Hacking a Bird in the Sky

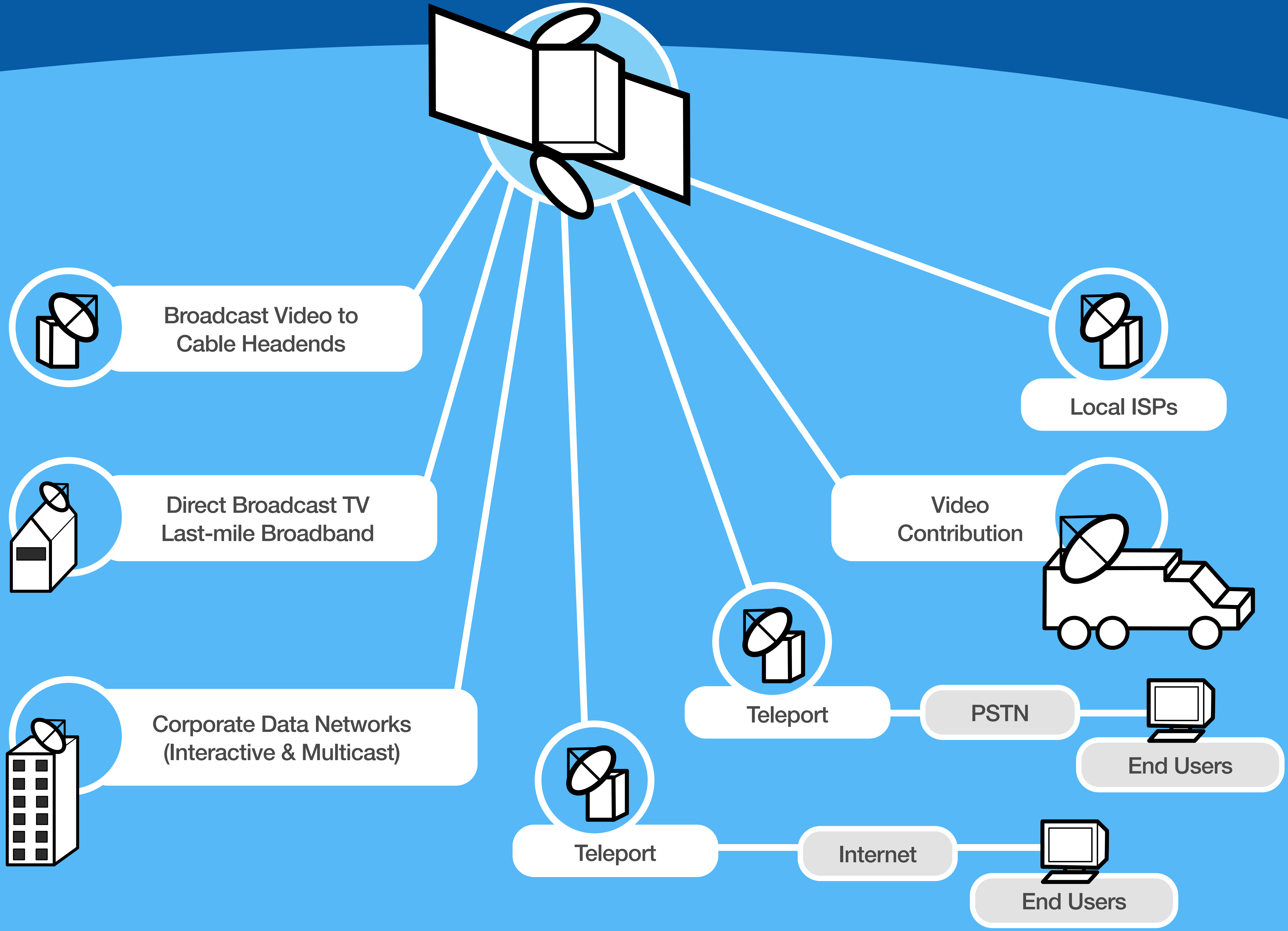
The Revenge of Angry Birds

Jim Geovedi, Raditya Iryandi, Raoul Chiesa

Satellite Communication

When terrestrial communication **FAIL**, we **PREVAIL**!

Arthur C. Clarke
1917-2008



Broadcast Video to Cable Headends

Direct Broadcast TV
Last-mile Broadband

Corporate Data Networks
(Interactive & Multicast)

