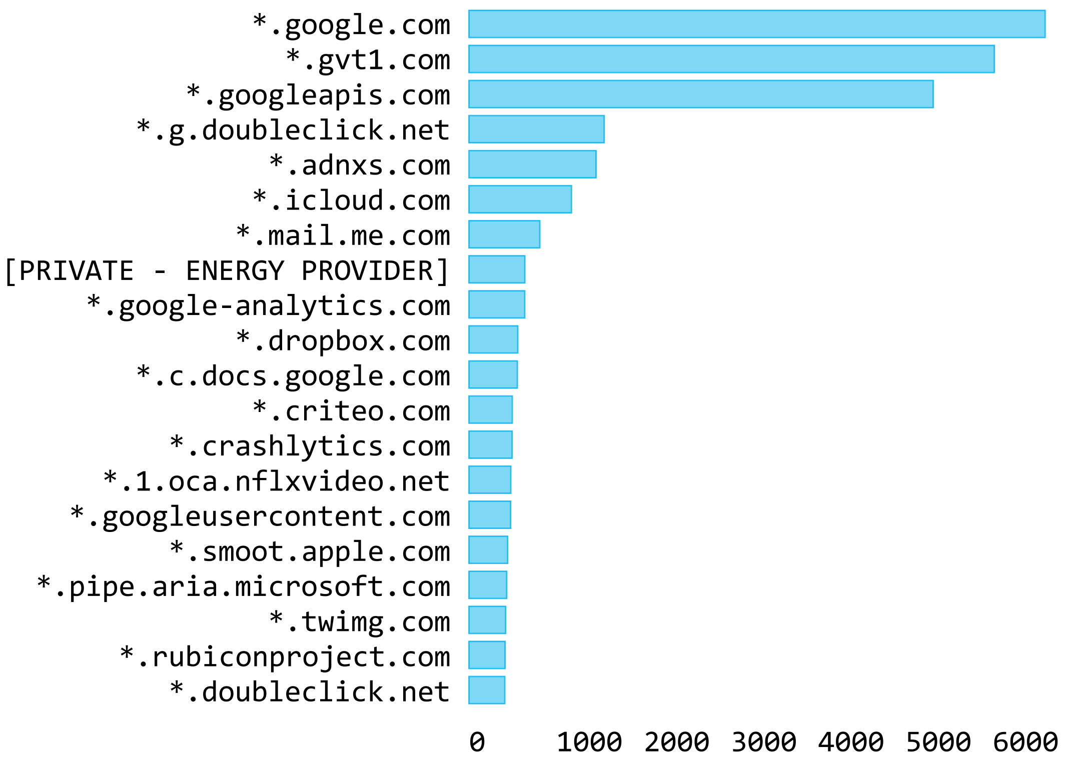
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

TLS != Privacy

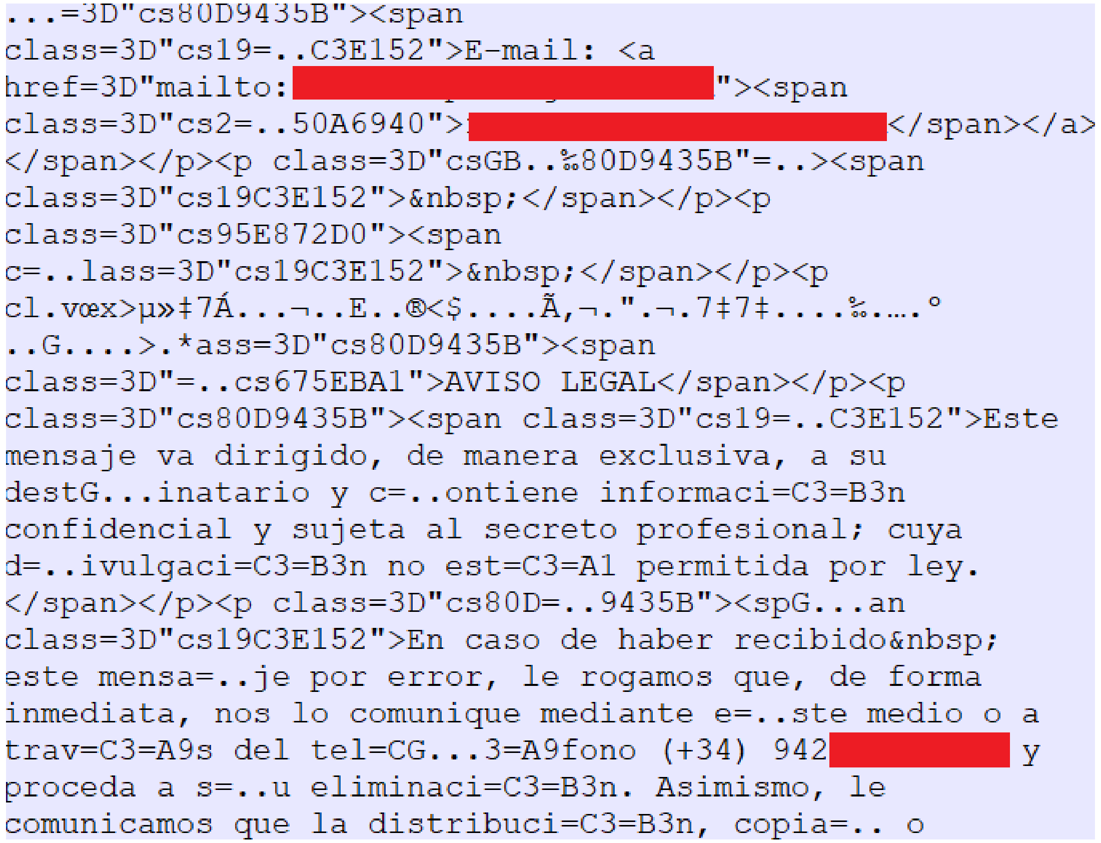


```
> DVB-DATA MultiProtocol Encapsulation
> Internet Protocol Version 4, Src: dns.google (8.8.4.4), Dst: [redacted]
> User Datagram Protocol, Src Port: 53, Dst Port: 43667
v Domain Name System (response)
    Transaction ID: 0x13c2
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > bolt.dropbox.com: type A, class IN
  v Answers
    > bolt.dropbox.com: type CNAME, class IN, cname bolt.v.dropbox.com
    > bolt.v.dropbox.com: type A, class IN, addr 162.125.18.133
    [Unsolicited: True]
> Stuffing
```

Top SSL Certificate Names (MPEG-TS Case Study)



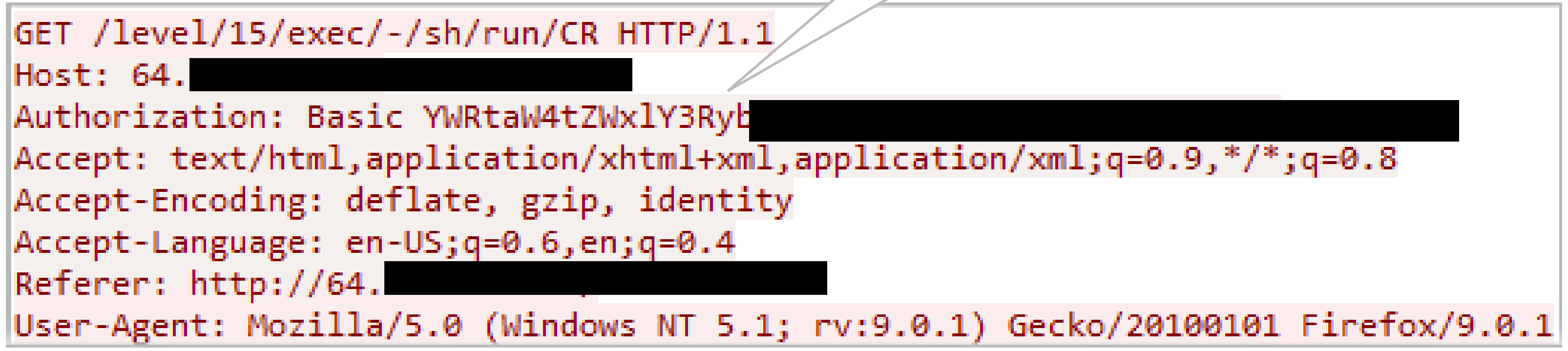
!TLS != Privacy



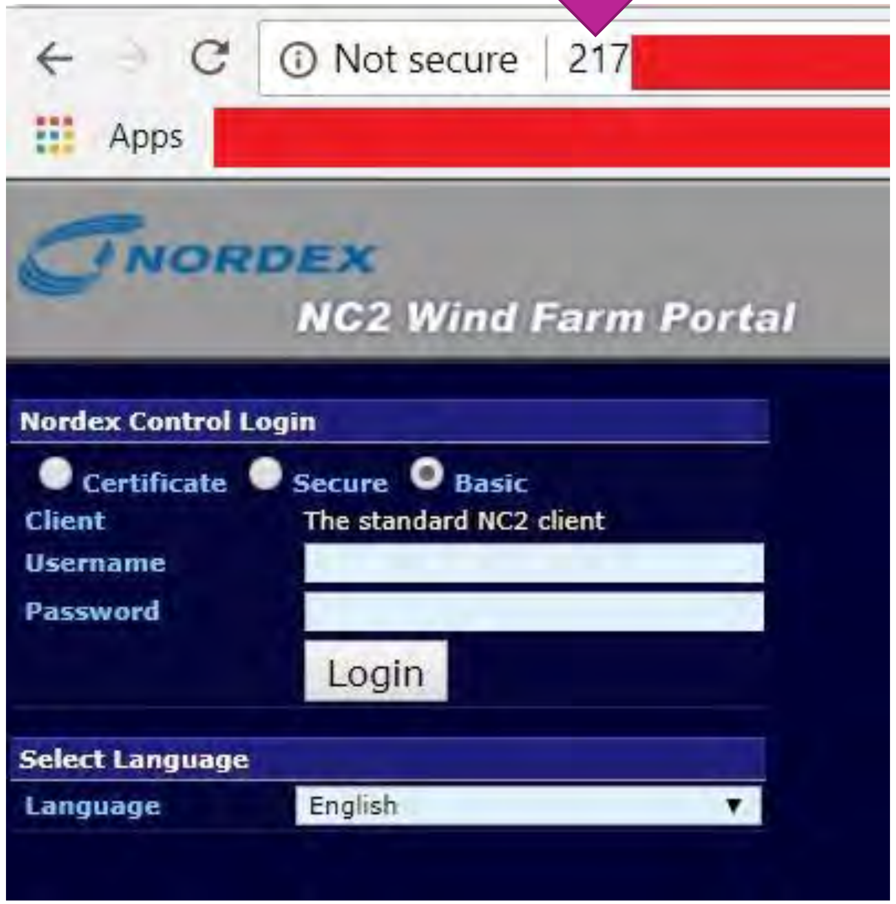
```
...=3D"cs80D9435B"><span
class=3D"cs19=..C3E152">E-mail: <a
href=3D"mailto:[redacted]"><span
class=3D"cs2=..50A6940">[redacted]</span></a>
</span></p><p class=3D"csGB..%80D9435B"=..><span
class=3D"cs19C3E152">&nbsp;</span></p><p
class=3D"cs95E872D0"><span
c=..lass=3D"cs19C3E152">&nbsp;</span></p><p
cl.vœx>µ»‡7Á...¬..E..®<$....Ã,¬.".¬.7‡7‡....‰.….°
..G....>.*ass=3D"cs80D9435B"><span
class=3D"=..cs675EBA1">AVISO LEGAL</span></p><p
class=3D"cs80D9435B"><span class=3D"cs19=..C3E152">Este
mensaje va dirigido, de manera exclusiva, a su
destG...inatario y c=..ontiene informaci=C3=B3n
confidencial y sujeta al secreto profesional; cuya
d=..ivulgaci=C3=B3n no est=C3=A1 permitida por ley.
</span></p><p class=3D"cs80D=..9435B"><spG...an
class=3D"cs19C3E152">En caso de haber recibido&nbsp;
este mensa=..je por error, le rogamos que, de forma
inmediata, nos lo comunique mediante e=..ste medio o a
trav=C3=A9s del tel=CG...3=A9fono (+34) 942[redacted] y
proceda a s=..u eliminaci=C3=B3n. Asimismo, le
comunicamos que la distribuci=C3=B3n, copia=.. o
```

IOT & Critical Infrastructure

“admin-electro…..”



```
GET /level/15/exec/-/sh/run/CR HTTP/1.1
Host: 64.[redacted]
Authorization: Basic YWRtaW4tZWxlY3Ryb[redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: deflate, gzip, identity
Accept-Language: en-US;q=0.6,en;q=0.4
Referer: http://64.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:9.0.1) Gecko/20100101 Firefox/9.0.1
```



Not secure | 217[redacted]

Apps [redacted]

Nordex Control Login

○ Certificate ○ Secure ● Basic

Client: The standard NC2 client

Username:

Password:

Login

Select Language

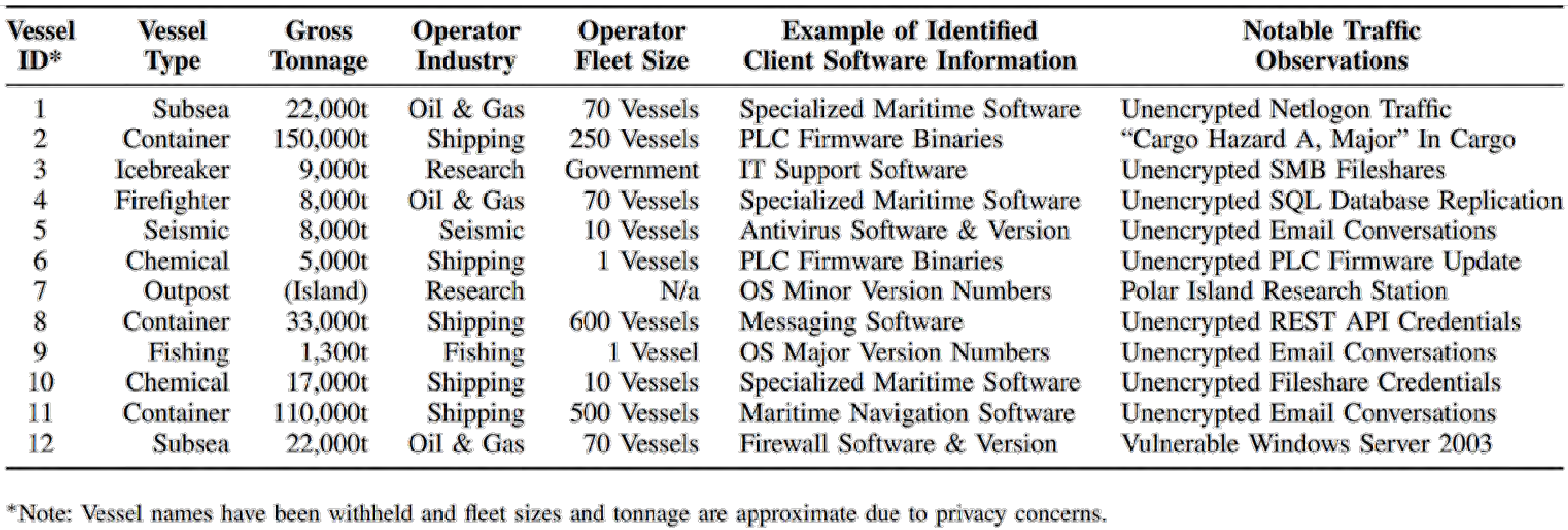
Language: English ▾

Maritime

Case Study: 100 Random Ships

Art: *Rodney's Fleet Taking in Prizes After the Moonlight Battle,* Dominic Serres, Public Domain

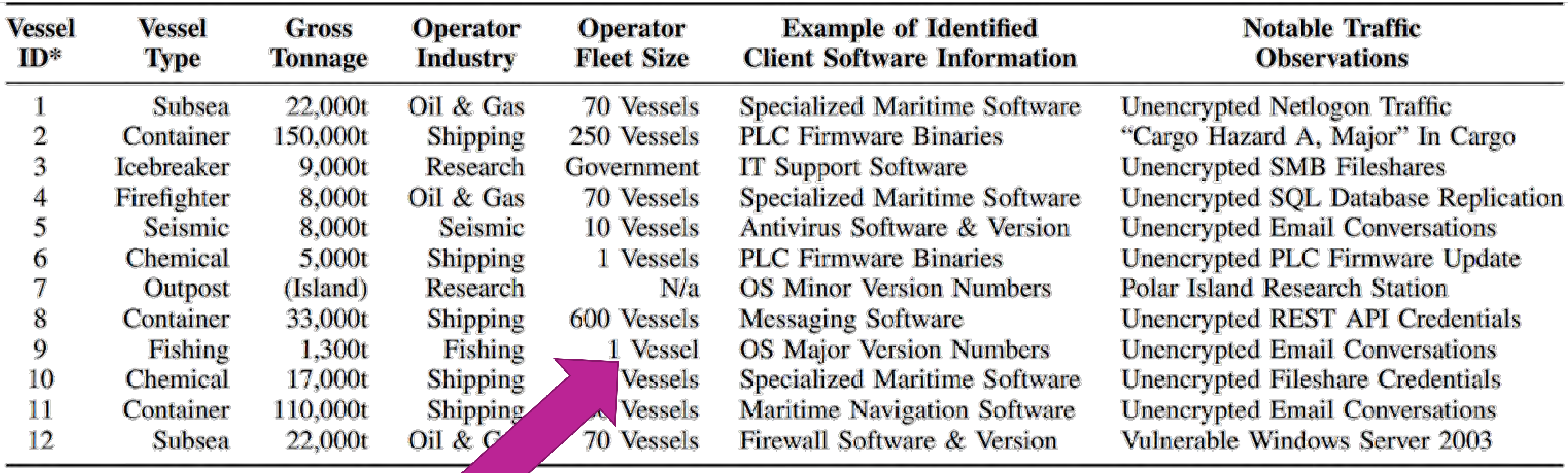
~10% of Vessels Identifiable



Vessel ID*	Vessel Type	Gross Tonnage	Operator Industry	Operator Fleet Size	Example of Identified Client Software Information	Notable Traffic Observations
1	Subsea	22,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted Netlogon Traffic
2	Container	150,000t	Shipping	250 Vessels	PLC Firmware Binaries	"Cargo Hazard A, Major" In Cargo
3	Icebreaker	9,000t	Research	Government	IT Support Software	Unencrypted SMB Fileshares
4	Firefighter	8,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted SQL Database Replication
5	Seismic	8,000t	Seismic	10 Vessels	Antivirus Software & Version	Unencrypted Email Conversations
6	Chemical	5,000t	Shipping	1 Vessels	PLC Firmware Binaries	Unencrypted PLC Firmware Update
7	Outpost	(Island)	Research	N/a	OS Minor Version Numbers	Polar Island Research Station
8	Container	33,000t	Shipping	600 Vessels	Messaging Software	Unencrypted REST API Credentials
9	Fishing	1,300t	Fishing	1 Vessel	OS Major Version Numbers	Unencrypted Email Conversations
10	Chemical	17,000t	Shipping	10 Vessels	Specialized Maritime Software	Unencrypted Fileshare Credentials
11	Container	110,000t	Shipping	500 Vessels	Maritime Navigation Software	Unencrypted Email Conversations
12	Subsea	22,000t	Oil & Gas	70 Vessels	Firewall Software & Version	Vulnerable Windows Server 2003

*Note: Vessel names have been withheld and fleet sizes and tonnage are approximate due to privacy concerns.

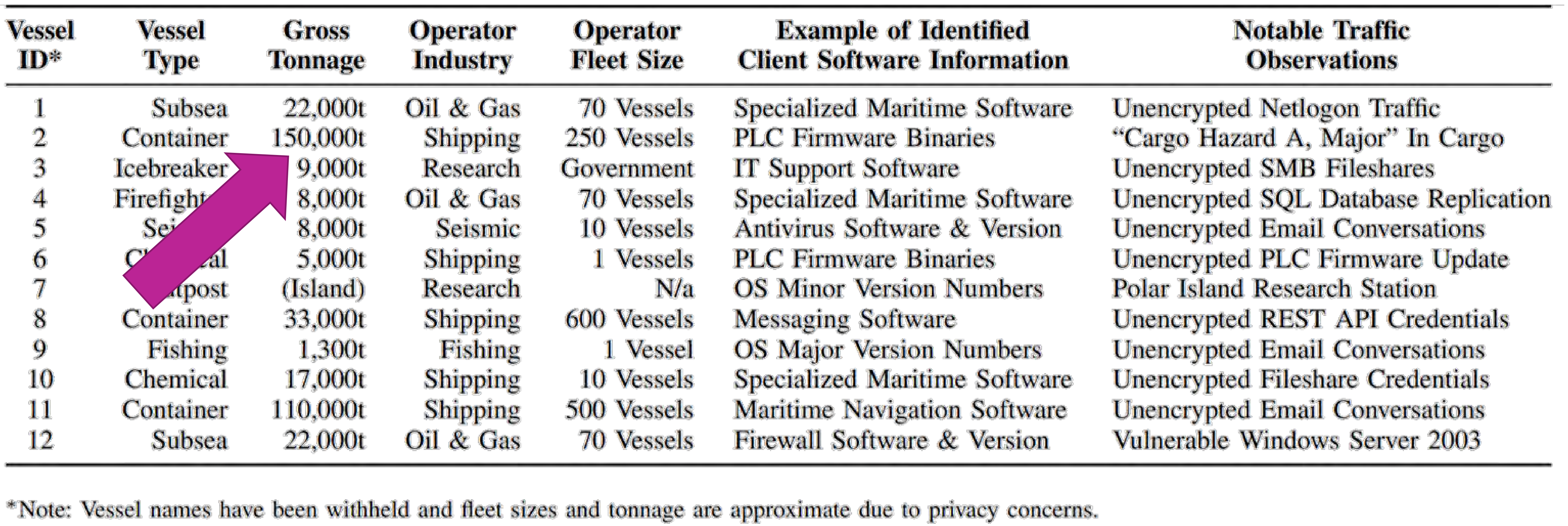
~10% of Vessels Identifiable



Vessel ID*	Vessel Type	Gross Tonnage	Operator Industry	Operator Fleet Size	Example of Identified Client Software Information	Notable Traffic Observations
1	Subsea	22,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted Netlogon Traffic
2	Container	150,000t	Shipping	250 Vessels	PLC Firmware Binaries	"Cargo Hazard A, Major" In Cargo
3	Icebreaker	9,000t	Research	Government	IT Support Software	Unencrypted SMB Fileshares
4	Firefighter	8,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted SQL Database Replication
5	Seismic	8,000t	Seismic	10 Vessels	Antivirus Software & Version	Unencrypted Email Conversations
6	Chemical	5,000t	Shipping	1 Vessels	PLC Firmware Binaries	Unencrypted PLC Firmware Update
7	Outpost	(Island)	Research	N/a	OS Minor Version Numbers	Polar Island Research Station
8	Container	33,000t	Shipping	600 Vessels	Messaging Software	Unencrypted REST API Credentials
9	Fishing	1,300t	Fishing	1 Vessel	OS Major Version Numbers	Unencrypted Email Conversations
10	Chemical	17,000t	Shipping	[illegible] Vessels	Specialized Maritime Software	Unencrypted Fileshare Credentials
11	Container	110,000t	Shipping	[illegible] Vessels	Maritime Navigation Software	Unencrypted Email Conversations
12	Subsea	22,000t	Oil & G[illegible]	70 Vessels	Firewall Software & Version	Vulnerable Windows Server 2003

*Note: Vessel names have been withheld and fleet sizes and tonnage are approximate due to privacy concerns.

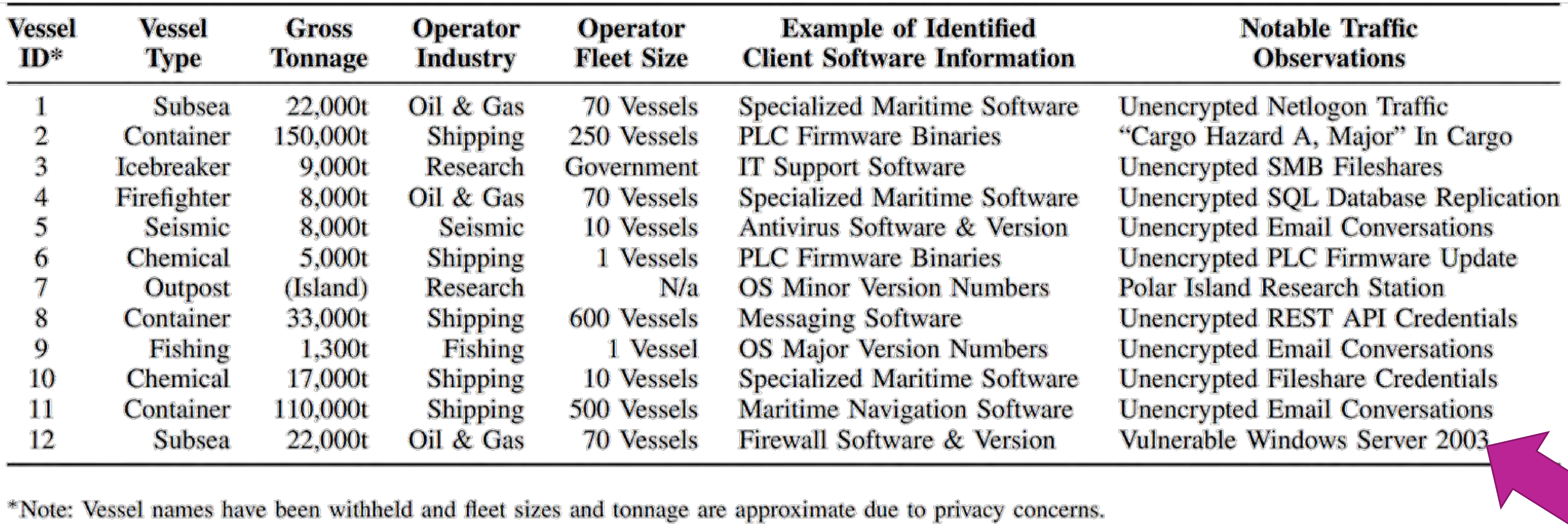
~10% of Vessels Identifiable



Vessel ID*	Vessel Type	Gross Tonnage	Operator Industry	Operator Fleet Size	Example of Identified Client Software Information	Notable Traffic Observations
1	Subsea	22,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted Netlogon Traffic
2	Container	150,000t	Shipping	250 Vessels	PLC Firmware Binaries	"Cargo Hazard A, Major" In Cargo
3	Icebreaker	9,000t	Research	Government	IT Support Software	Unencrypted SMB Fileshares
4	Firefighter	8,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted SQL Database Replication
5	Seismic	8,000t	Seismic	10 Vessels	Antivirus Software & Version	Unencrypted Email Conversations
6	Chemical	5,000t	Shipping	1 Vessels	PLC Firmware Binaries	Unencrypted PLC Firmware Update
7	Outpost	(Island)	Research	N/a	OS Minor Version Numbers	Polar Island Research Station
8	Container	33,000t	Shipping	600 Vessels	Messaging Software	Unencrypted REST API Credentials
9	Fishing	1,300t	Fishing	1 Vessel	OS Major Version Numbers	Unencrypted Email Conversations
10	Chemical	17,000t	Shipping	10 Vessels	Specialized Maritime Software	Unencrypted Fileshare Credentials
11	Container	110,000t	Shipping	500 Vessels	Maritime Navigation Software	Unencrypted Email Conversations
12	Subsea	22,000t	Oil & Gas	70 Vessels	Firewall Software & Version	Vulnerable Windows Server 2003

*Note: Vessel names have been withheld and fleet sizes and tonnage are approximate due to privacy concerns.

