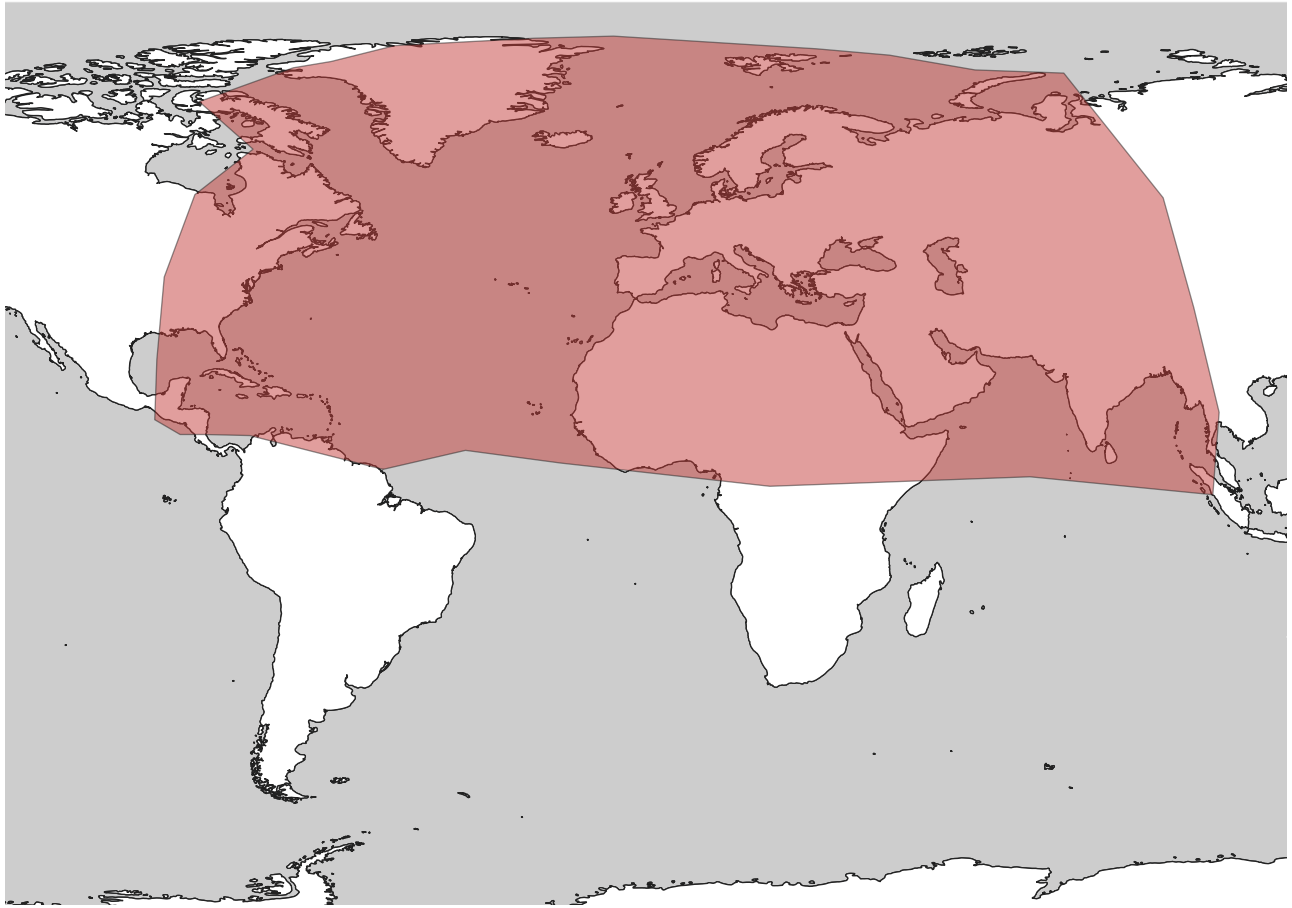
A Space Parable: Takeaways from Exploiting Satellite Broadband