Local ISPs

Video
Contribution

Teleport

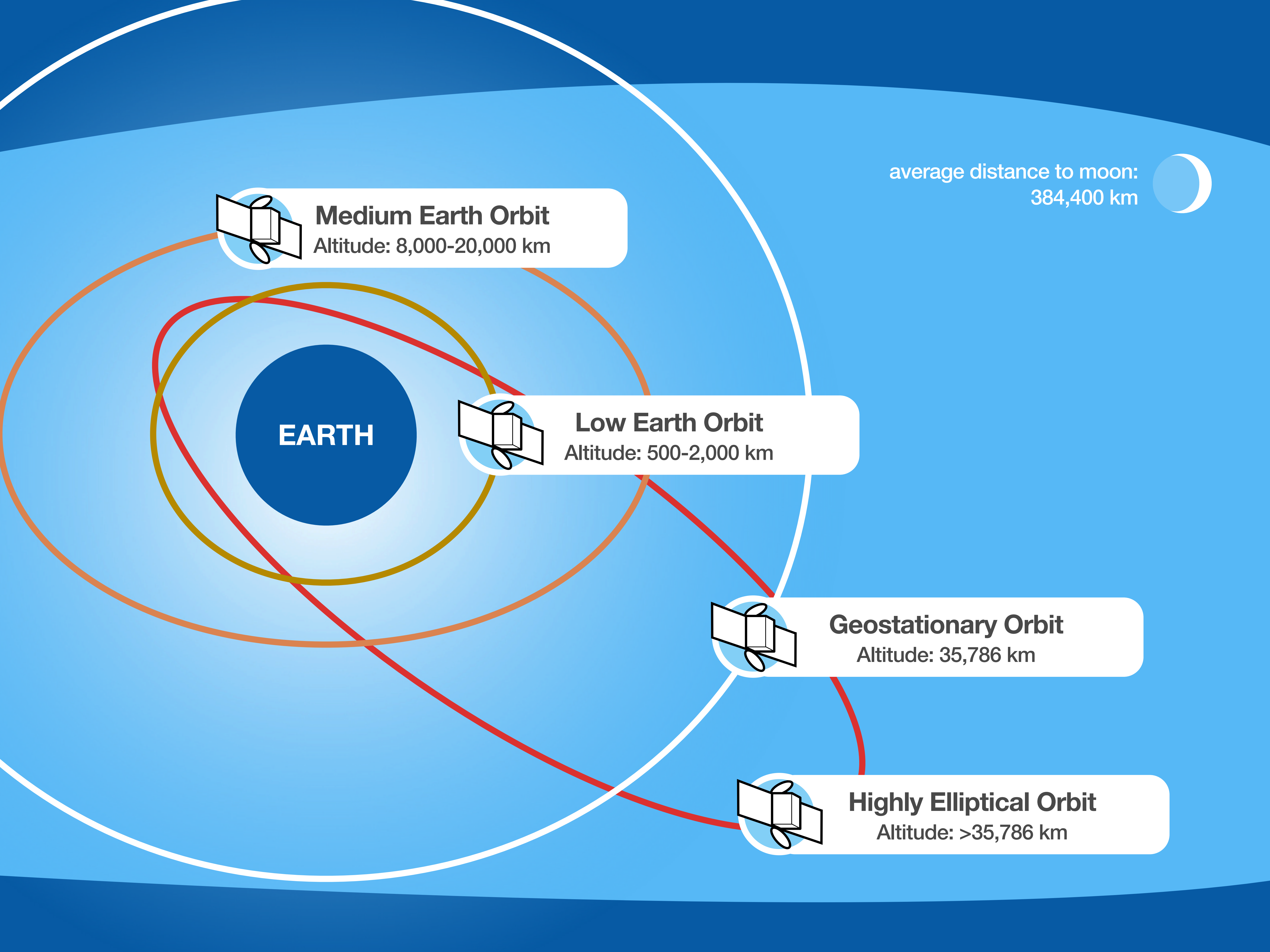
PSTN

End Users

Teleport

Internet

End Users



EARTH

Medium Earth Orbit

Altitude: 8,000-20,000 km

Low Earth Orbit

Altitude: 500-2,000 km

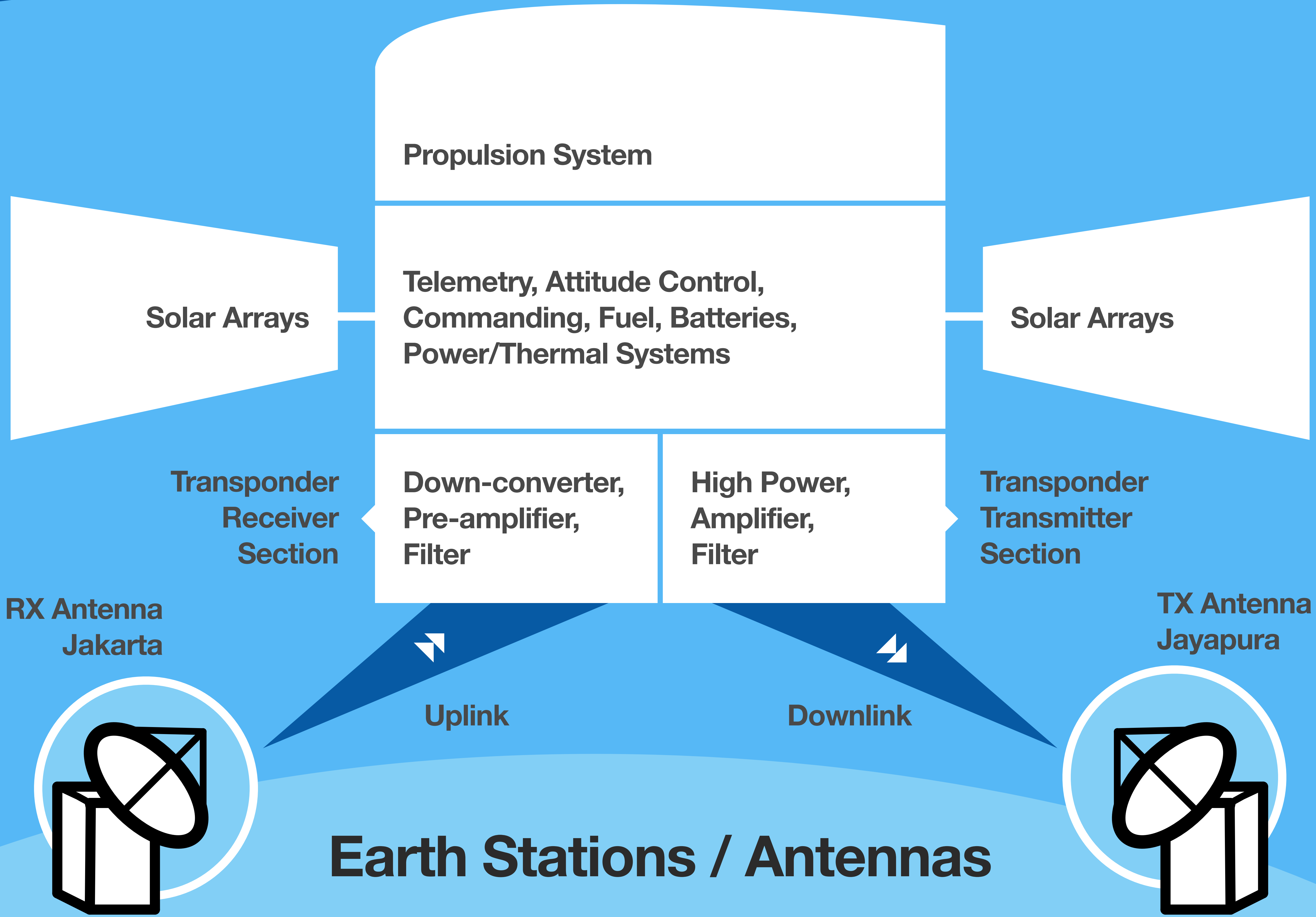
Geostationary Orbit