~10% of Vessels Identifiable



Vessel ID*	Vessel Type	Gross Tonnage	Operator Industry	Operator Fleet Size	Example of Identified Client Software Information	Notable Traffic Observations
1	Subsea	22,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted Netlogon Traffic
2	Container	150,000t	Shipping	250 Vessels	PLC Firmware Binaries	“Cargo Hazard A, Major” In Cargo
3	Icebreaker	9,000t	Research	Government	IT Support Software	Unencrypted SMB Fileshares
4	Firefighter	8,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted SQL Database Replication
5	Seismic	8,000t	Seismic	10 Vessels	Antivirus Software & Version	Unencrypted Email Conversations
6	Chemical	5,000t	Shipping	1 Vessels	PLC Firmware Binaries	Unencrypted PLC Firmware Update
7	Outpost	(Island)	Research	N/a	OS Minor Version Numbers	Polar Island Research Station
8	Container	33,000t	Shipping	600 Vessels	Messaging Software	Unencrypted REST API Credentials
9	Fishing	1,300t	Fishing	1 Vessel	OS Major Version Numbers	Unencrypted Email Conversations
10	Chemical	17,000t	Shipping	10 Vessels	Specialized Maritime Software	Unencrypted Fileshare Credentials
11	Container	110,000t	Shipping	500 Vessels	Maritime Navigation Software	Unencrypted Email Conversations
12	Subsea	22,000t	Oil & Gas	70 Vessels	Firewall Software & Version	Vulnerable Windows Server 2003

*Note: Vessel names have been withheld and fleet sizes and tonnage are approximate due to privacy concerns.

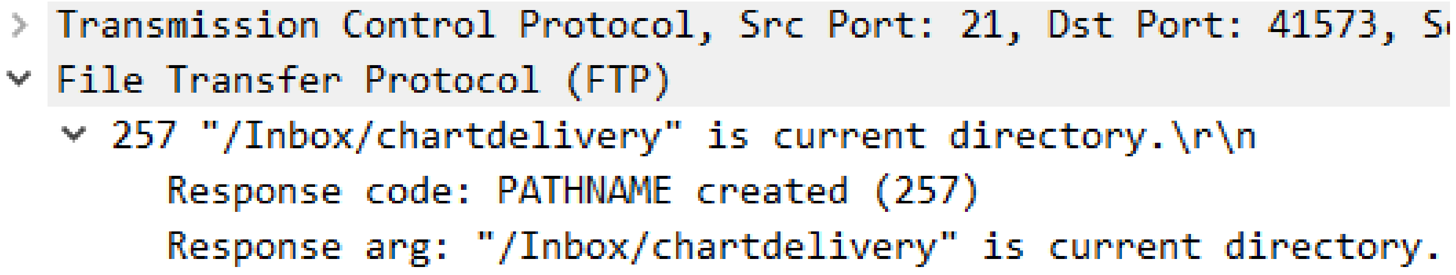
ECDIS

- Electronic Chart Display and Information System
- Standard Formats Support Cryptographic Verification
  - But we observed more than 15,000 unsigned charts files in transit
- Many also use proprietary formats

Photo: *Navigation system used on an oil tanker*, Hervé Cozanet, Wikimedia Commons, CC BY-SA 3.0

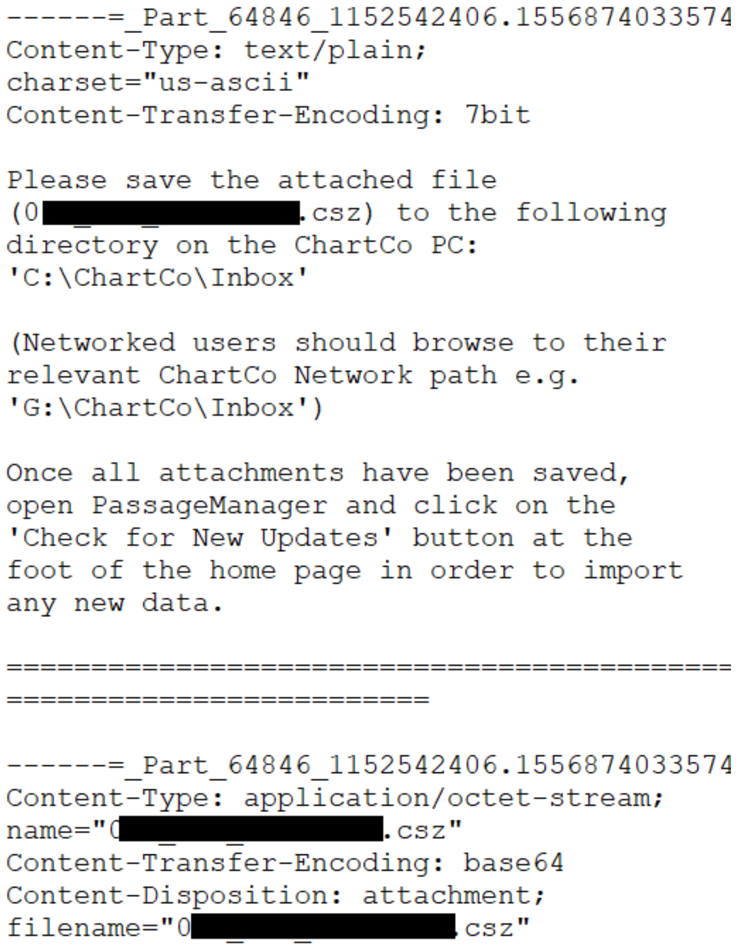
Listening Can Be Enough...

Publicly Routable FTP Fileshares



```
> Transmission Control Protocol, Src Port: 21, Dst Port: 41573, S
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.
```

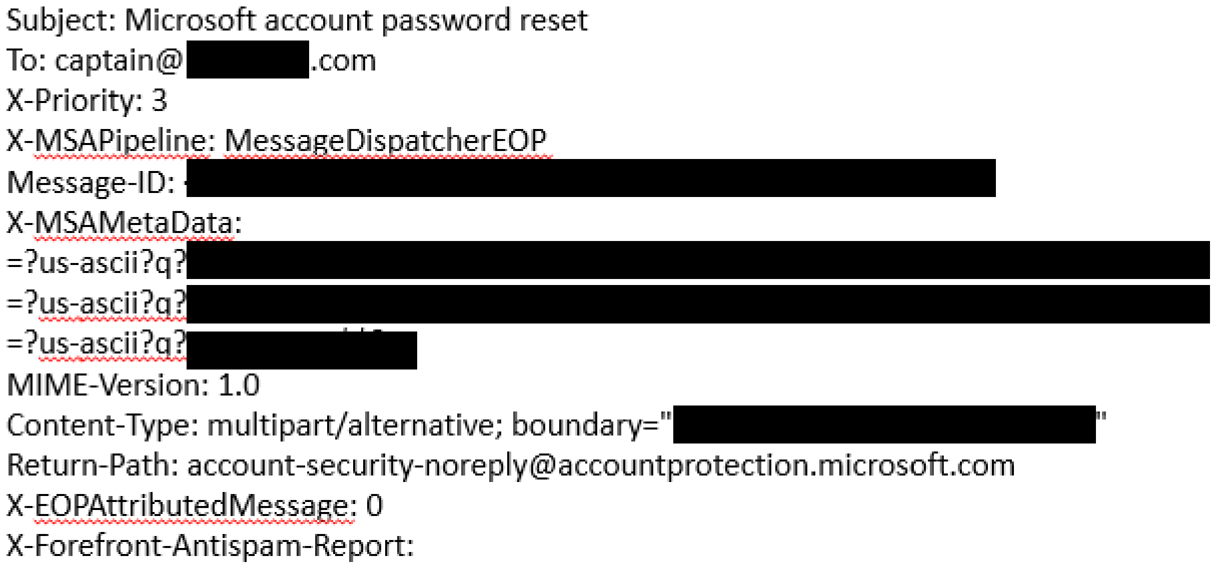
Chart Update Via Email



```
------=_Part_64846_1152542406.1556874033574
Content-Type: text/plain;
charset="us-ascii"
Content-Transfer-Encoding: 7bit

Please save the attached file
(0[redacted].csz) to the following
directory on the ChartCo PC:
'C:\ChartCo\Inbox'

(Networked users should browse to their
relevant ChartCo Network path e.g.
'G:\ChartCo\Inbox')

Once all attachments have been saved,
open PassageManager and click on the
'Check for New Updates' button at the
foot of the home page in order to import
any new data.

==========================================
========================

------=_Part_64846_1152542406.1556874033574
Content-Type: application/octet-stream;
name="[redacted].csz"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="0[redacted]csz"
```

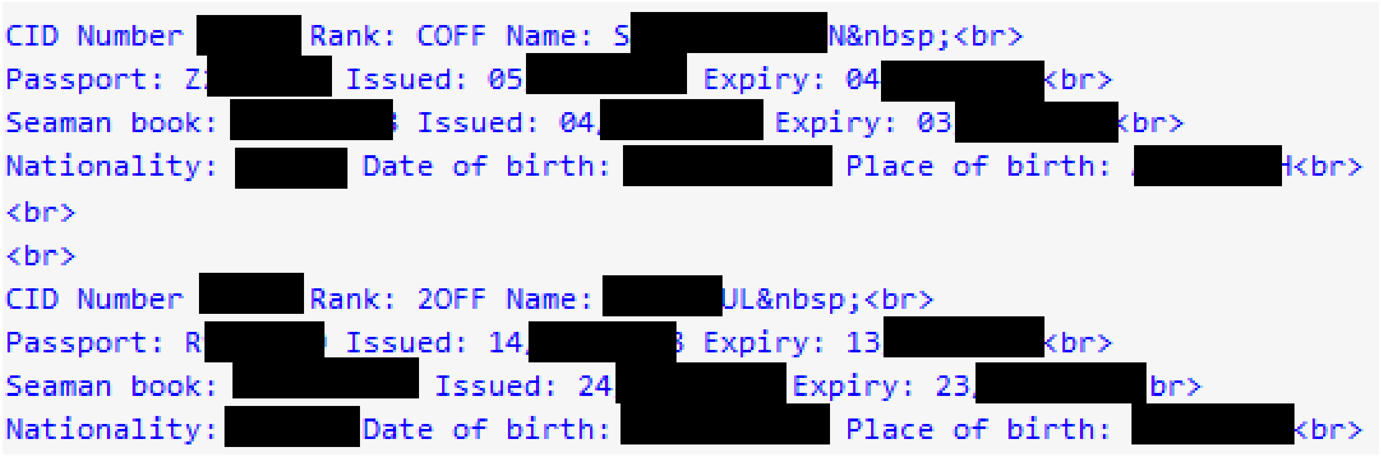
General Privacy

Captain of Billionaire's Yacht – MSFT Acct.



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 Transmitted to Port Authorities



```
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>
```

Aviation

Where Did the Planes Go????