JAMES PAVUR, OXFORD UNIVERSITY

The Experiments



What We Found

9 FORTUNE GLOBAL 500 MEMBERS

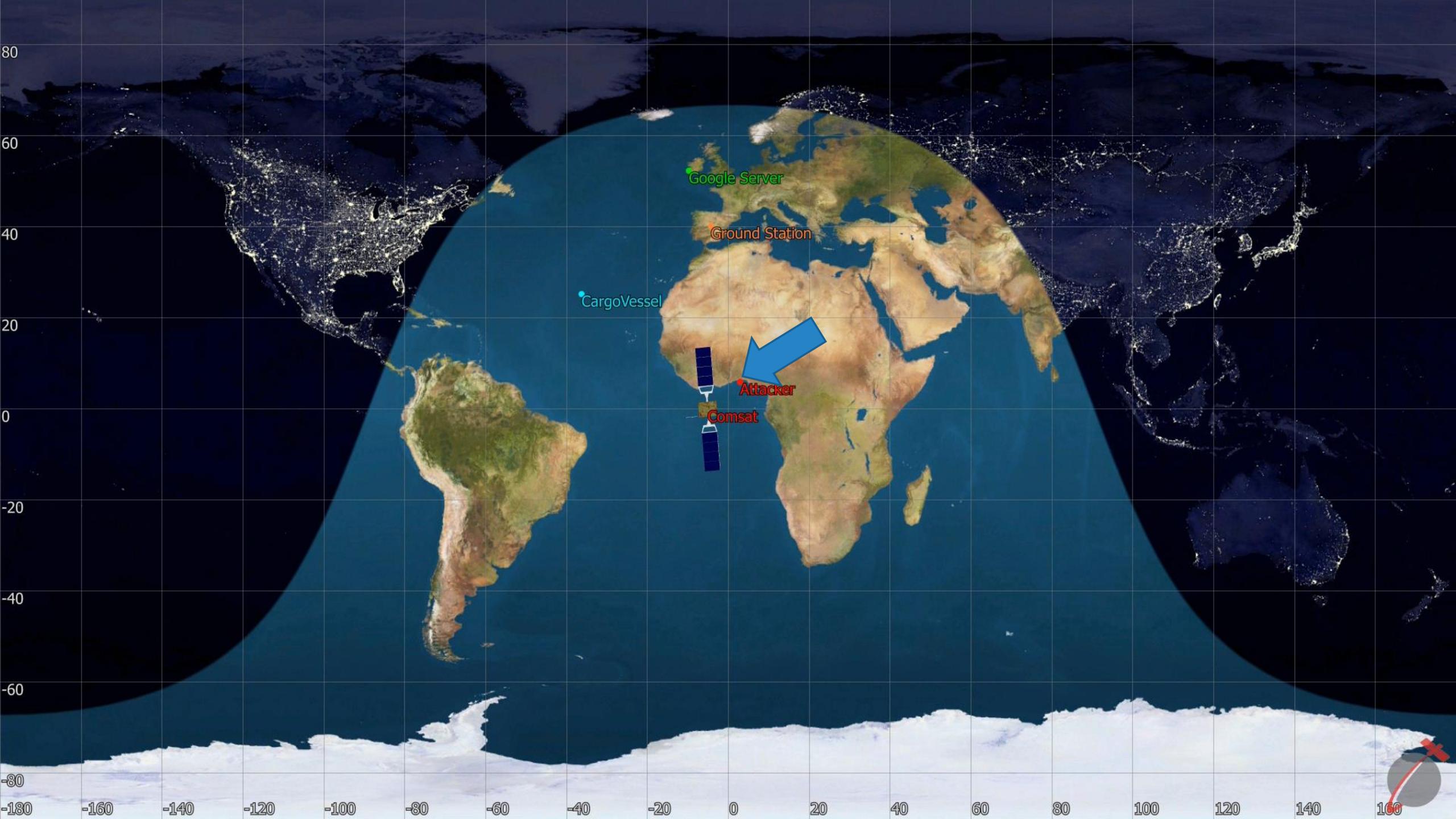
6 OF 10 LARGEST AIRLINES

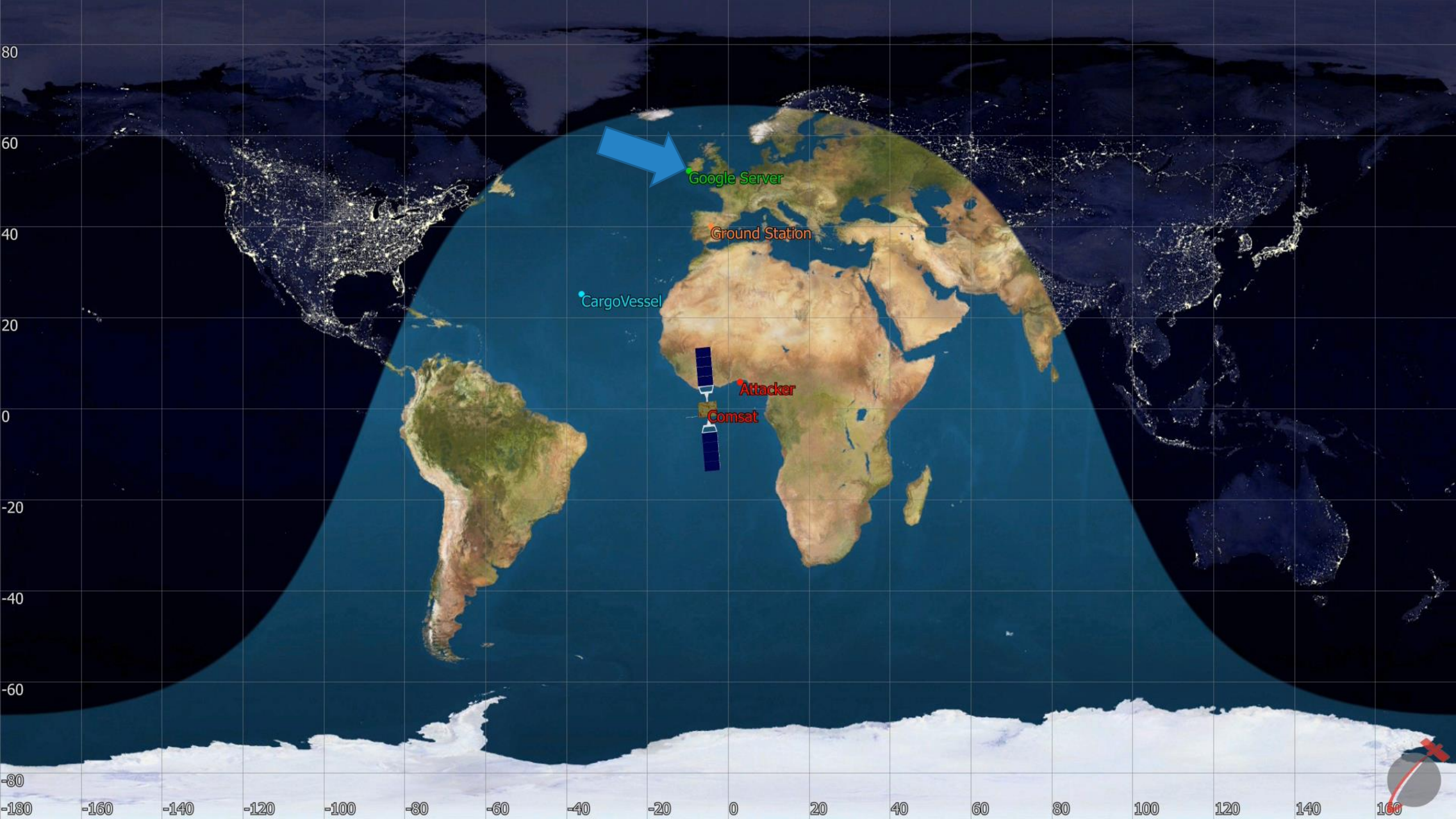
~40% MARITIME CARGO MARKET

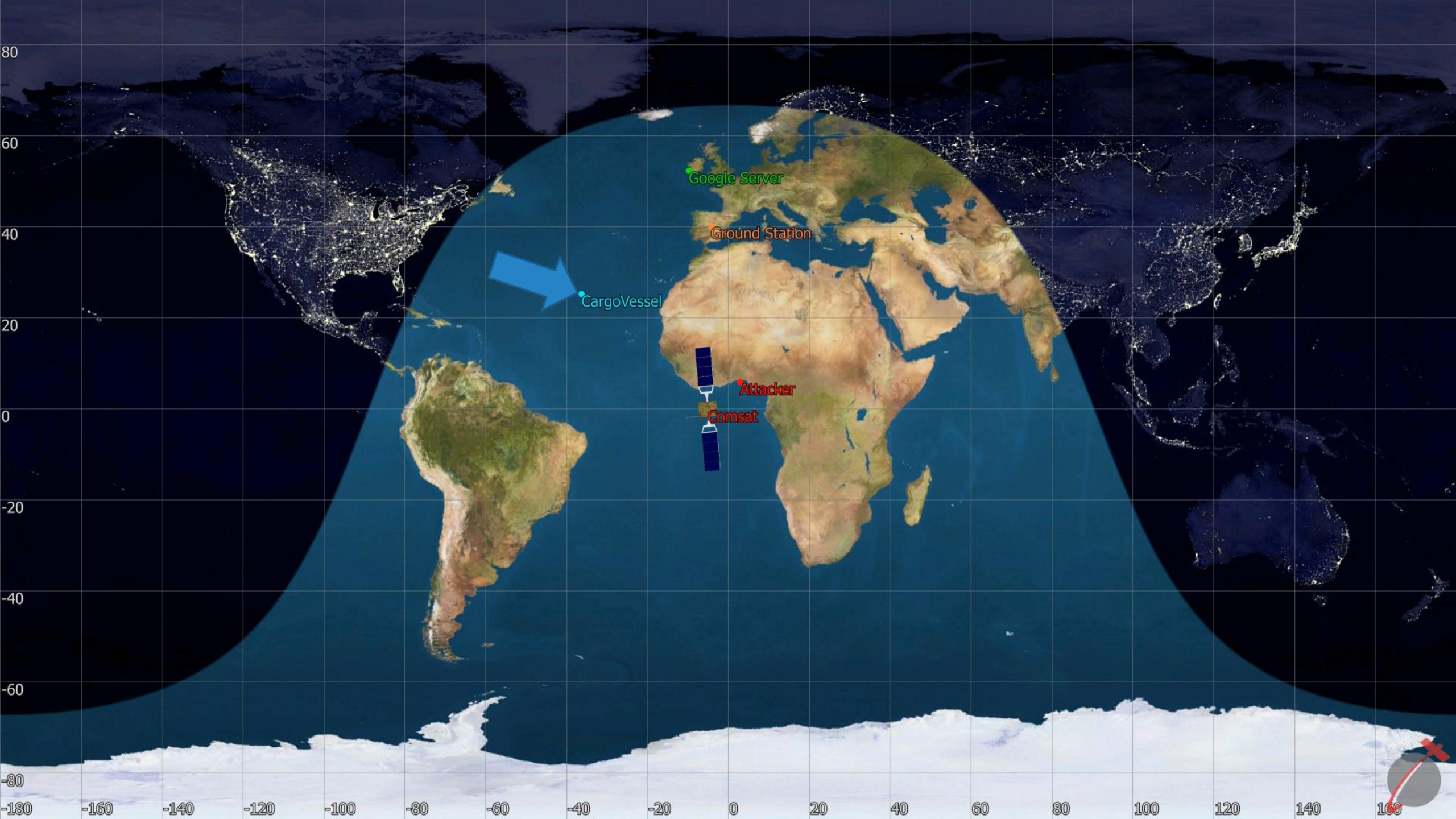
GOVERNMENTAL AGENCIES

YOU?