Altitude: 35,786 km

Highly Elliptical Orbit

Altitude: >35,786 km

average distance to moon:
384,400 km



Propulsion System

Telemetry, Attitude Control, Commanding, Fuel, Batteries, Power/Thermal Systems

Solar Arrays

Solar Arrays

Transponder Receiver Section

Down-converter, Pre-amplifier, Filter

High Power, Amplifier, Filter

Transponder Transmitter Section

RX Antenna Jakarta

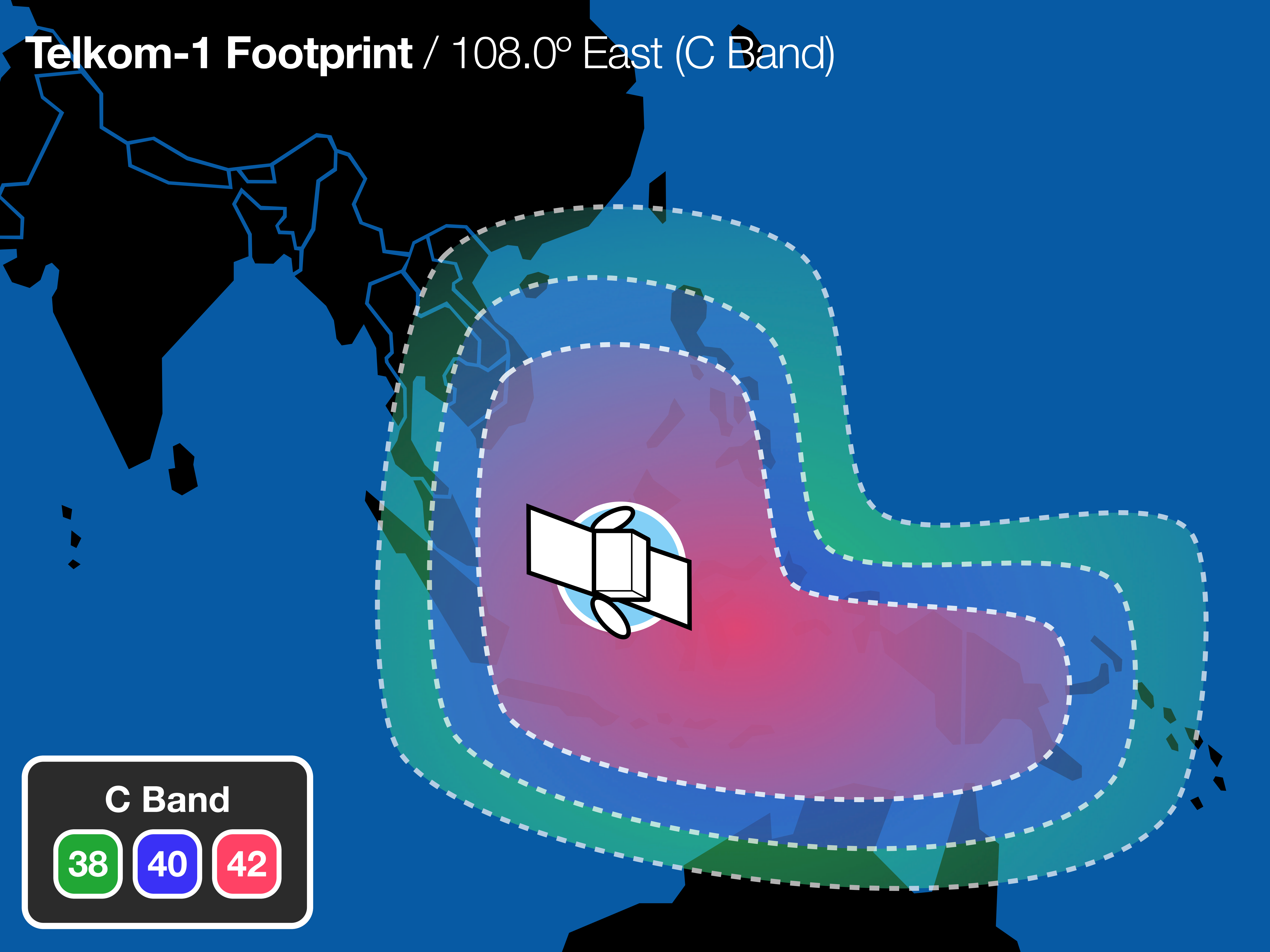
TX Antenna Jayapura

Uplink

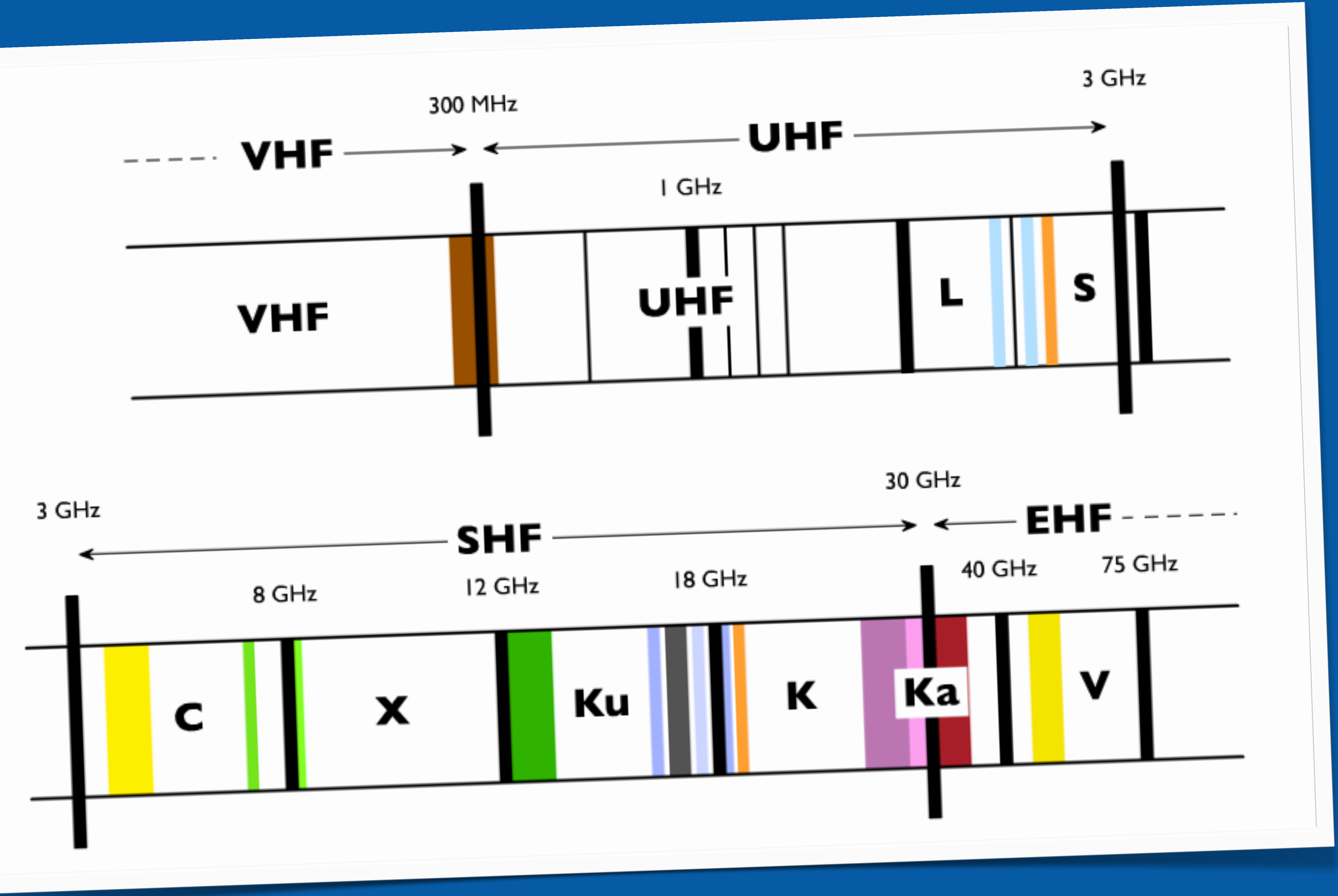
Downlink

Earth Stations / Antennas

Telkom-1 Footprint / 108.0º East (C Band)