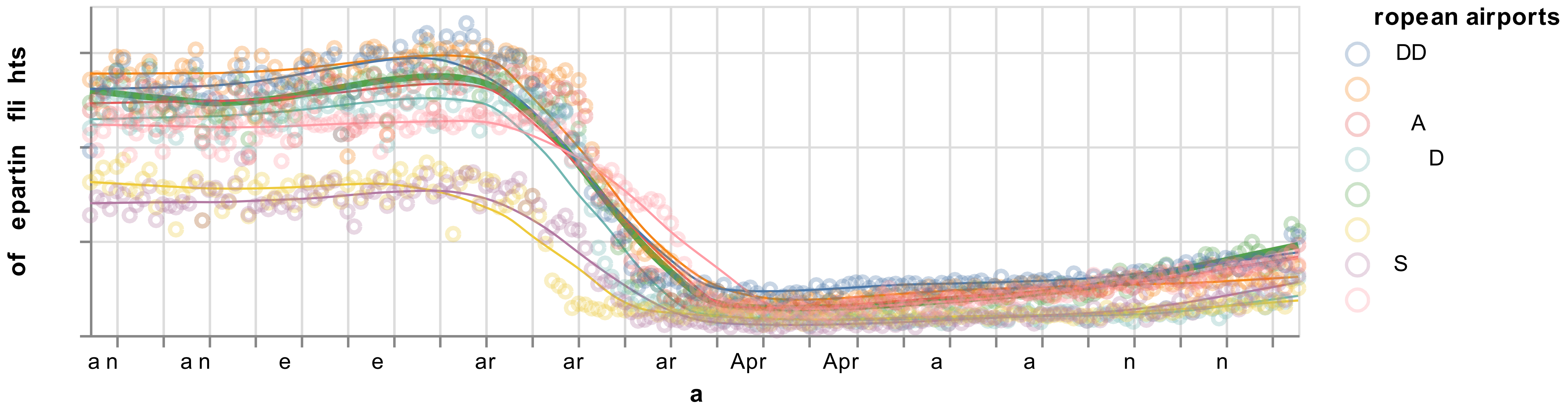
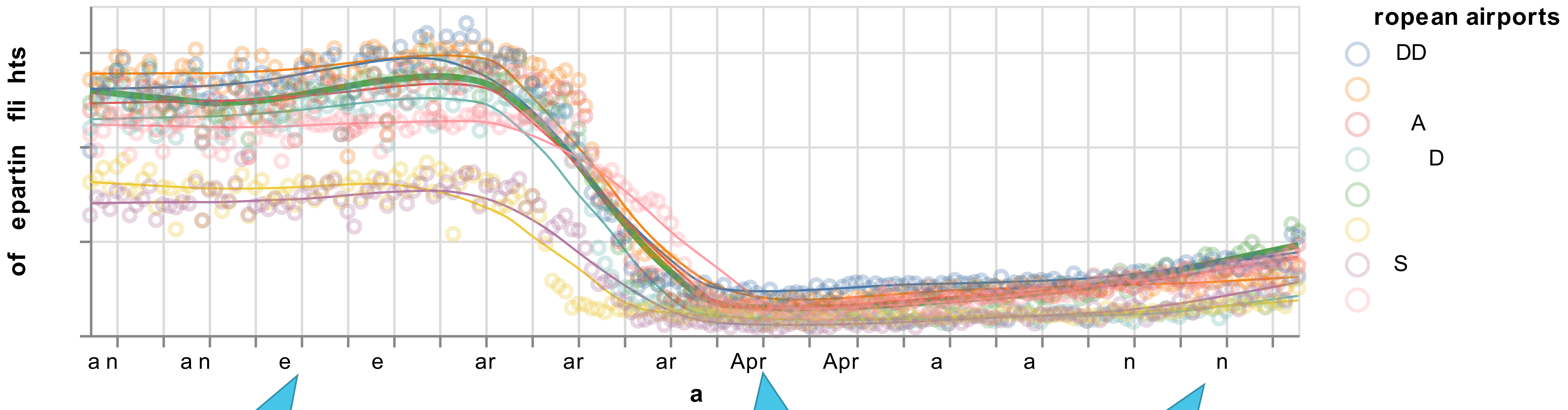


Chart: Xavier Olive, *Impact of COVID-19 on worldwide aviation*, https://traffic-viz.github.io/scenarios/covid19.html

Where Did the Planes Go????



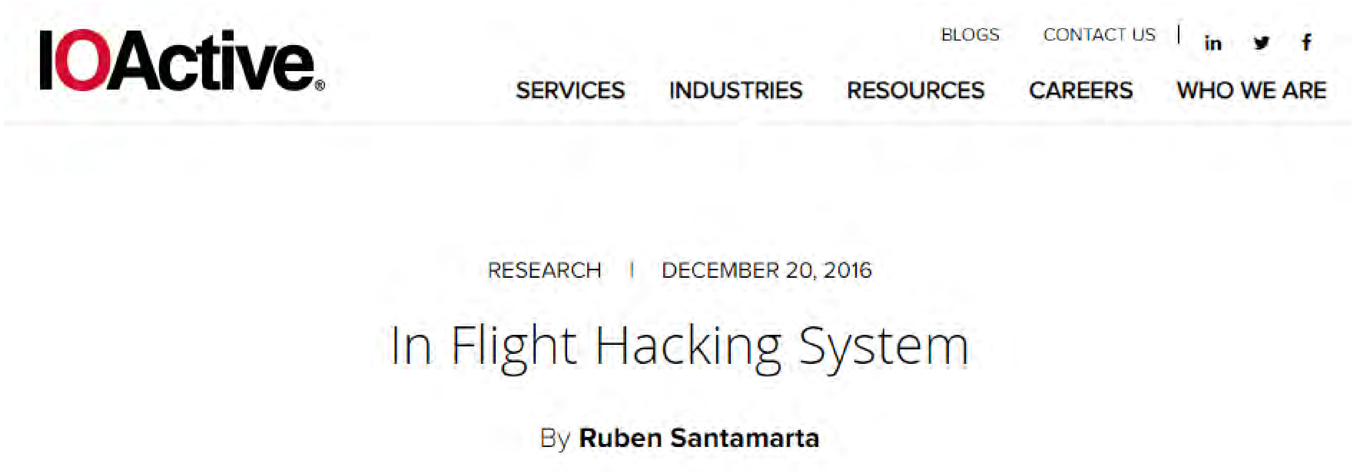
Lots of Useless Nonsense (e.g. Instagram Traffic)

Almost Entirely Essential Traffic

People Who Really Need to Travel

Chart: Xavier Olive, *Impact of COVID-19 on worldwide aviation*, https://traffic-viz.github.io/scenarios/covid19.html

Crossing the "Red Line"



IOActive

BLOGS CONTACT US | in 🐦 f

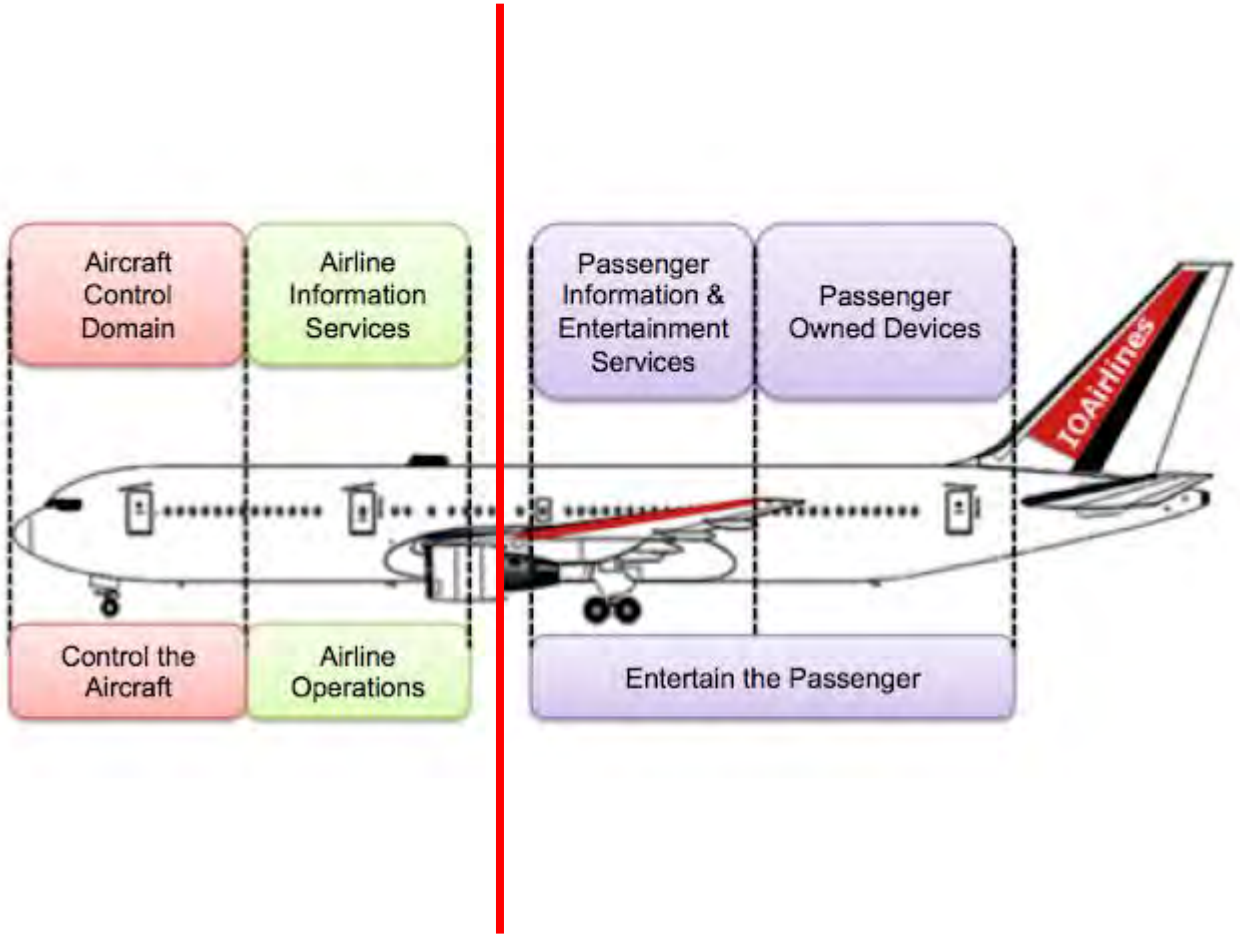
SERVICES INDUSTRIES RESOURCES CAREERS WHO WE ARE

RESEARCH | DECEMBER 20, 2016

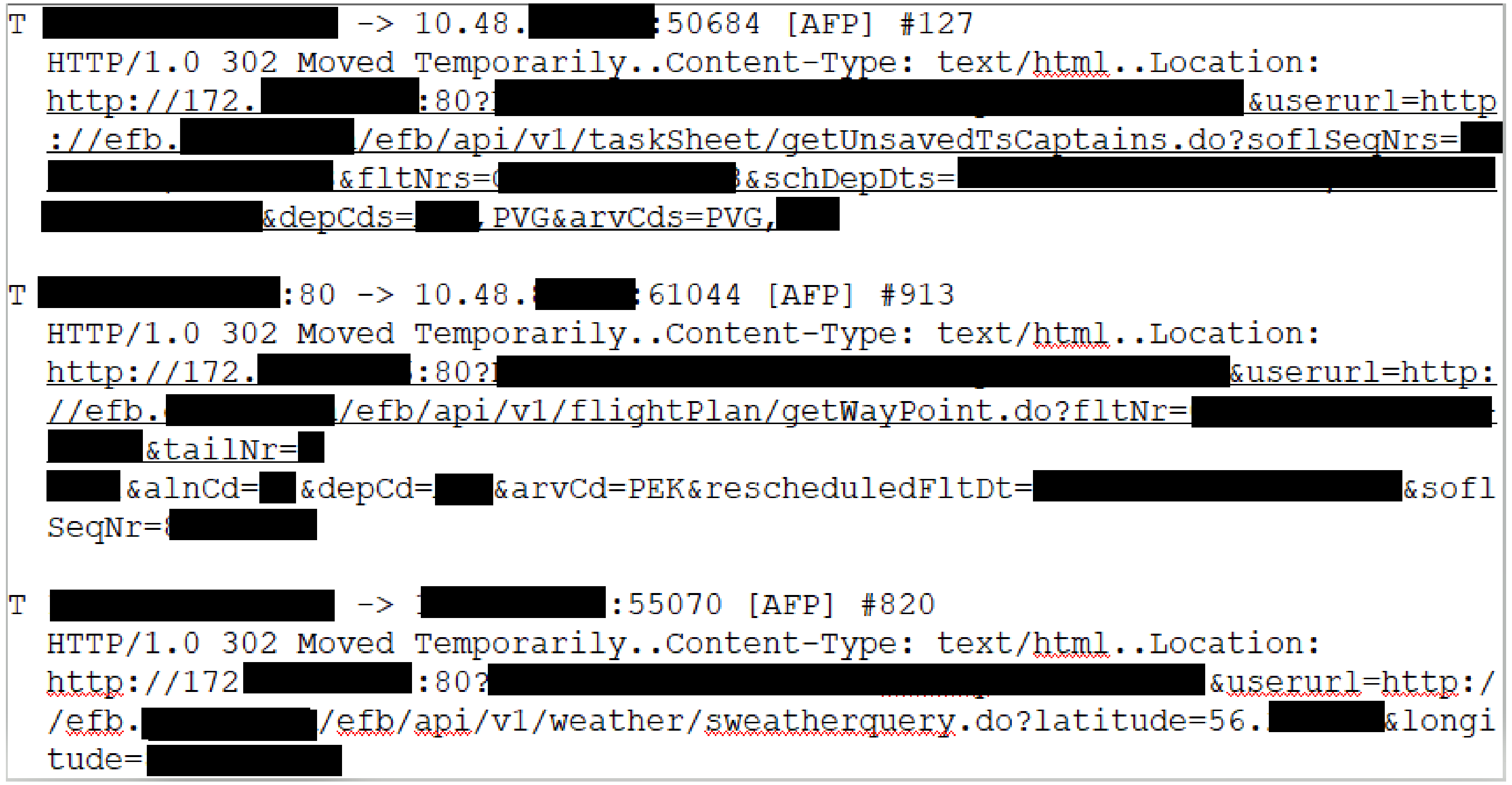
In Flight Hacking System

By **Ruben Santamarta**

"A primary concern is the sharing of these SATCOM devices between different data domains, which could allow an attacker [...] to pivot from a compromised IFE to certain avionics"