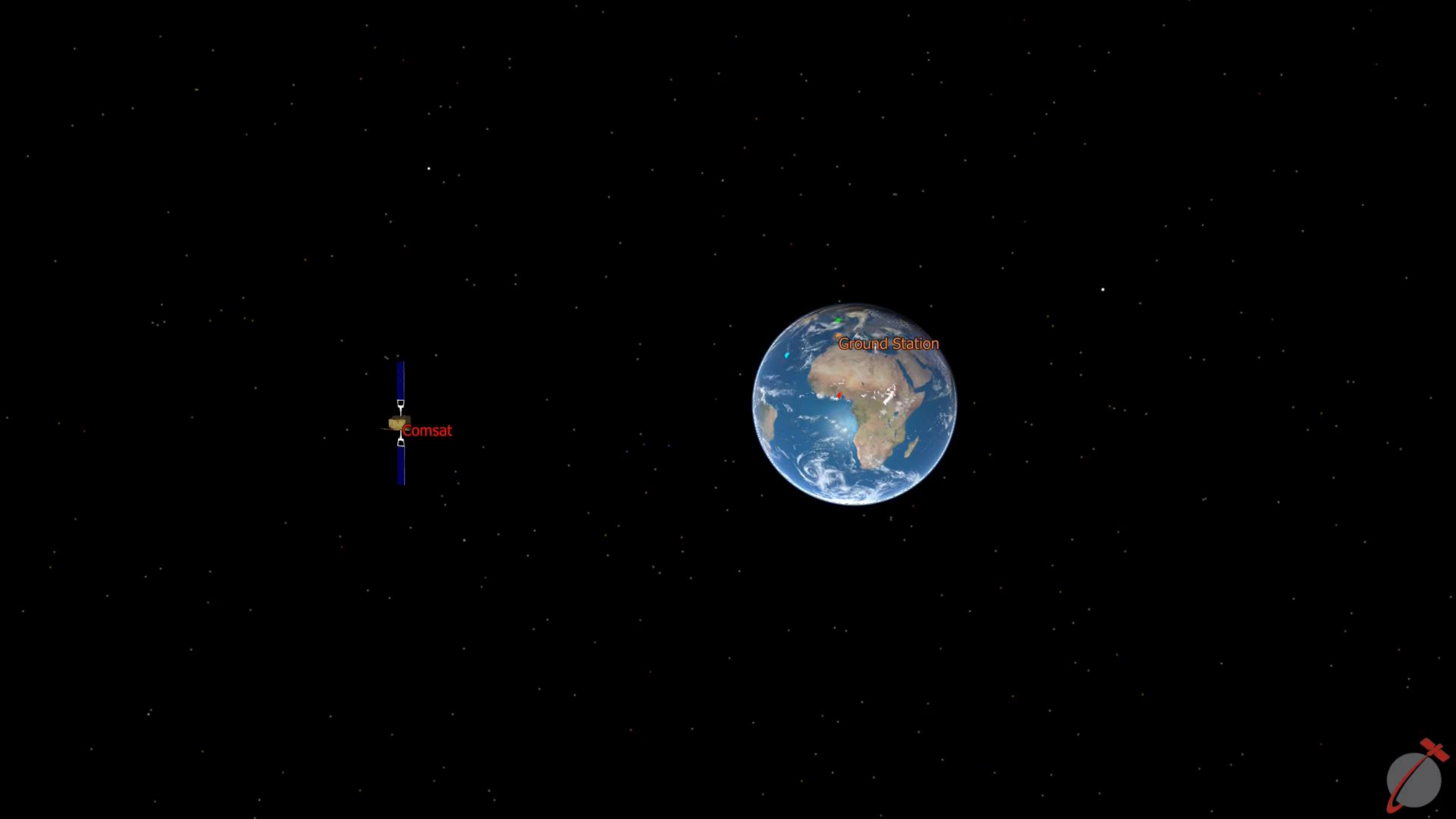
SATCOM Crash Course


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


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


Ground Station
Comsat

Theory to Practice

Nation-State Tech

MDM9000 Satellite Modem

For Intelligence Gathering, WGS and Milsatcom Networks

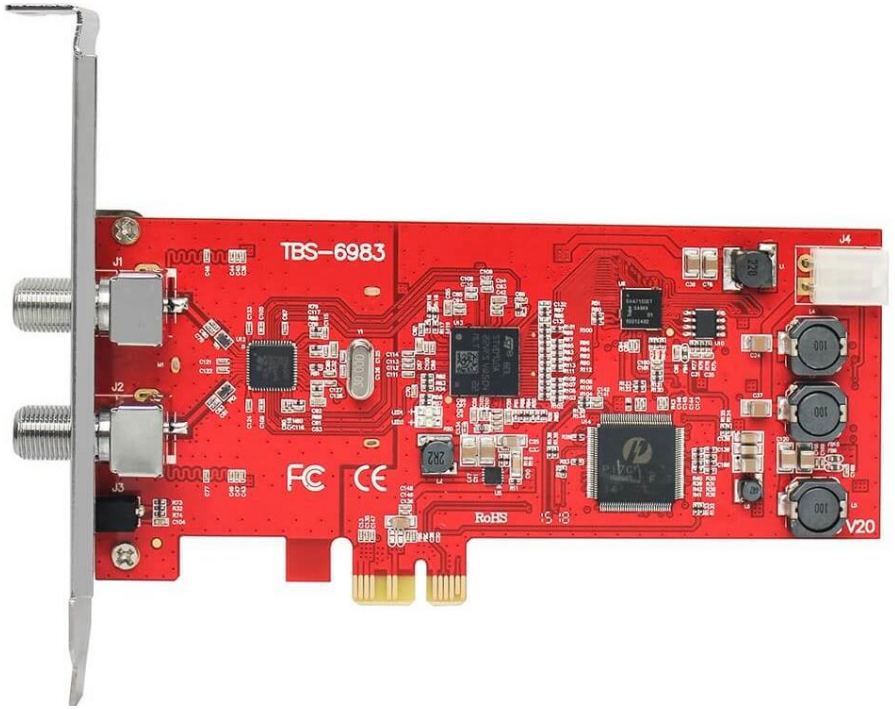
Description

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.