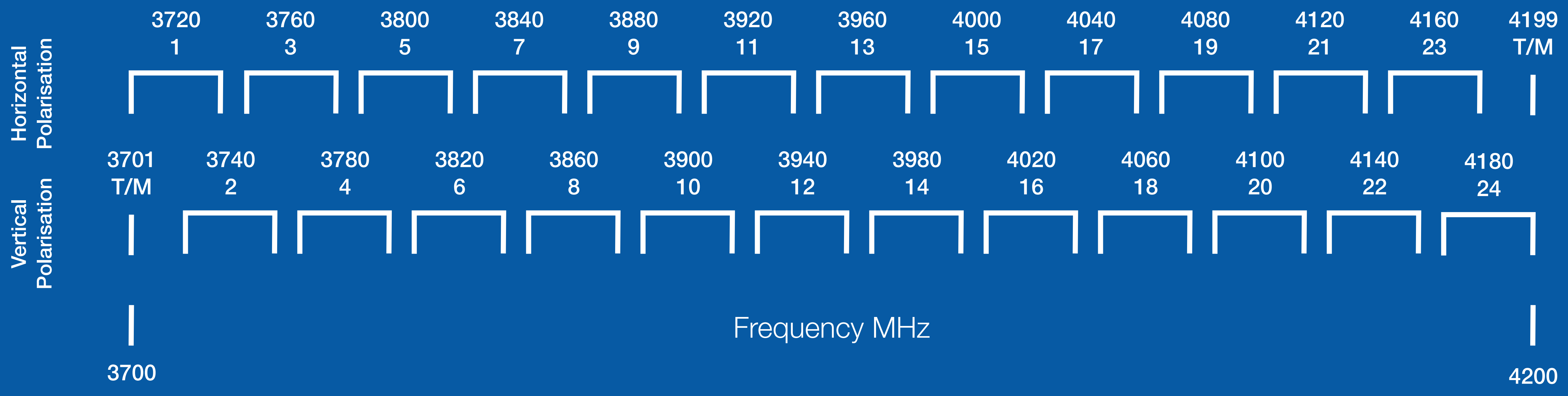


Frequency Band Designations



Example of Frequency and Polarisation Distribution

Transmit



Horizontal Polarisation

3720 1 · 3760 3 · 3800 5 · 3840 7 · 3880 9 · 3920 11 · 3960 13 · 4000 15 · 4040 17 · 4080 19 · 4120 21 · 4160 23 · 4199 T/M

Vertical Polarisation

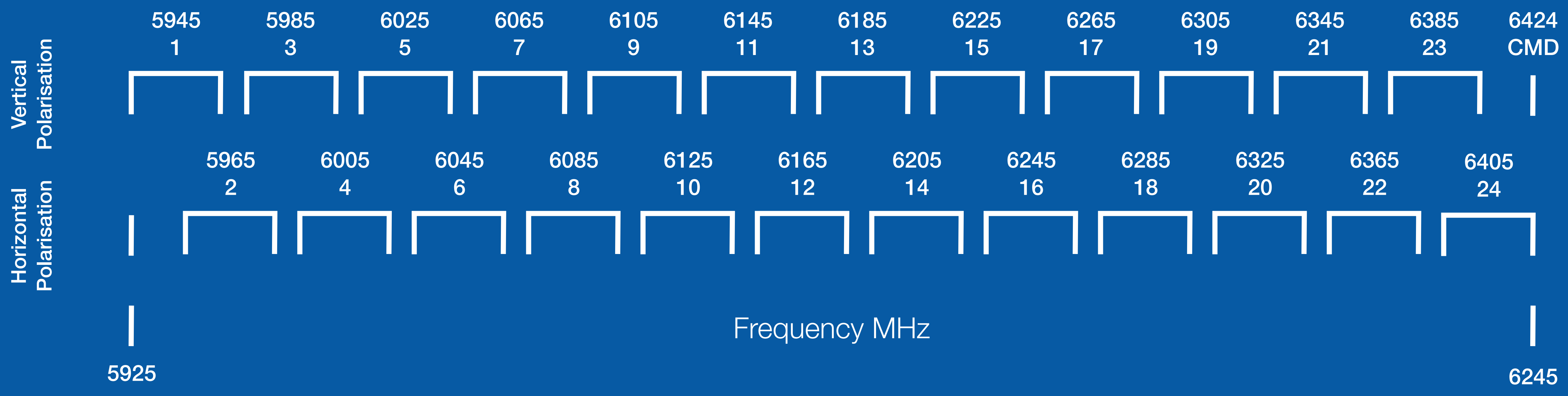
3701 T/M · 3740 2 · 3780 4 · 3820 6 · 3860 8 · 3900 10 · 3940 12 · 3980 14 · 4020 16 · 4060 18 · 4100 20 · 4140 22 · 4180 24

Frequency MHz

3700

4200

Receive



Vertical Polarisation

5945 1 · 5985 3 · 6025 5 · 6065 7 · 6105 9 · 6145 11 · 6185 13 · 6225 15 · 6265 17 · 6305 19 · 6345 21 · 6385 23 · 6424 CMD

Horizontal Polarisation

5965 2 · 6005 4 · 6045 6 · 6085 8 · 6125 10 · 6165 12 · 6205 14 · 6245 16 · 6285 18 · 6325 20 · 6365 22 · 6405 24