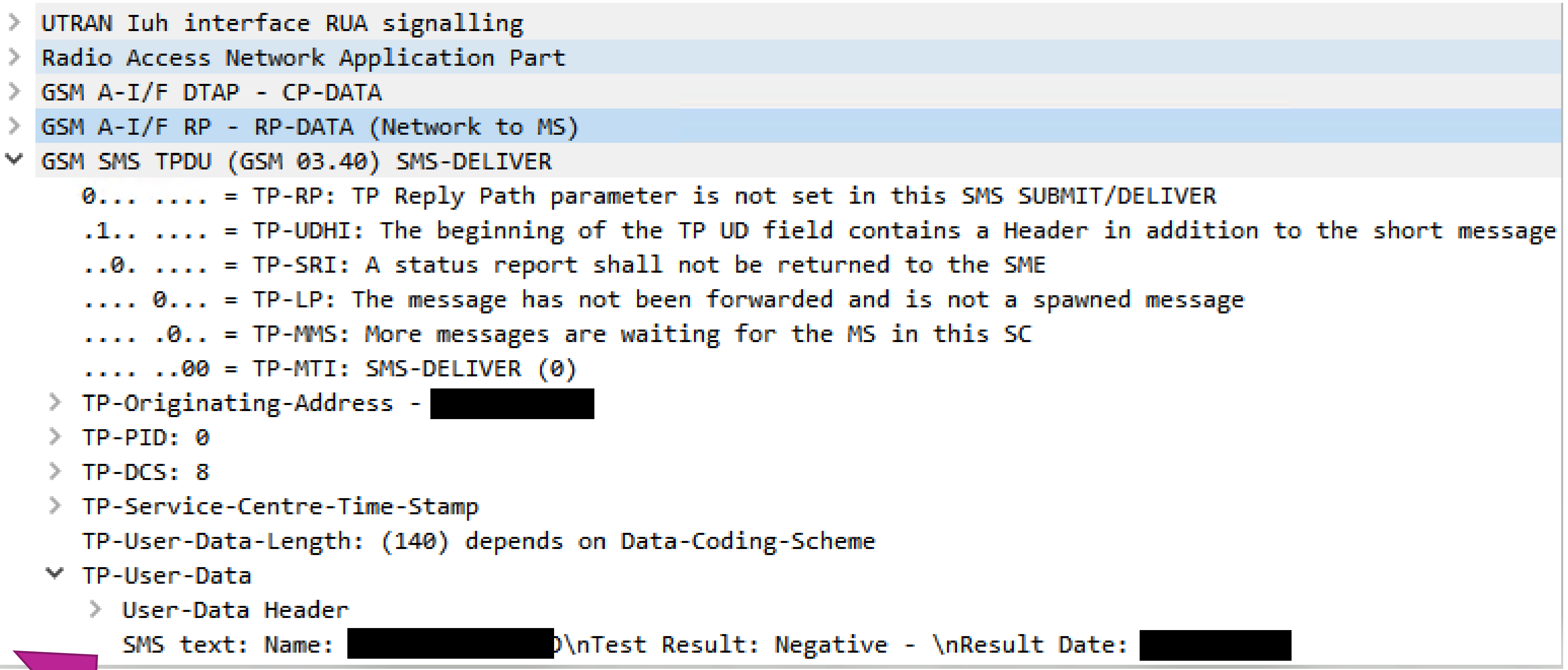
The Loneliest EFB



```
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]
```

Photo: *Gulfstream Aerospace G150*, Robert Frola, 2011, Flickr, GFDL.

GSM @ 30,000ft

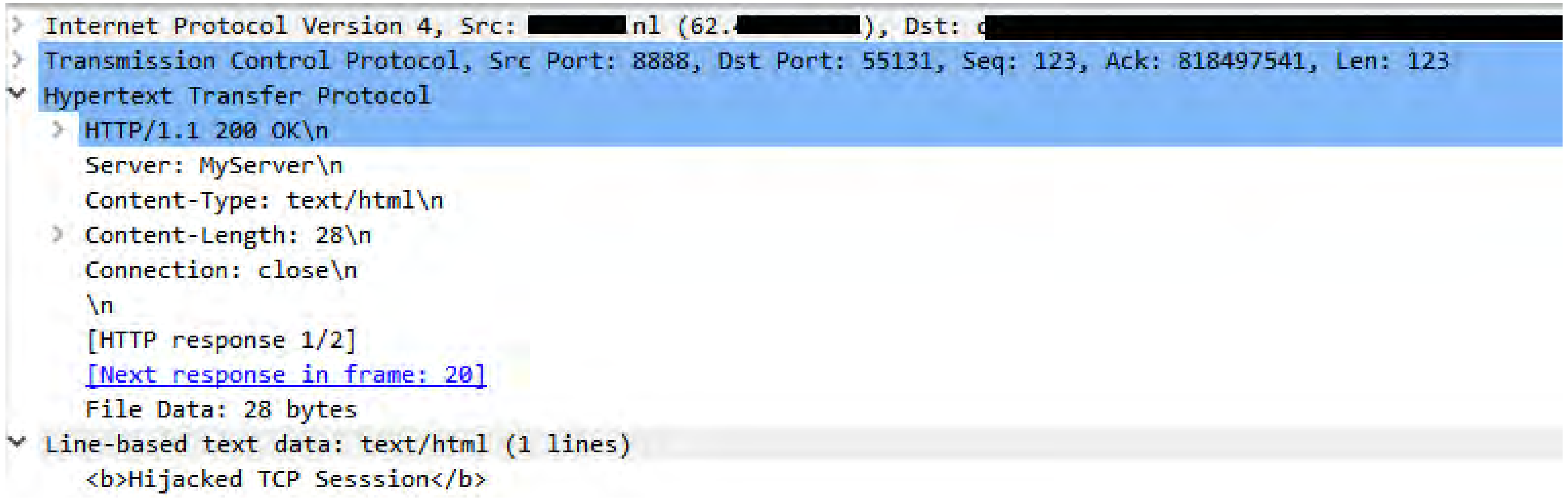


```
> UTRAN Iuh interface RUA signalling
> Radio Access Network Application Part
> GSM A-I/F DTAP - CP-DATA
> GSM A-I/F RP - RP-DATA (Network to MS)
v GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .1.. .... = TP-UDHI: The 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]
```

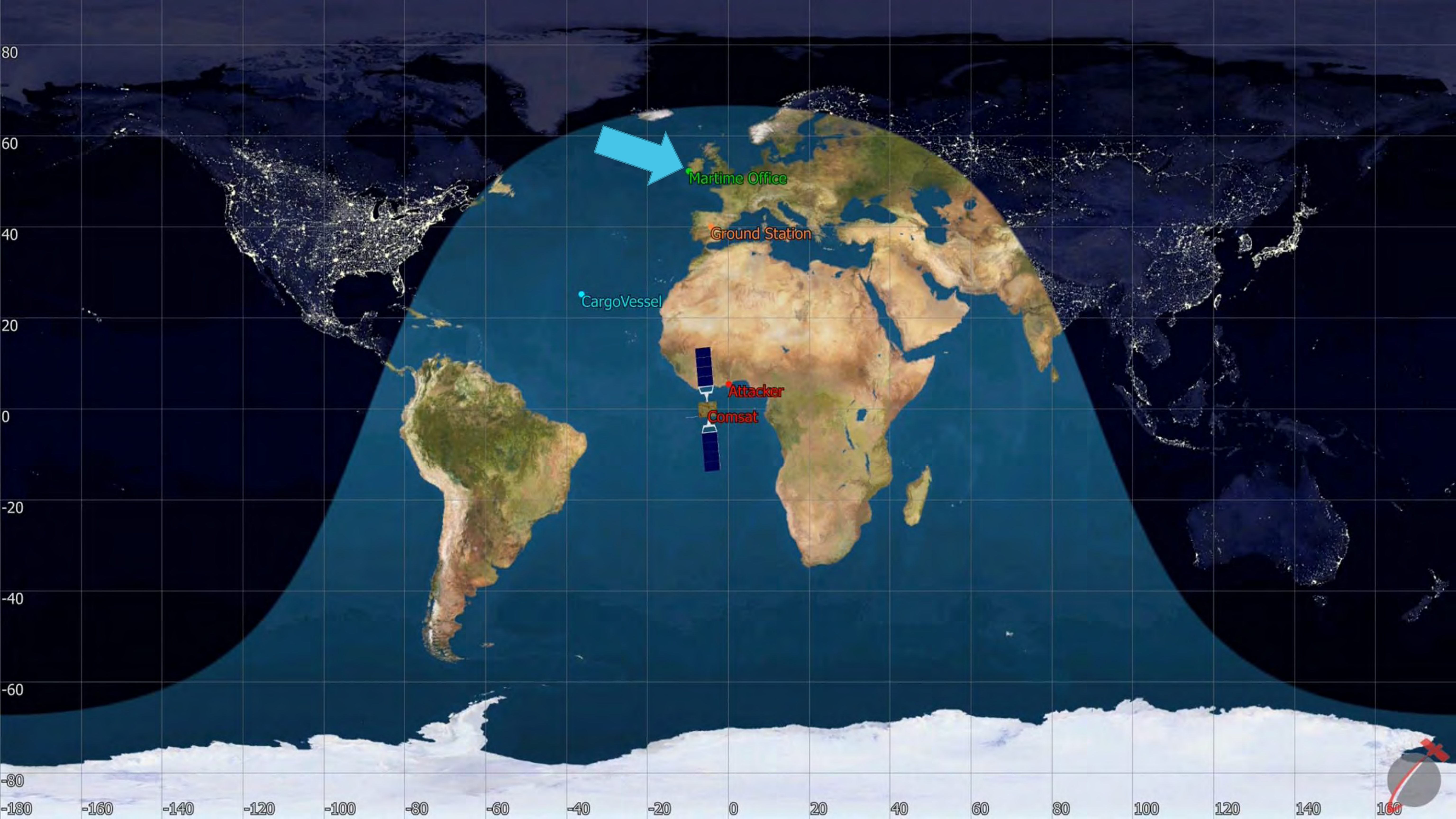
Active Attacks?

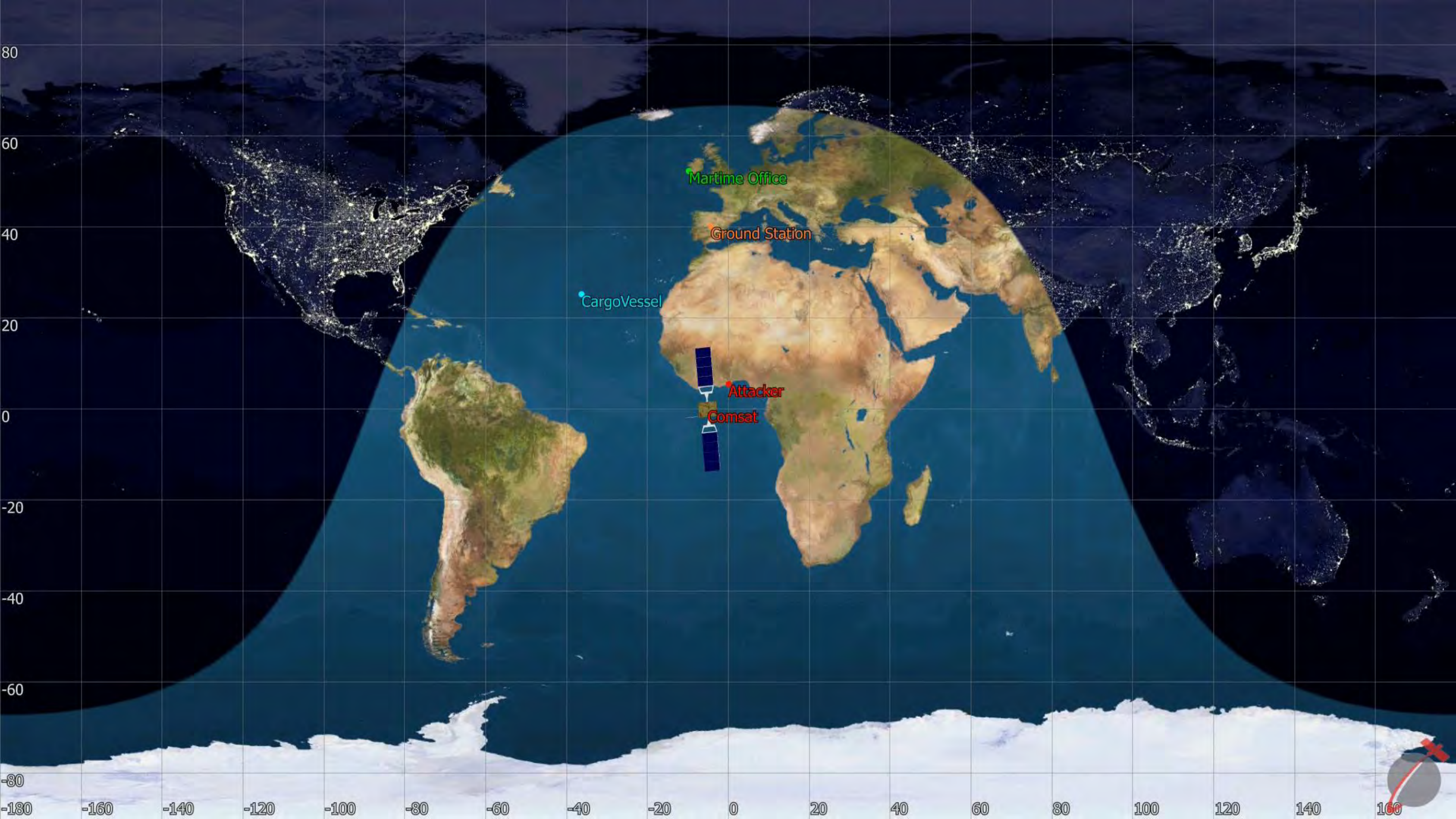
TCP Session Hijacking

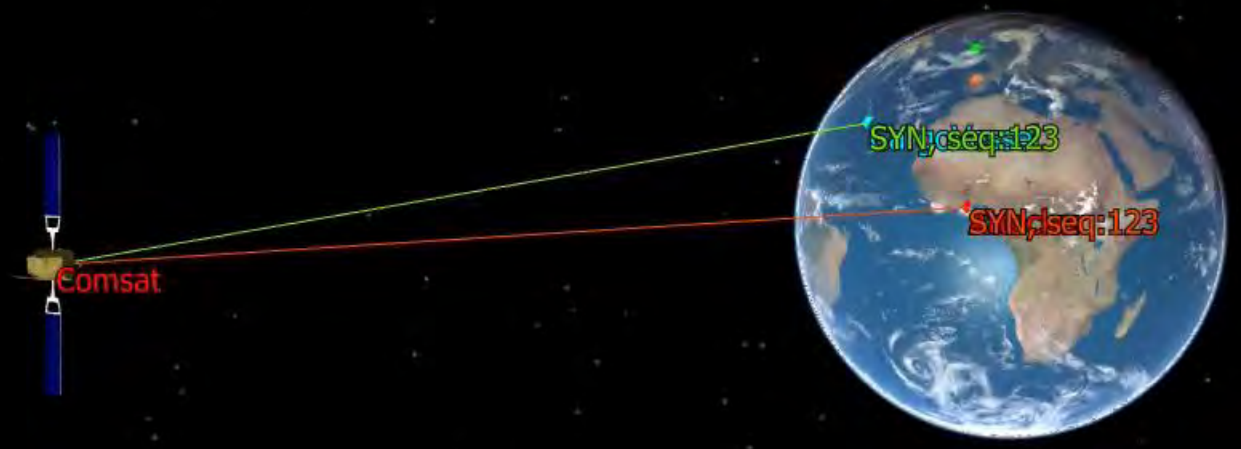
- Snoop TCP sequence numbers
- Impersonate satellite-terminal conversation endpoint
  - Possibly bi-directional, but more complex
- Network Requirements
  - IPs must be routable to attacker
  - No TCP sequence number altering proxies