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

$300 of TV Equipment

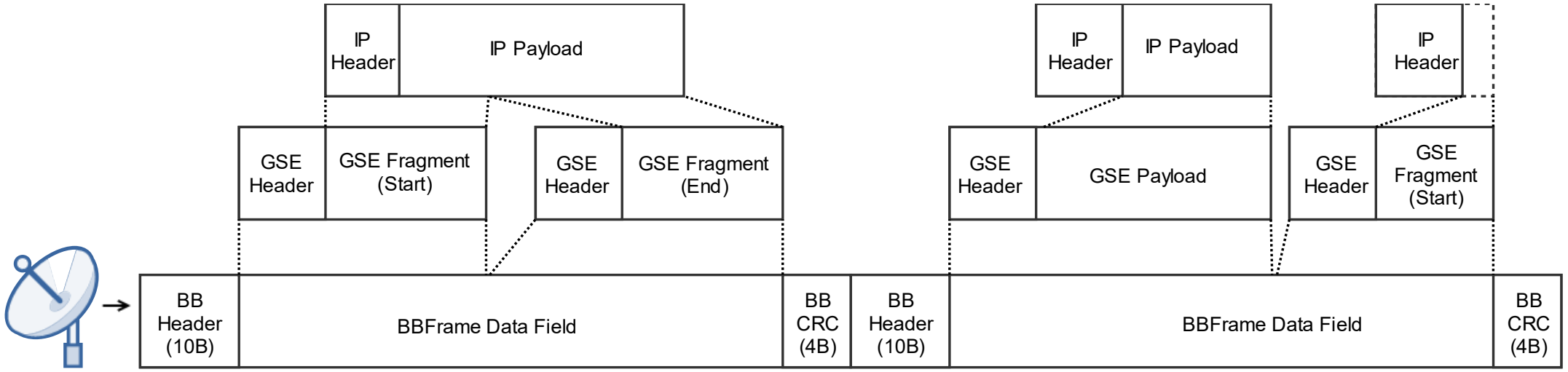


Selfsat H30D ~$90 (or any satellite dish + LNB)

TBS-6983/6903 ~$200-300 (or comparable PCIE tuner)

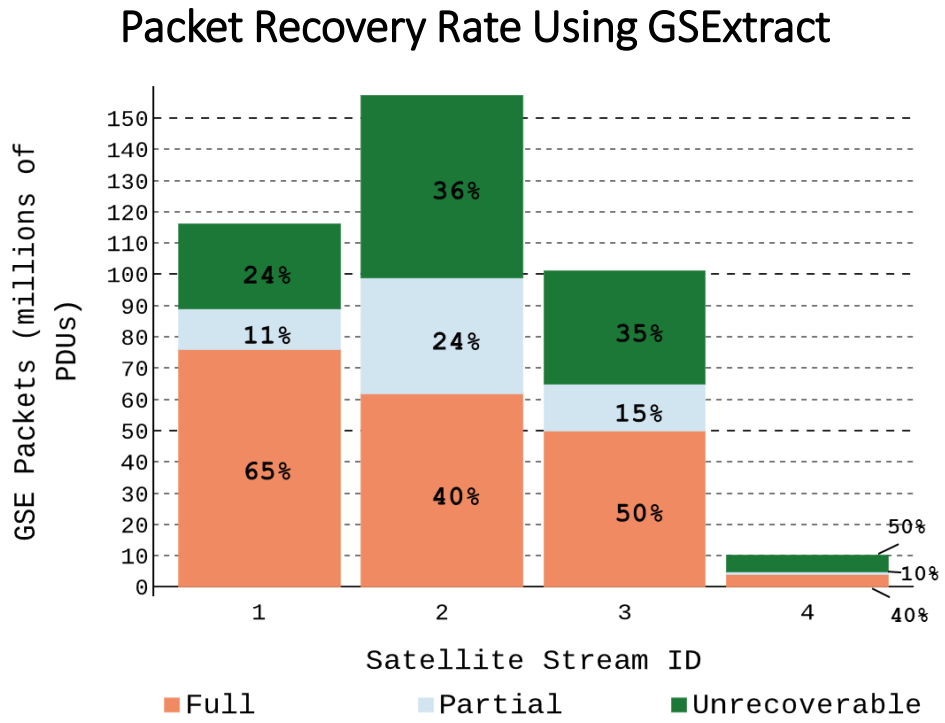
GSE (Generic Stream Encapsulation)

- More modern, popular among enterprise “VSAT” customers
- In practice, networks assume equipment in the $25k-$100k range
  - Doesn’t work well on our hardware (32 APSK)…



Corruption Disruption

- Built “GSExtract” - a forensic tool to reconstruct lossy feeds
  - Applies simple rules to find likely packet headers / re-assemble broken fragments
  - More detail here: https://doi.ieeecomputersociety.org/10.1109/SP40000.2020.00056
- Try it out
  - https://github.com/ssloxford/gsextract