Frequency MHz

5925

6245

Channel spacing = 40 MHz — Usable bandwidth = 36 MHz

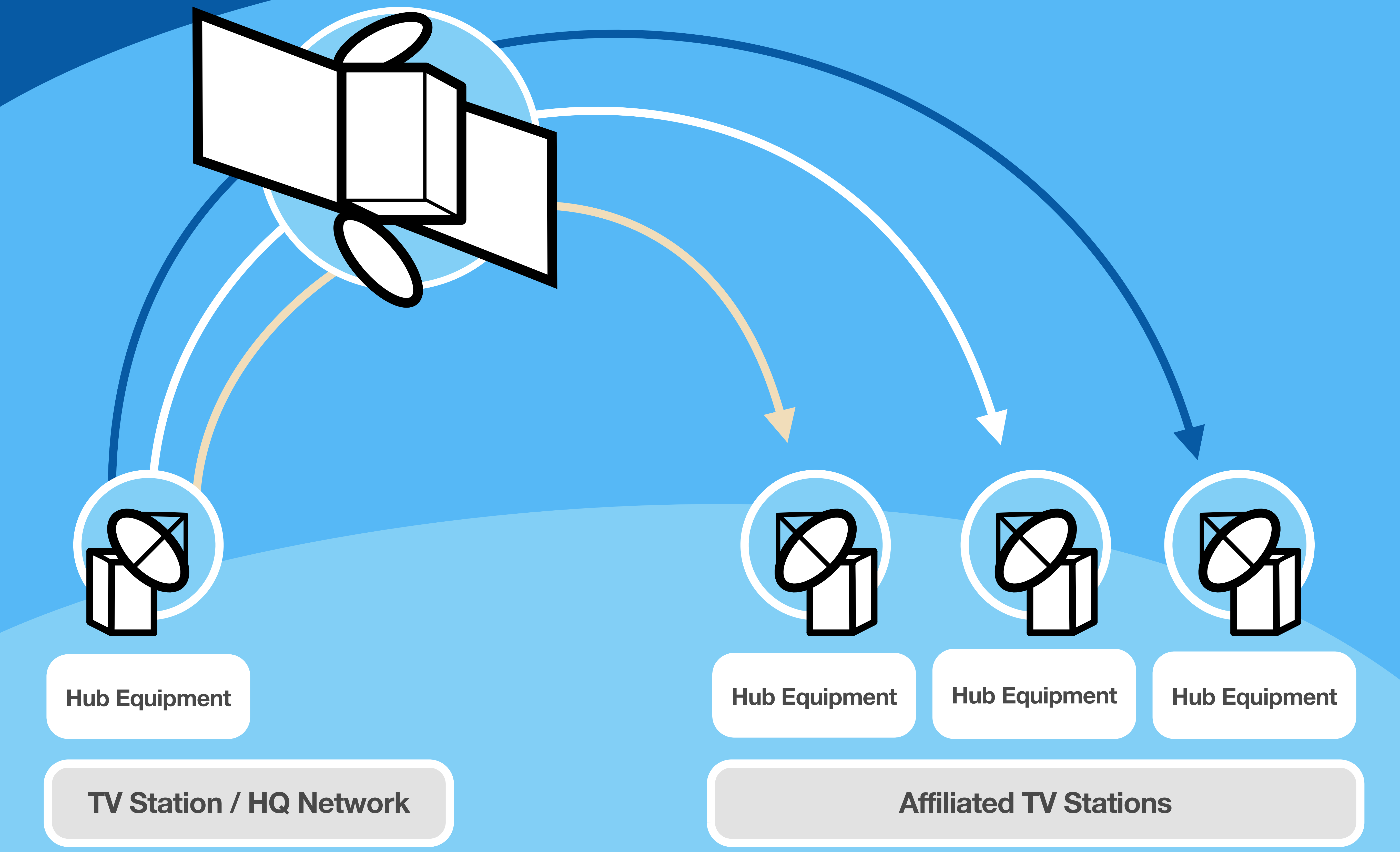
VSAT / Very Small Aperture Terminal

- **Two-way** satellite communication
- Use **small dish** antennas
  (diameter: 75cm-2,4m)
- Managed by the **HUB**
  (master earth station)