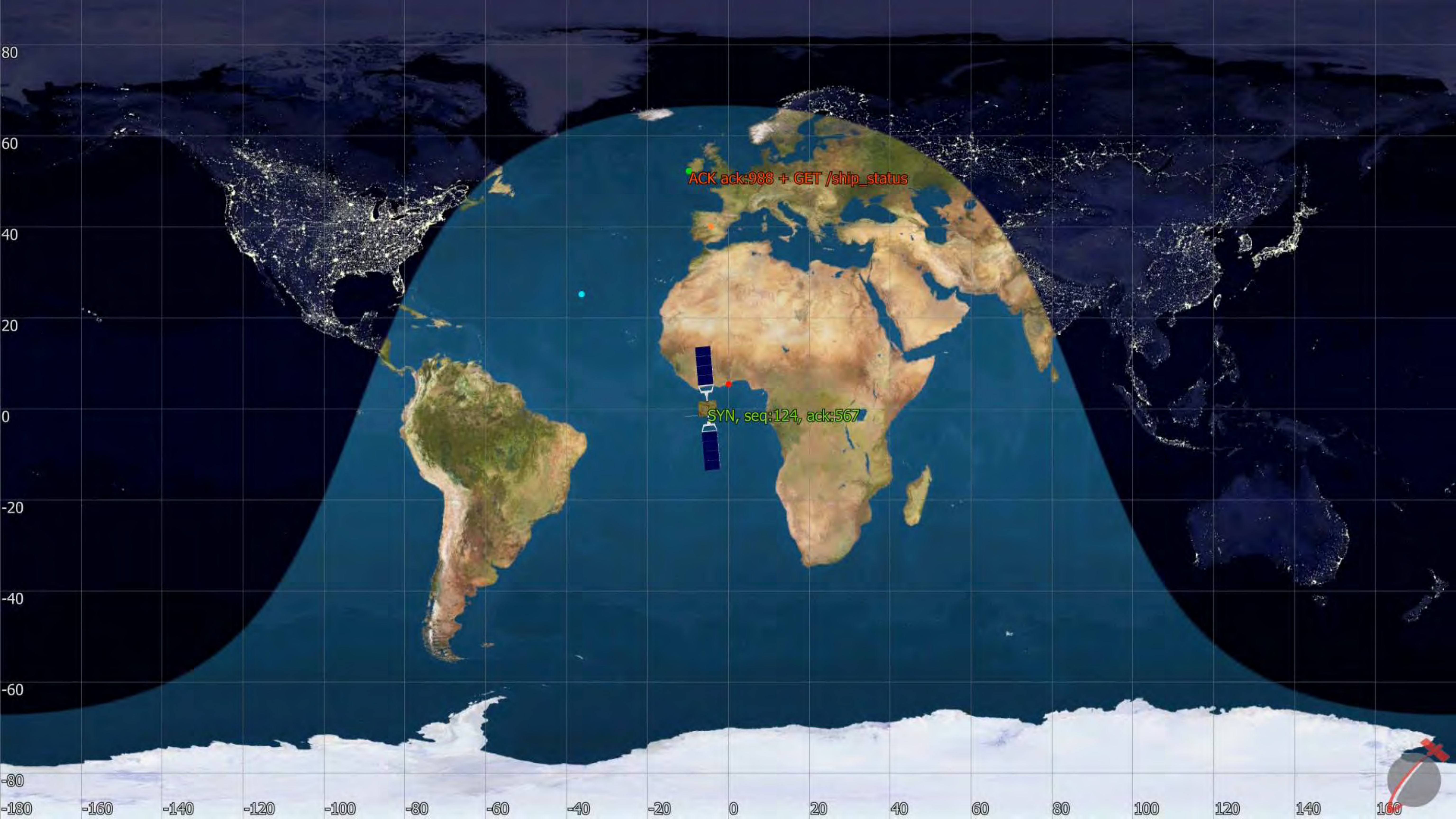


```
> Internet Protocol Version 4, Src: [redacted]nl (62.[redacted]), Dst: [redacted]
> Transmission Control Protocol, Src Port: 8888, Dst Port: 55131, Seq: 123, Ack: 818497541, Len: 123
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\n
    Server: MyServer\n
    Content-Type: text/html\n
  > Content-Length: 28\n
    Connection: close\n
    \n
    [HTTP response 1/2]
    [Next response in frame: 20]
    File Data: 28 bytes
v Line-based text data: text/html (1 lines)
    <b>Hijacked TCP Sesssion</b>
```


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
Martime Office
Ground Station
CargoVessel
Attacker
Comsat

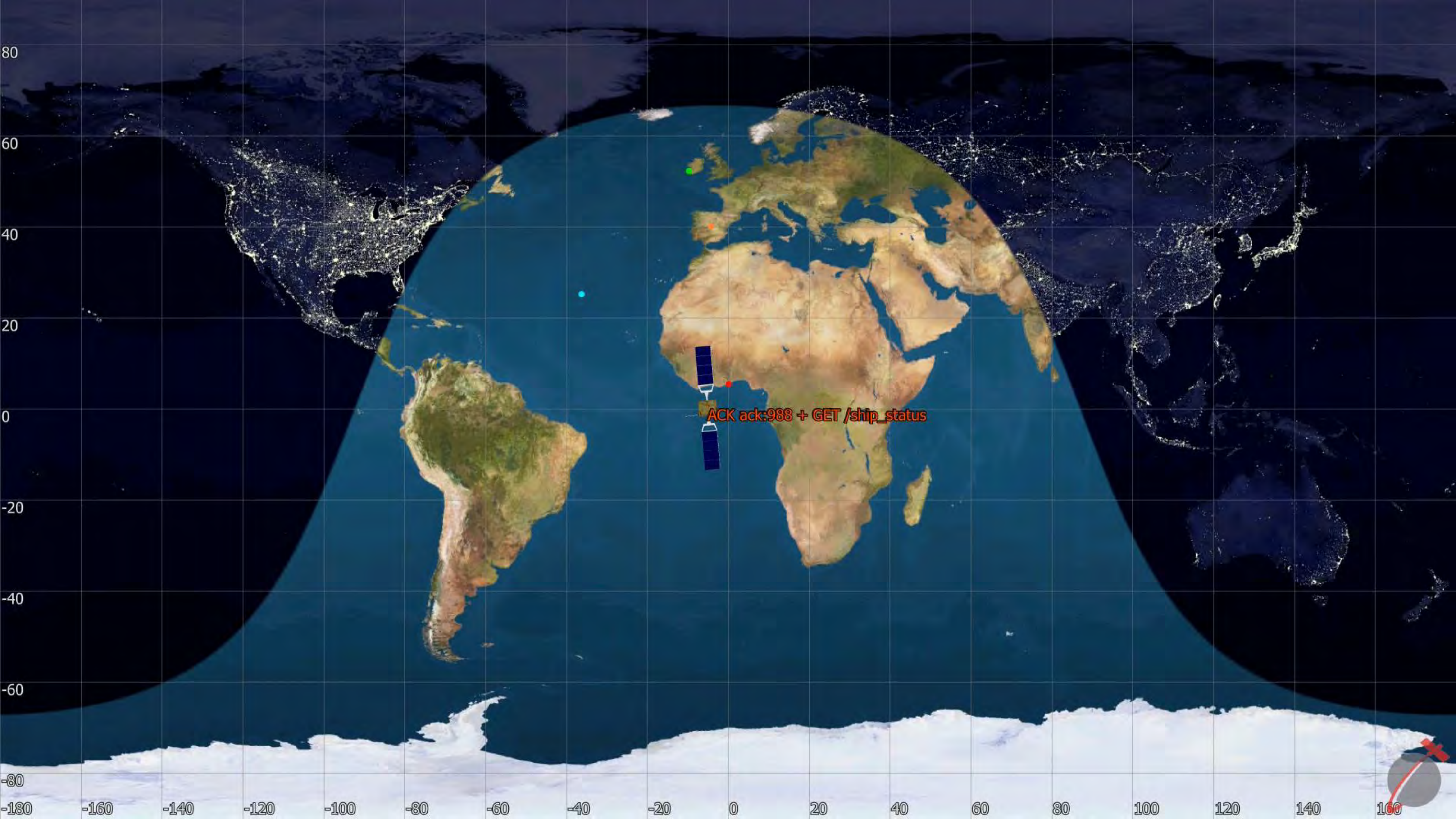

Martime Office
Ground Station
CargoVessel
Attacker
Comsat
80
60
40
20
0
-20
-40
-60
-80
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160

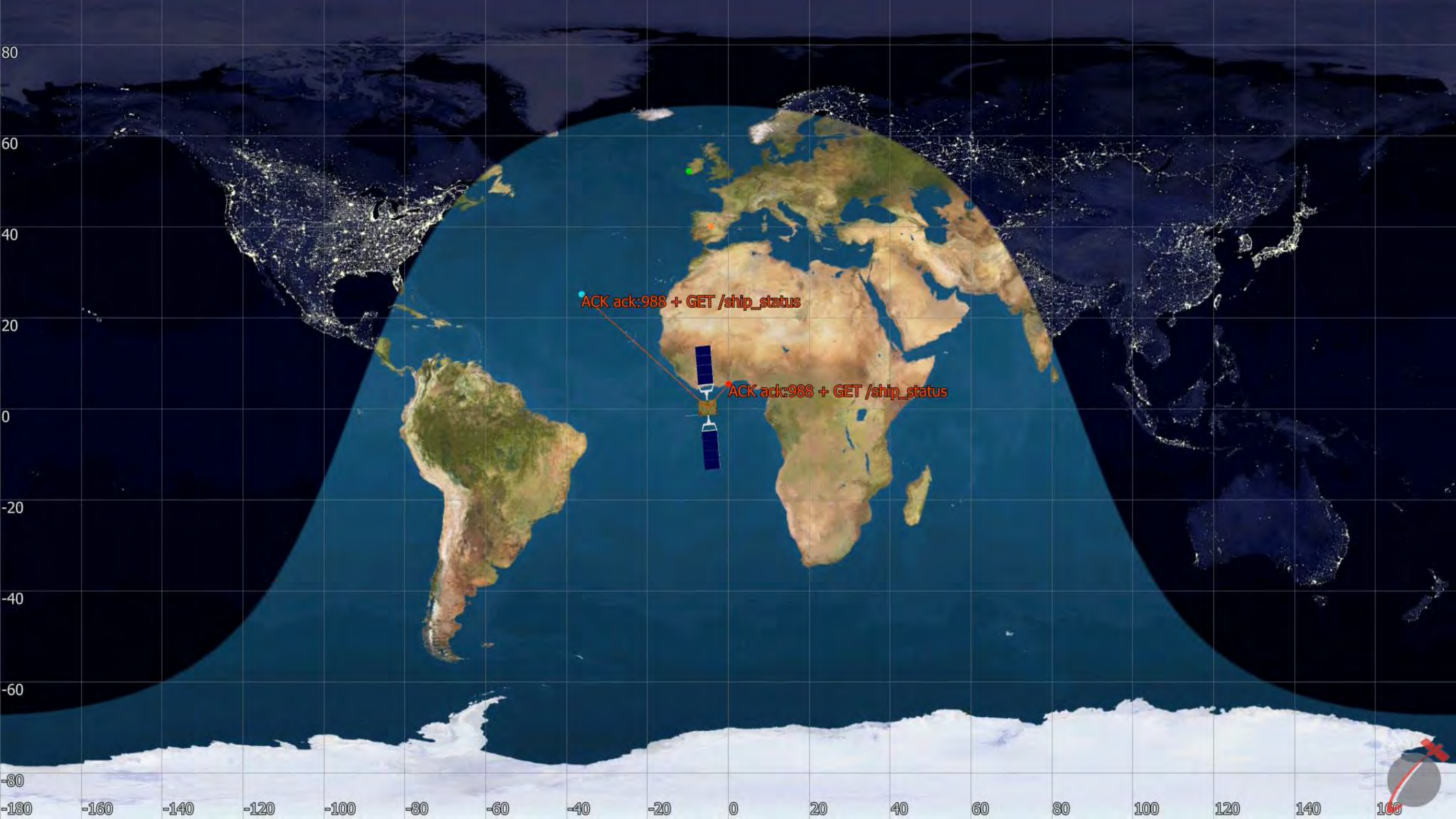

SYN, seq:123
SYN, seq:123
Comsat



ACK ack:988 + GET /ship_status

SYN, seq:124, ack:567


80
60
40
20
0
-20
-40
-60
-80
ACK ack:988 + GET /ship_status
-180
-160
-140
-120
-100
-80
-60
-40
-20
0
20
40
60
80
100
120
140
160