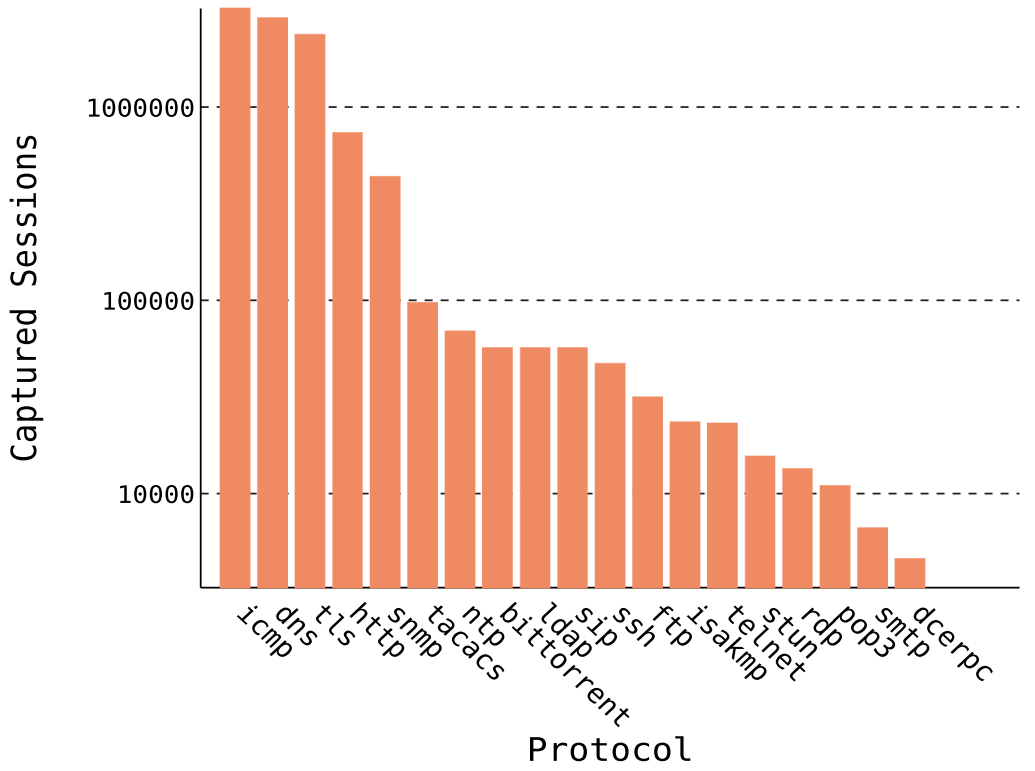
Findings

The Basics

NO DEFAULT ENCRYPTION

ISP-ESQUE VANTAGE POINT

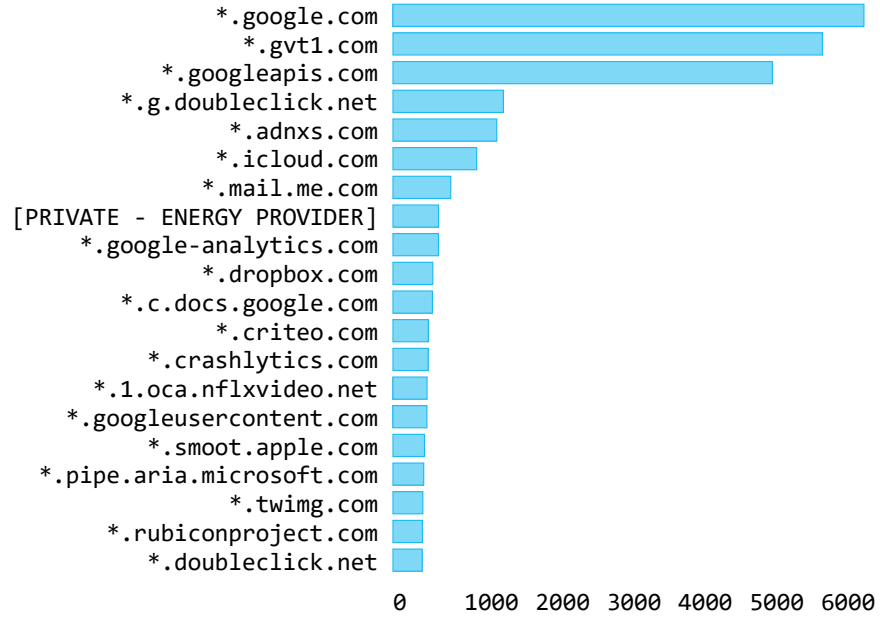
BREACH THE PERIMETER



TLS?

```
> 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)



Communications

```
...=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"> </span></p><p
class=3D"cs95E872D0"><span
c=..lass=3D"cs19C3E152"> </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 
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
```

Maritime

Case Study: 100 Random IPs

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.

Case Study: 100 Random IPs

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	1[illegible]ssels	Specialized Maritime Software	Unencrypted Fileshare Credentials
11	Container	110,000t	Shipping	[illegible]ssels	Maritime Navigation Software	Unencrypted Email Conversations
12	Subsea	22,000t	Oil & Gas	[illegible] 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.

Case Study: 100 Random IPs

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	Firefigh	8,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted SQL Database Replication
5	Se	8,000t	Seismic	10 Vessels	Antivirus Software & Version	Unencrypted Email Conversations
6	C ical	5,000t	Shipping	1 Vessels	PLC Firmware Binaries	Unencrypted PLC Firmware Update
7	utpost	(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.

Case Study: 100 Random IPs

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

```
> 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.
```

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

CID Number [redacted] Rank: COFF Name: S[redacted]N
Passport: Z[redacted] Issued: 05[redacted] Expiry: 04[redacted]
Seaman book: [redacted] Issued: 04[redacted] Expiry: 03[redacted]
Nationality: [redacted] Date of birth: [redacted] Place of birth: [redacted]

CID Number [redacted] Rank: 2OFF Name: [redacted]UL
Passport: R[redacted] Issued: 14[redacted] Expiry: 13[redacted]
Seaman book: [redacted] Issued: 24[redacted] Expiry: 23[redacted]br>
Nationality: [redacted] Date of birth: [redacted] Place of birth: [redacted]

Aviation

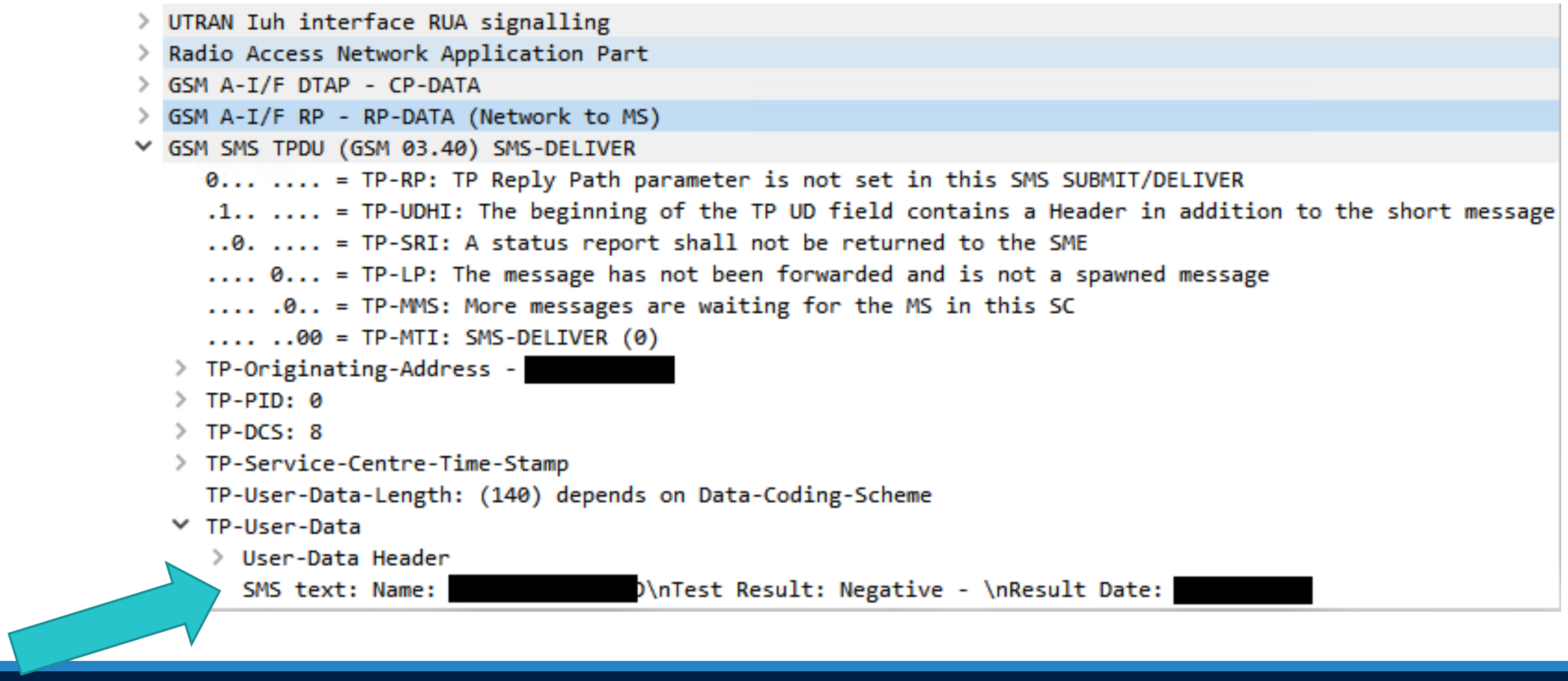
Electronic Flight Bags