VSAT / Services

- One-way multicast
- One-way with terrestrial return
- Two-way satellite access

VSAT Network Topologies / Simplex Transmission



Hub Equipment

TV Station / HQ Network

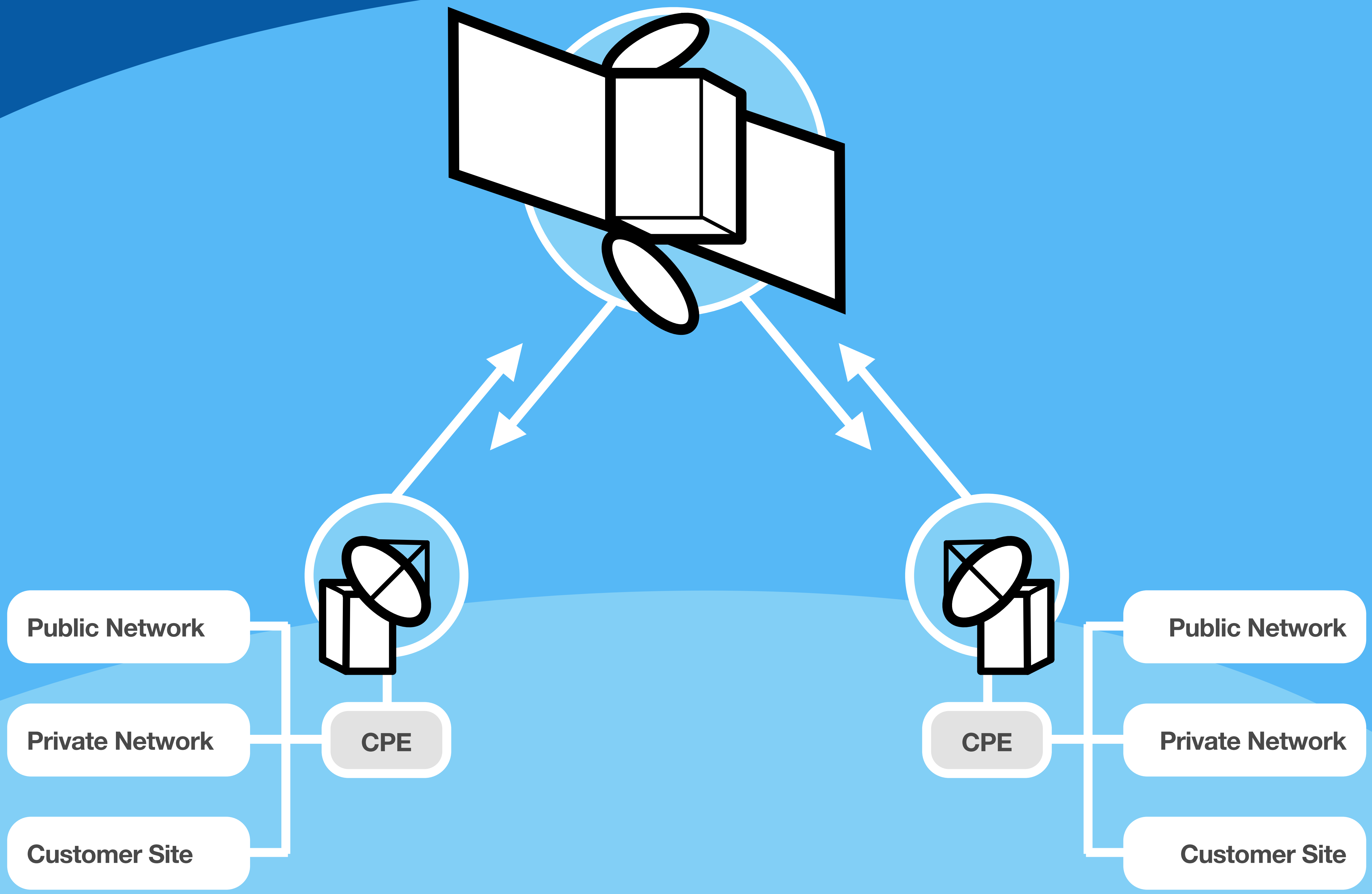
Hub Equipment

Hub Equipment