ACK ack:988 + GET /ship_status

ACK ack:988 + GET /ship_status

Ethics and Disclosure

Adhered to legal obligations in jurisdiction of data collection

- Data stored securely and only while needed
- Data was never shared with 3rd parties
- Encryption untouched
- Won’t “name and shame”

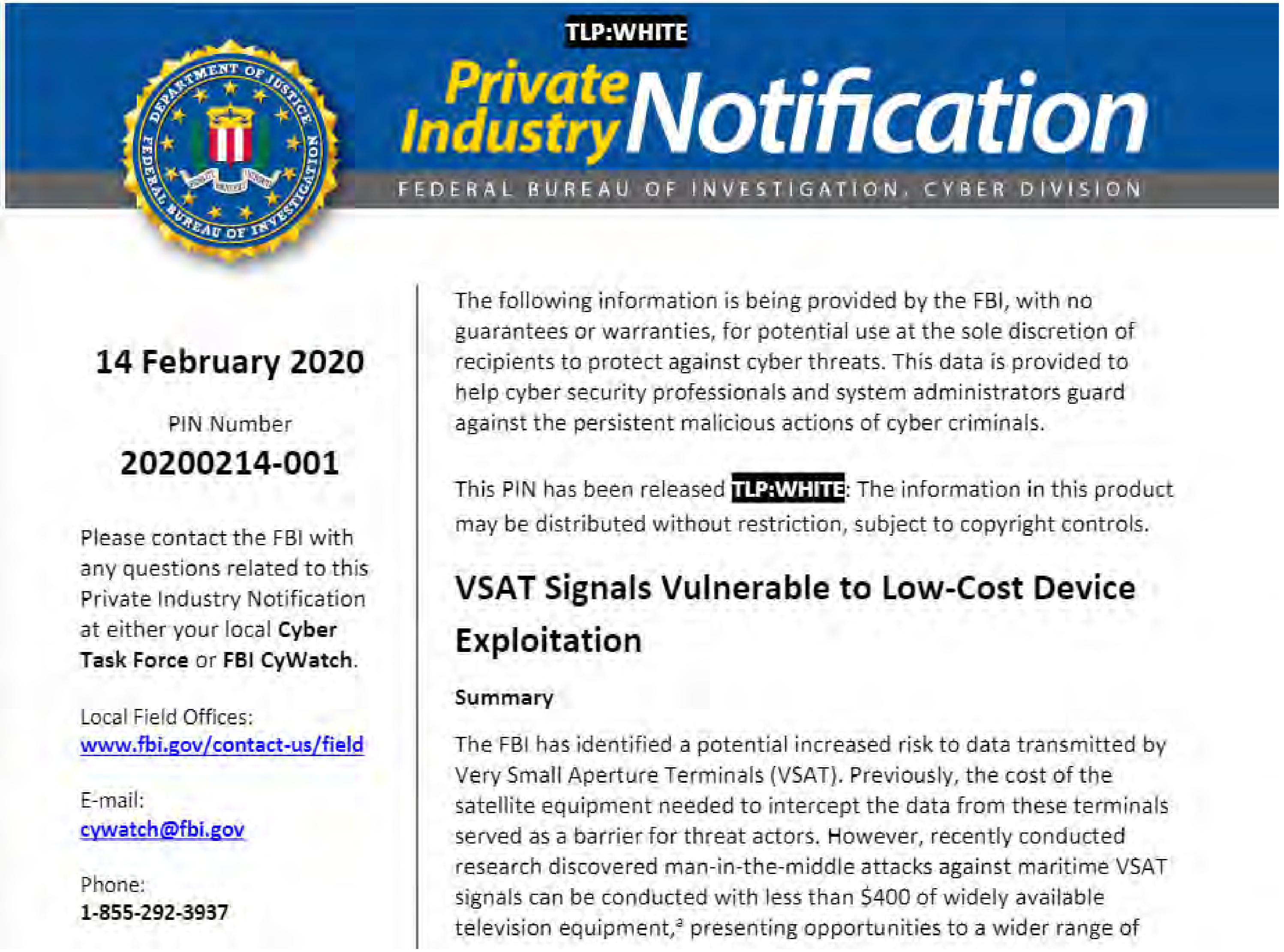
Followed responsible disclosure process

- Contacted satellite operators in 2019
- Reached out to some of the largest impacted customers

Vast majority of companies were receptive

- Shared findings directly to CISOs of several large orgs
- Unclear if any changes have been made…
- Only one organization threatened legal action if we published!

Thanks FBI!



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 February 2020

PIN Number

20200214-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

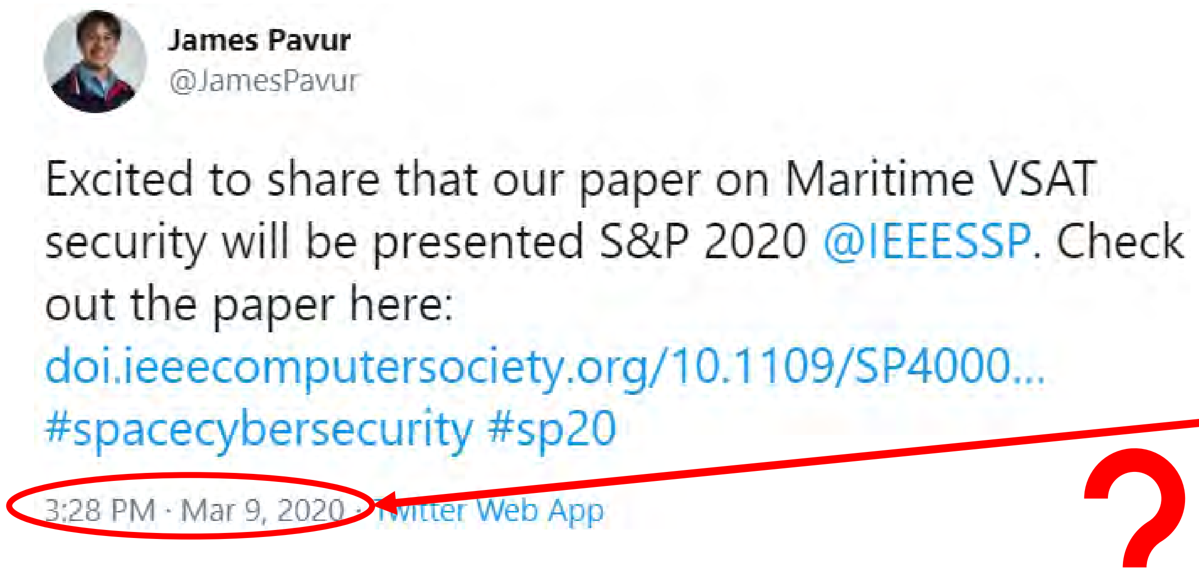
This PIN has been released **TLP:WHITE**: The information in this product may be distributed without restriction, subject to copyright controls.

VSAT Signals Vulnerable to Low-Cost Device Exploitation

Summary

The FBI has identified a potential increased risk to data transmitted by Very Small Aperture Terminals (VSAT). Previously, the cost of the satellite equipment needed to intercept the data from these terminals served as a barrier for threat actors. However, recently conducted research discovered man-in-the-middle attacks against maritime VSAT signals can be conducted with less than $400 of widely available television equipment,[a] presenting opportunities to a wider range of

Thanks FBI!

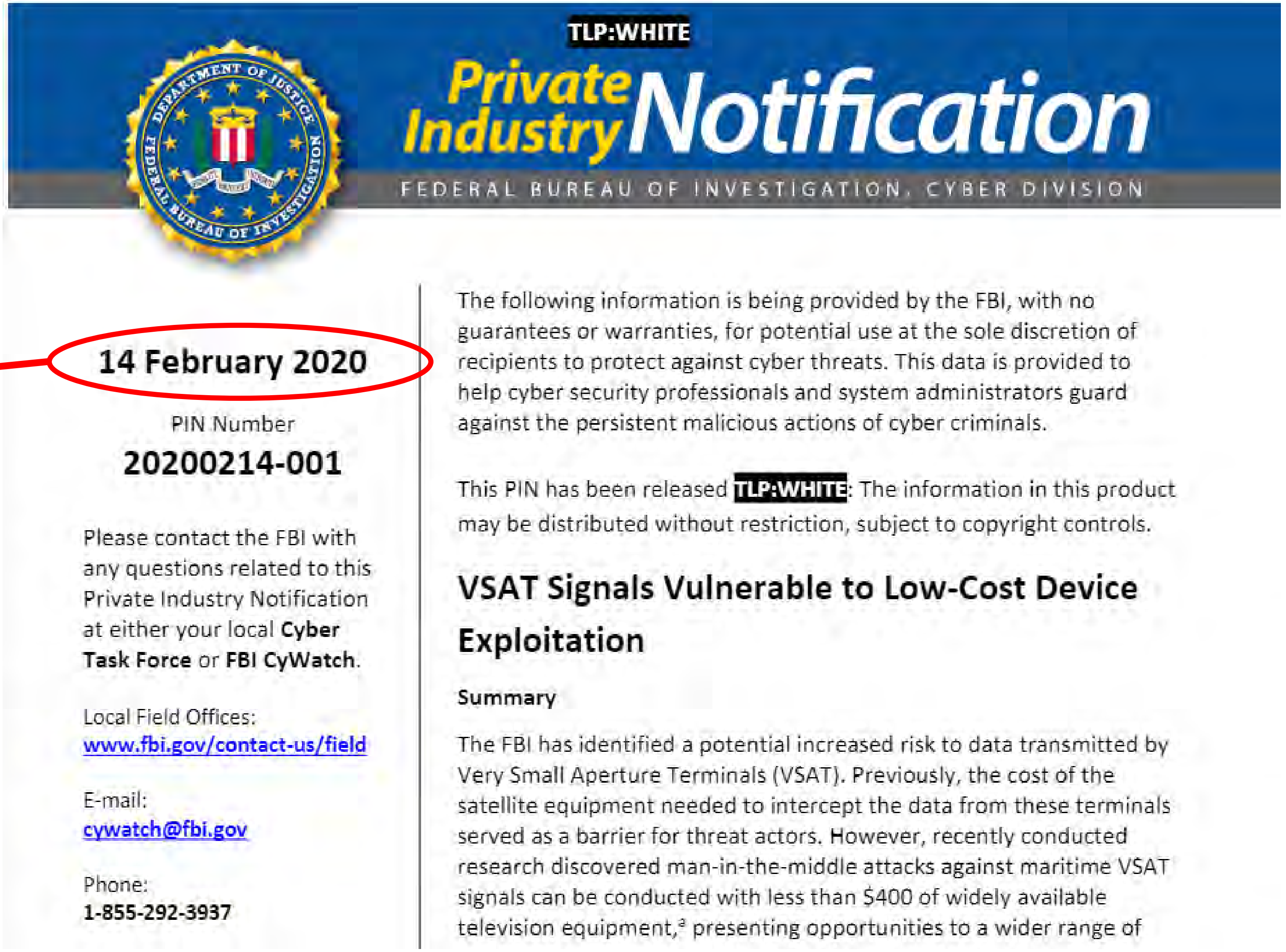


James Pavur
@JamesPavur

Excited to share that our paper on Maritime VSAT security will be presented S&P 2020 @IEEESSP. Check out the paper here: doi.ieeecomputersociety.org/10.1109/SP4000... #spacecybersecurity #sp20

3:28 PM · Mar 9, 2020 · Twitter Web App

?



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 February 2020

PIN Number

20200214-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

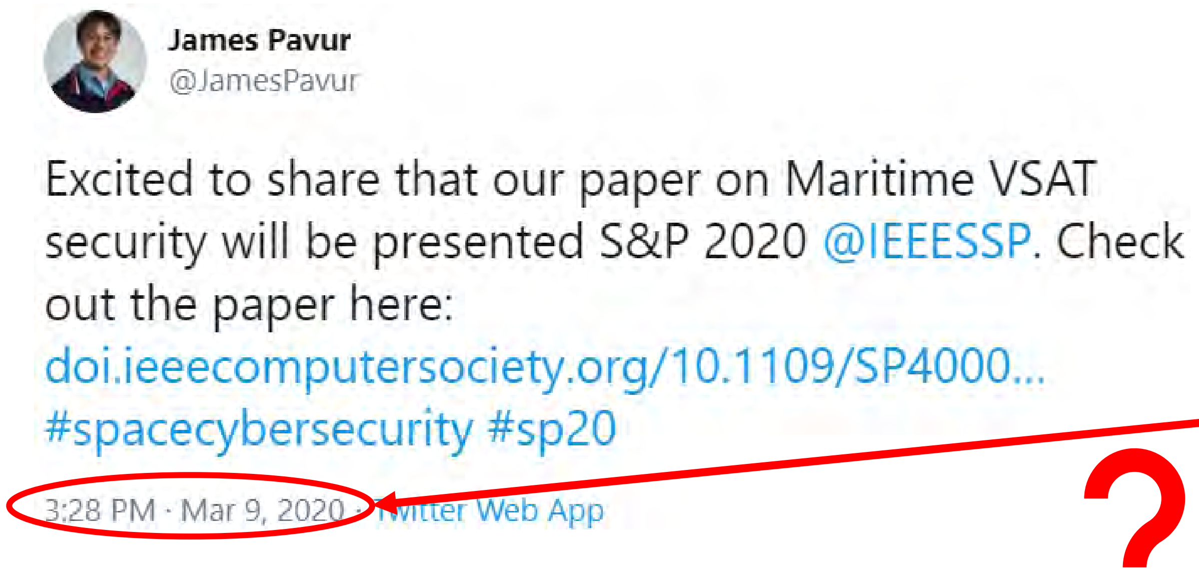
This PIN has been released **TLP:WHITE**: The information in this product may be distributed without restriction, subject to copyright controls.