```
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]
```

Femtocells


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)
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 -
TP-PID: 0
TP-DCS: 8
TP-Service-Centre-Time-Stamp
TP-User-Data-Length: (140) depends on Data-Coding-Scheme
TP-User-Data
User-Data Header
SMS text: Name:
)\nTest Result: Negative - \nResult Date:

Active Attacks?

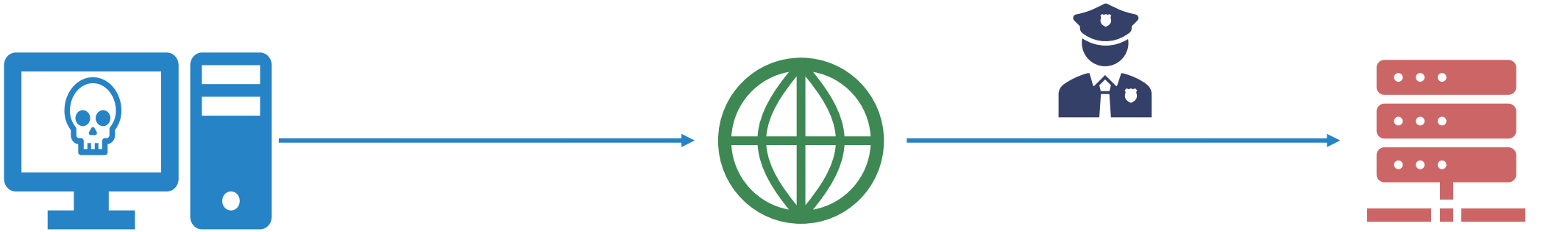
“Untraceable” Exfiltration: Requirements

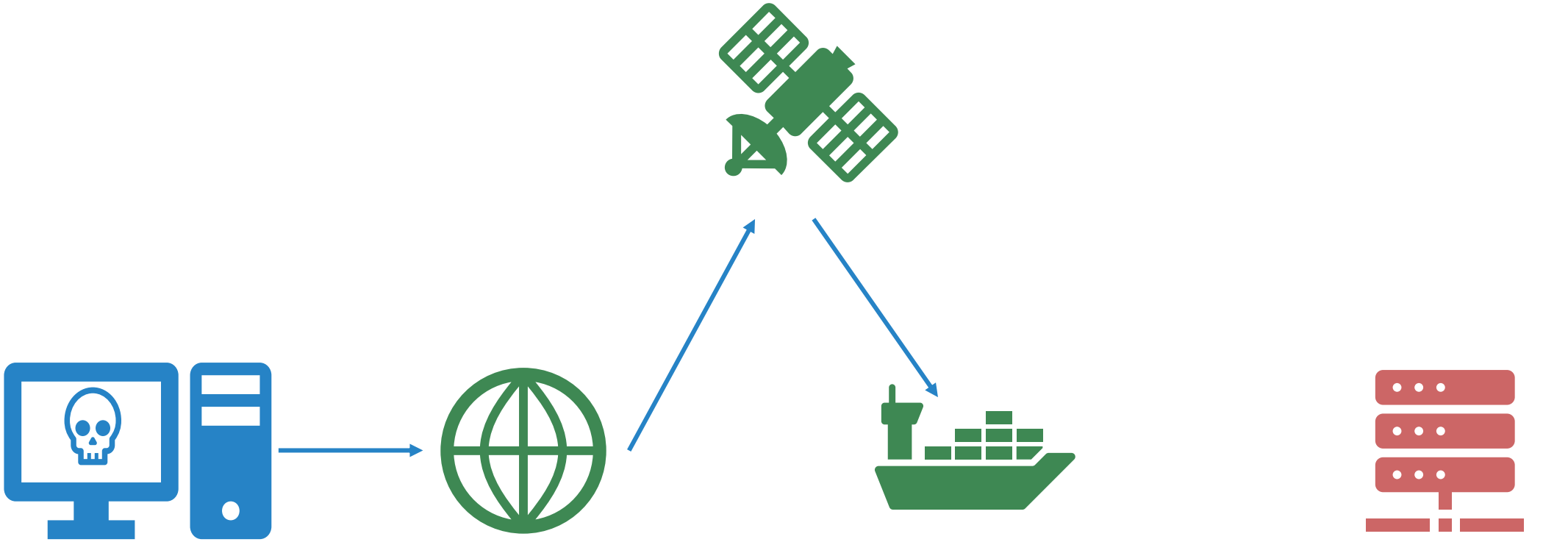
ROUTE FROM COMPROMISED HOST TO SATELLITE IP

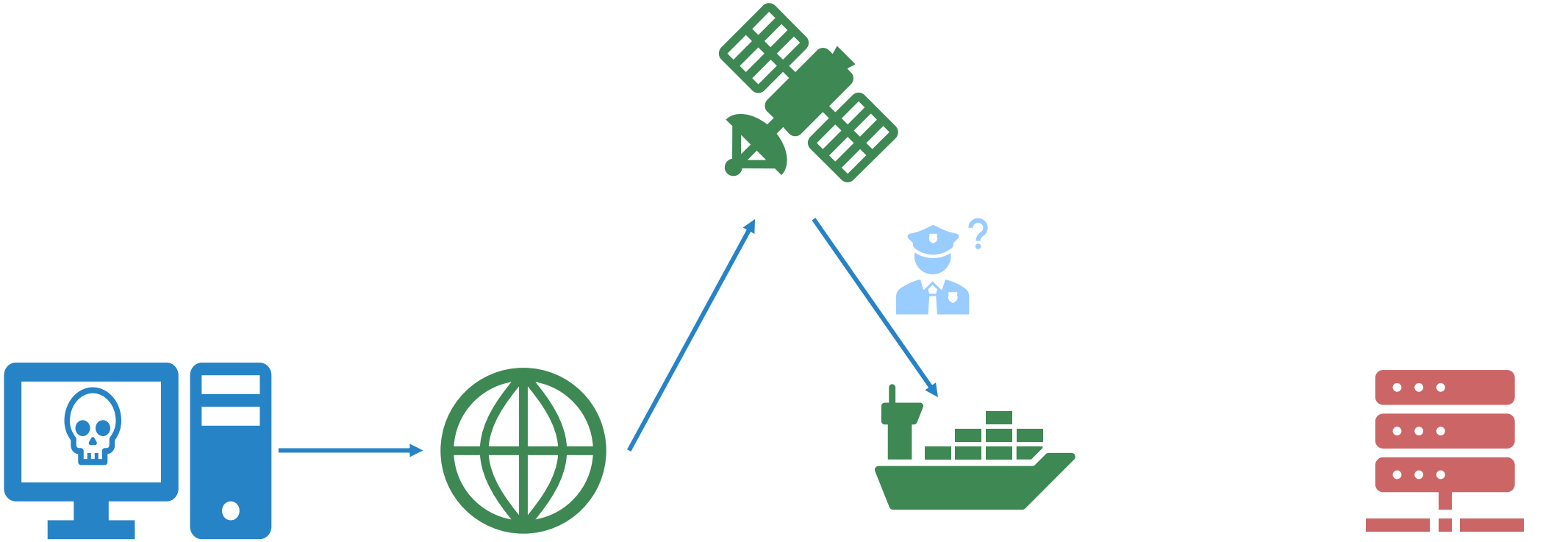
DISH INSIDE FORWARD LINK FOOTPRINT

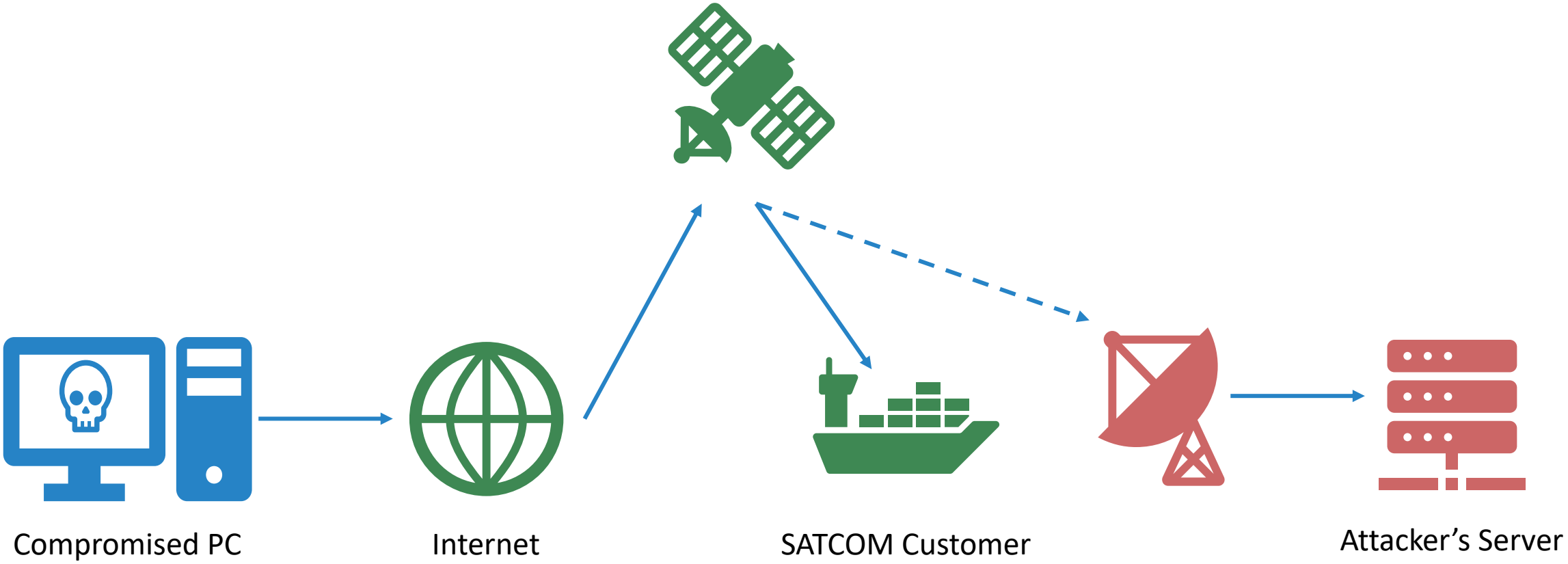

?
Compromised PC
Attacker’s Server


Compromised PC
Internet
Attacker’s Server


Compromised PC
Internet
Attacker’s Server


Compromised PC
Internet
SATCOM Customer
Attacker’s Server


Compromised PC
Internet
SATCOM Customer
Attacker’s Server


Compromised PC
Internet
SATCOM Customer
Attacker’s Server

Ethics & 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

?

[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

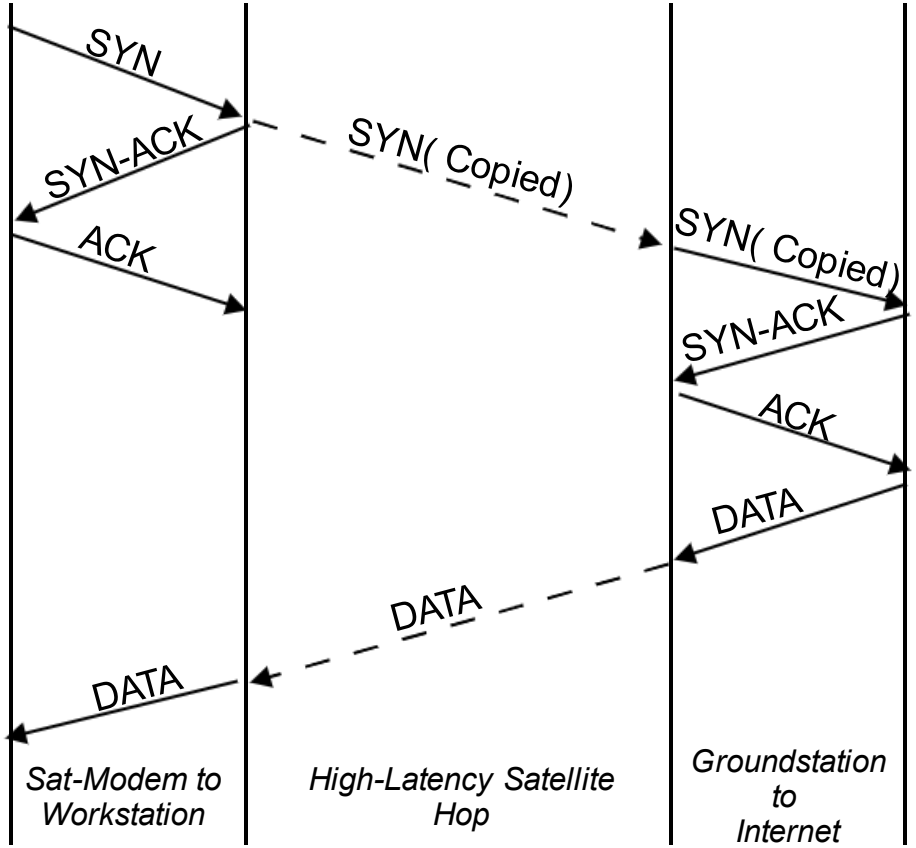
Summary

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

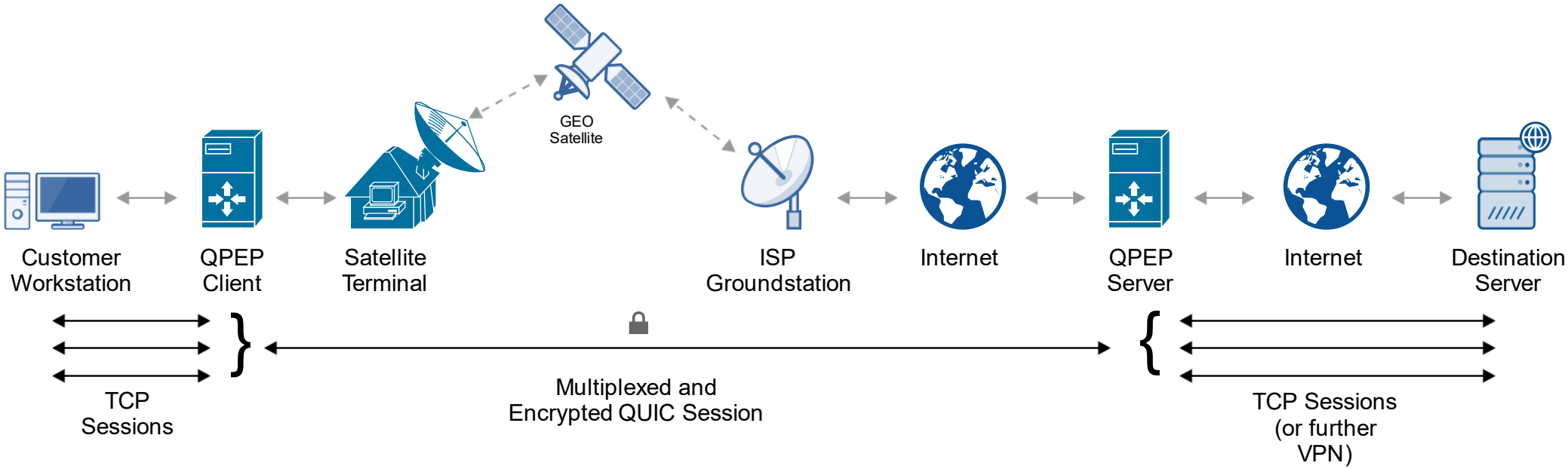
Why????

Performance First!

- 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

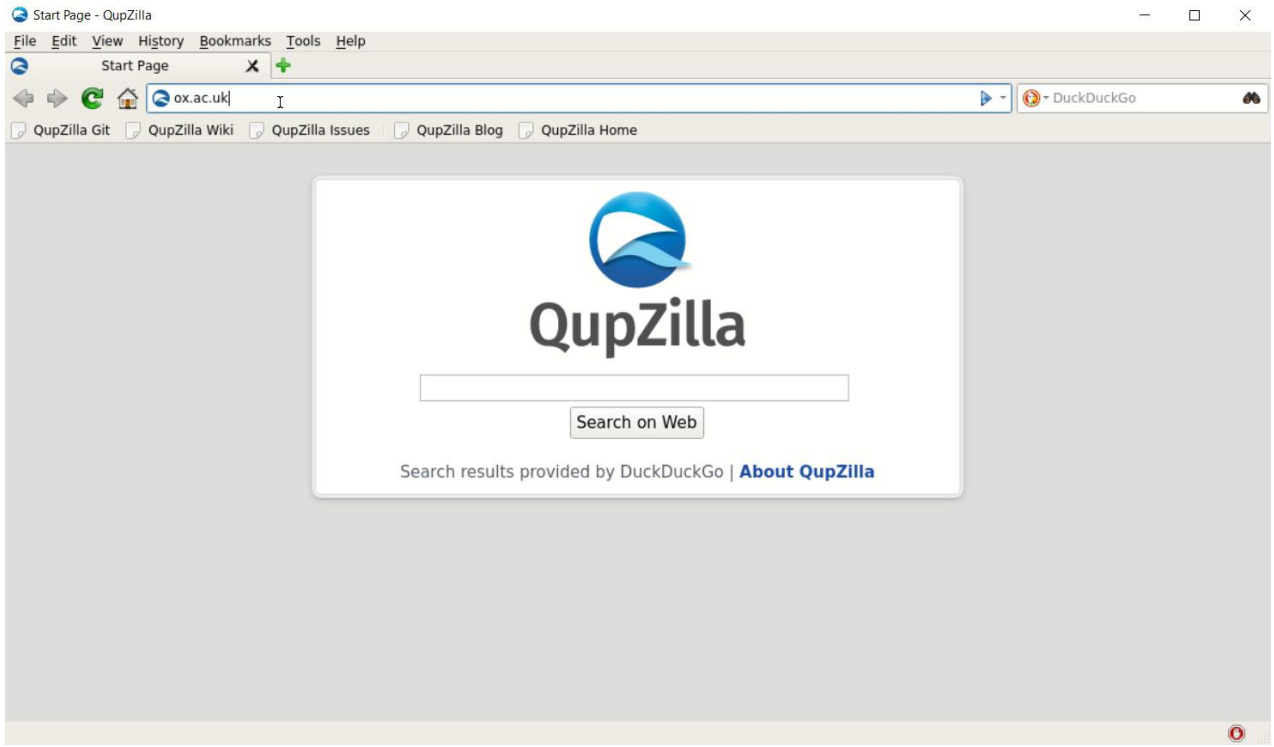


QPEP: VPN + PEP



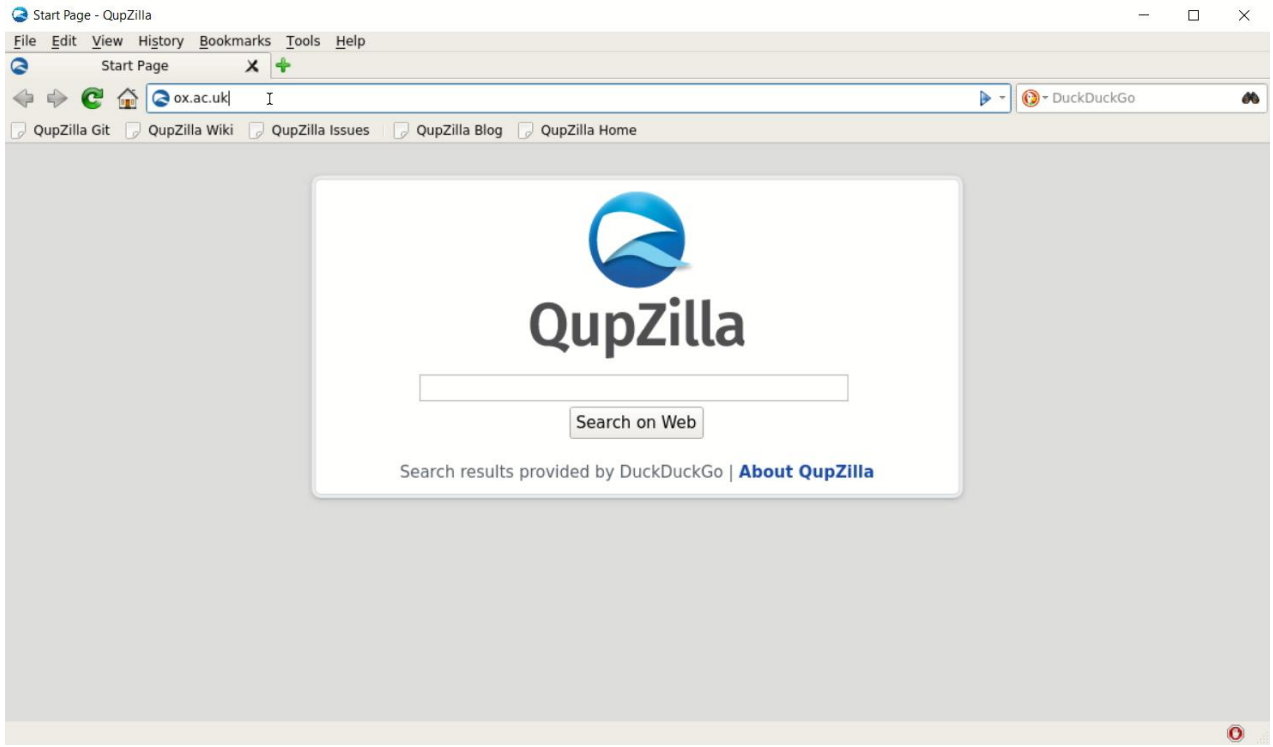
Contribute / Try It Out: https://github.com/ssloxford/qpep

Traditional VPN Encryption (OpenVPN)



~25 seconds

Encrypted PEP (QPEP)



~14 seconds

Lessons Learned

Threat Models Change

Security is Shared

Security Doesn’t Always Win

Questions? – james.pavur@cs.ox.ac.uk

- Longer presentation on this research: “Whispers Among the Stars” at DEFCON 28: https://www.youtube.com/watch?v=ku0Q_Wey4K0
- Academic Publications:
  - Pavur, James, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. “A Tale of Sea and Sky: On the Security of Maritime VSAT Communications.” In *2020 IEEE Symposium on Security and Privacy (S&P)*. Oakland, CA: IEEE, 2020.
  - Pavur, James, Daniel Moser, Vincent Lenders, and Ivan Martinovic. “Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband.” ACM, 2019.
  - Pavur, James, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. “QPEP: A QUIC-Based Approach to Encrypted Performance Enhancing Proxies for High-Latency Satellite Broadband.” (Under Peer-Review, Pre-print at *ArXiv:2002.05091 [Cs]*, February 12, 2020. http://arxiv.org/abs/2002.05091).