VSAT Signals Vulnerable to Low-Cost Device Exploitation

Summary

The FBI has identified a potential increased risk to data transmitted by Very Small Aperture Terminals (VSAT). Previously, the cost of the satellite equipment needed to intercept the data from these terminals served as a barrier for threat actors. However, recently conducted research discovered man-in-the-middle attacks against maritime VSAT signals can be conducted with less than $400 of widely available television equipment,[a] presenting opportunities to a wider range of

Thanks FBI!



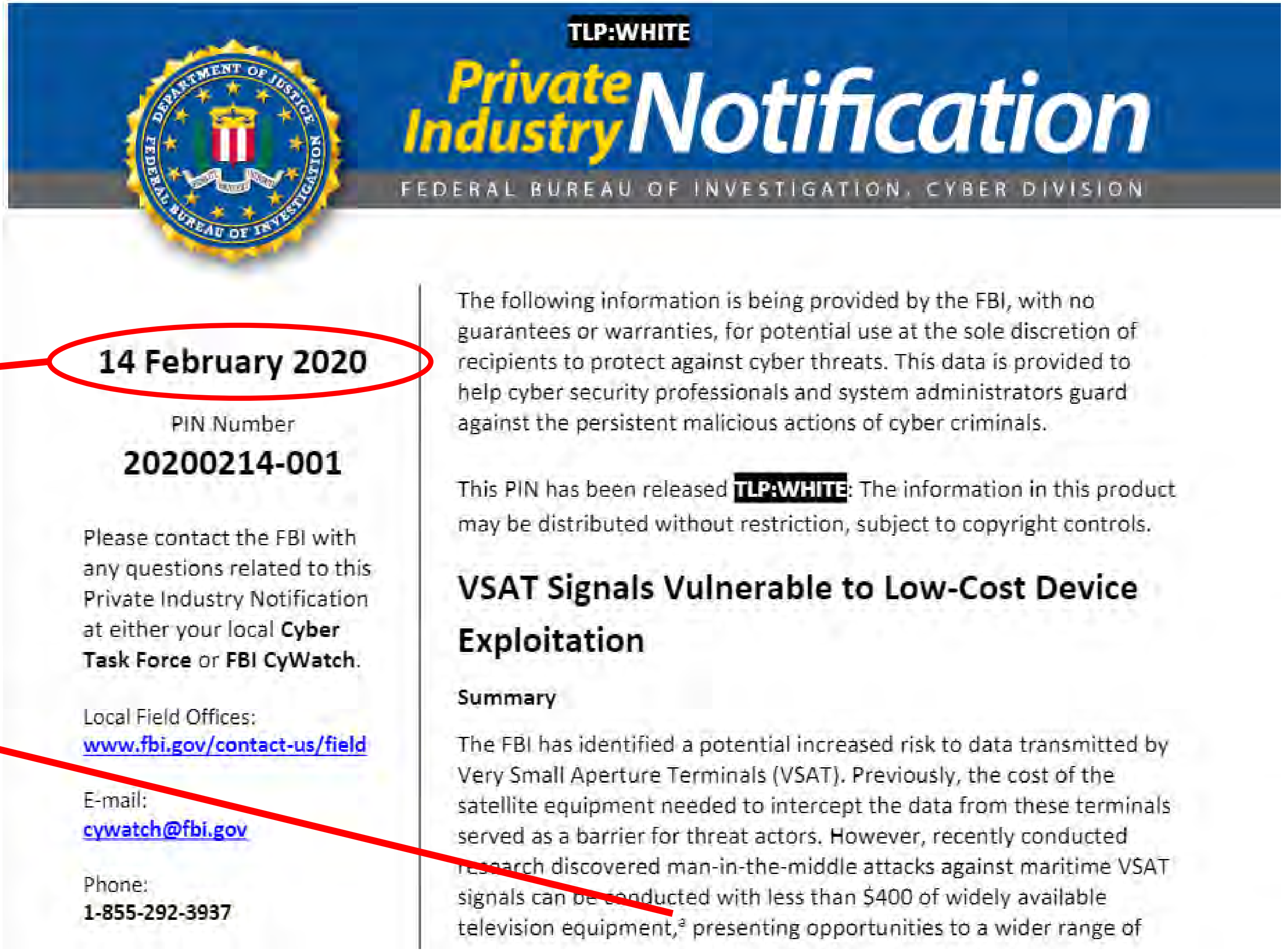
James Pavur
@JamesPavur

Excited to share that our paper on Maritime VSAT security will be presented S&P 2020 @IEEESSP. Check out the paper here: doi.ieeecomputersociety.org/10.1109/SP4000... #spacecybersecurity #sp20

3:28 PM · Mar 9, 2020 · Twitter Web App

?

[a] The materials used in the researchers experiment included a TBS-6903 DVB-S2X PCI card, Selfsat H30D satellite dish, and 3 meter coaxial cable.



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 February 2020

PIN Number
20200214-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:WHITE**: The information in this product may be distributed without restriction, subject to copyright controls.

VSAT Signals Vulnerable to Low-Cost Device Exploitation

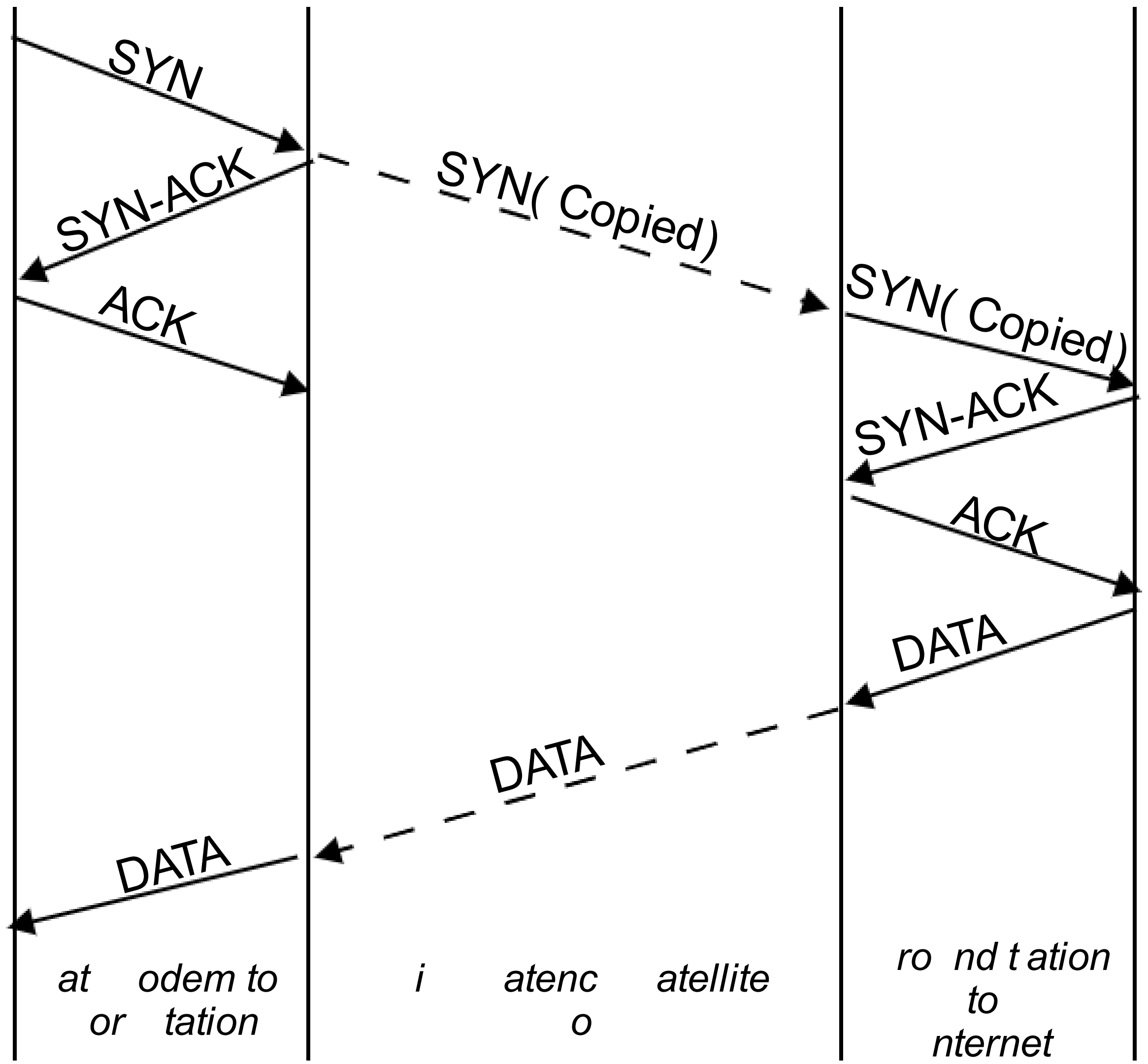
Summary

The FBI has identified a potential increased risk to data transmitted by Very Small Aperture Terminals (VSAT). Previously, the cost of the satellite equipment needed to intercept the data from these terminals served as a barrier for threat actors. However, recently conducted research discovered man-in-the-middle attacks against maritime VSAT signals can be conducted with less than $400 of widely available television equipment,[a] presenting opportunities to a wider range of

Mitigations and Defenses

Why Does This Happen?

- Not 100% Incompetence / Ignorance
- Latency -> Miserable TCP Experience
- S s fix wit “ e rforman e n an ing rox ies” s
    - Basically a benevolent Man-In-The-Middle attack
- an ’t se tra itional en -to-end VPN and PEP



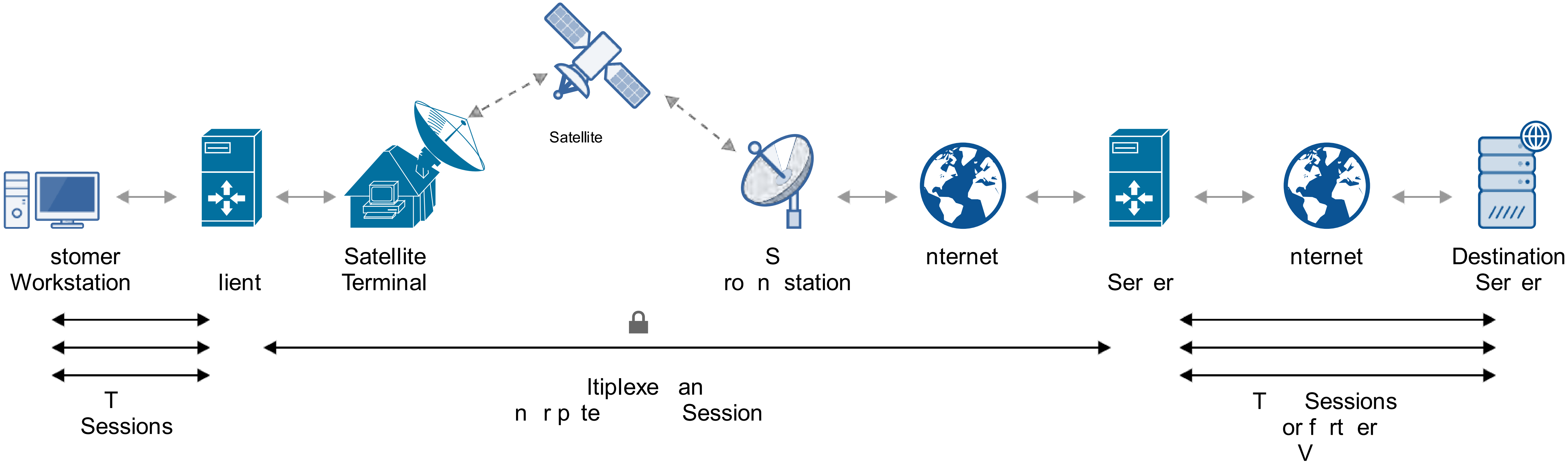
Short-Term Fixes

Accept VPN performance hit

Use TLS / DNSSEC / etc.

ISP: Alter sequence numbers in PEP

Longer-Term – “QPEP”



Satellite

stomer
Workstation

lient

Satellite
Terminal

S
ro n station

nternet

Ser er

nternet

Destination
Ser er

T
Sessions

ltiplexe an
n r p te Session

T Sessions
or f rt er
V

QPEP Design Principles

OPEN SOURCE

ACCESSIBLE & SIMPLE

TARGET INDIVIDUALS (NOT ISPS)

Contribute Here: https://github.com/ssloxford/qpep

Traditional VPN Encryption (OpenVPN)

ox.ac.uk

~25 seconds

Encrypted PEP (QPEP)

ox.ac.uk

~14 seconds

Key Takeaways

- Satellite Broadband Traffic is Vulnerable to Long-Range Eavesdropping Attacks
- Satellite Customers Across Domains Leak Sensitive Data Over Satellite Links
- Performance and Privacy Don’t Need to Trade Off in SATCOMs Design

T e “Next o ” i n now n. Encr t ever t in .

Questions/Ideas: james.pavur@cs.ox.ac.uk

Special thanks to a.i. solutions for offering academic access to FreeFlyer, used in our animations!