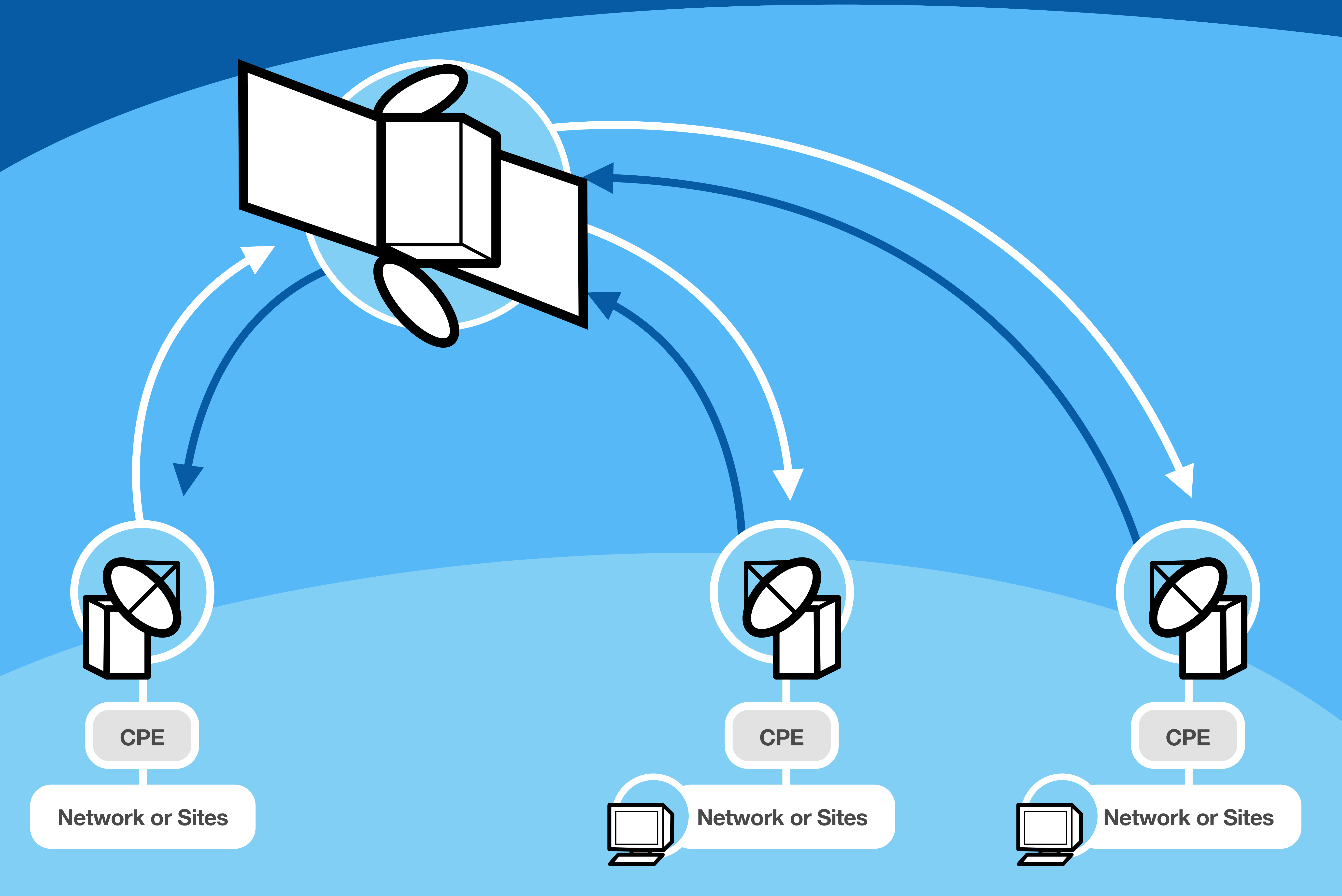
Hub Equipment

Affiliated TV Stations

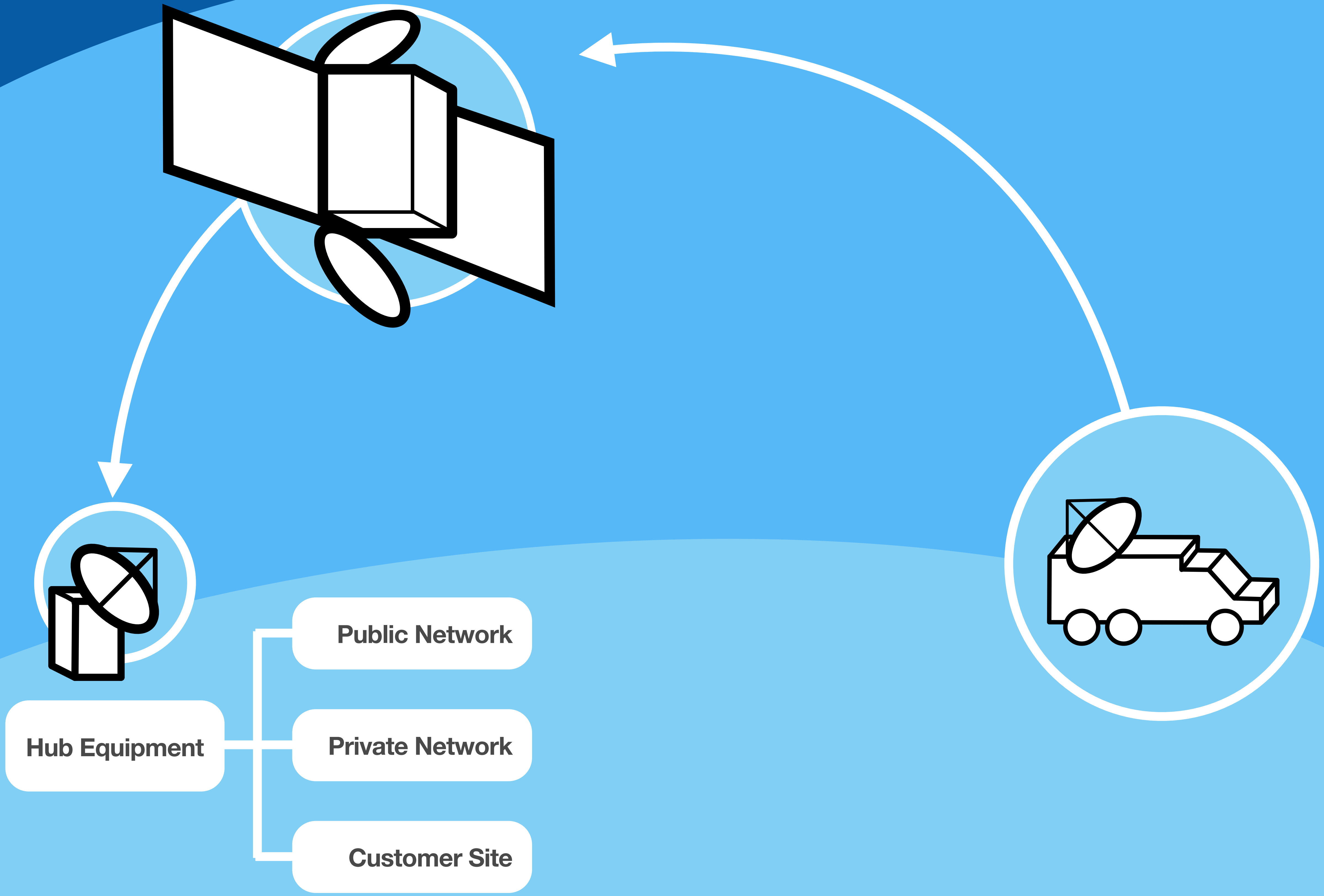
VSAT Network Topologies / Point-to-Point Duplex Transmission



VSAT Network Topologies / Point-to-Multipoint Transmission



VSAT Network Topologies / Mobile Antenna Service



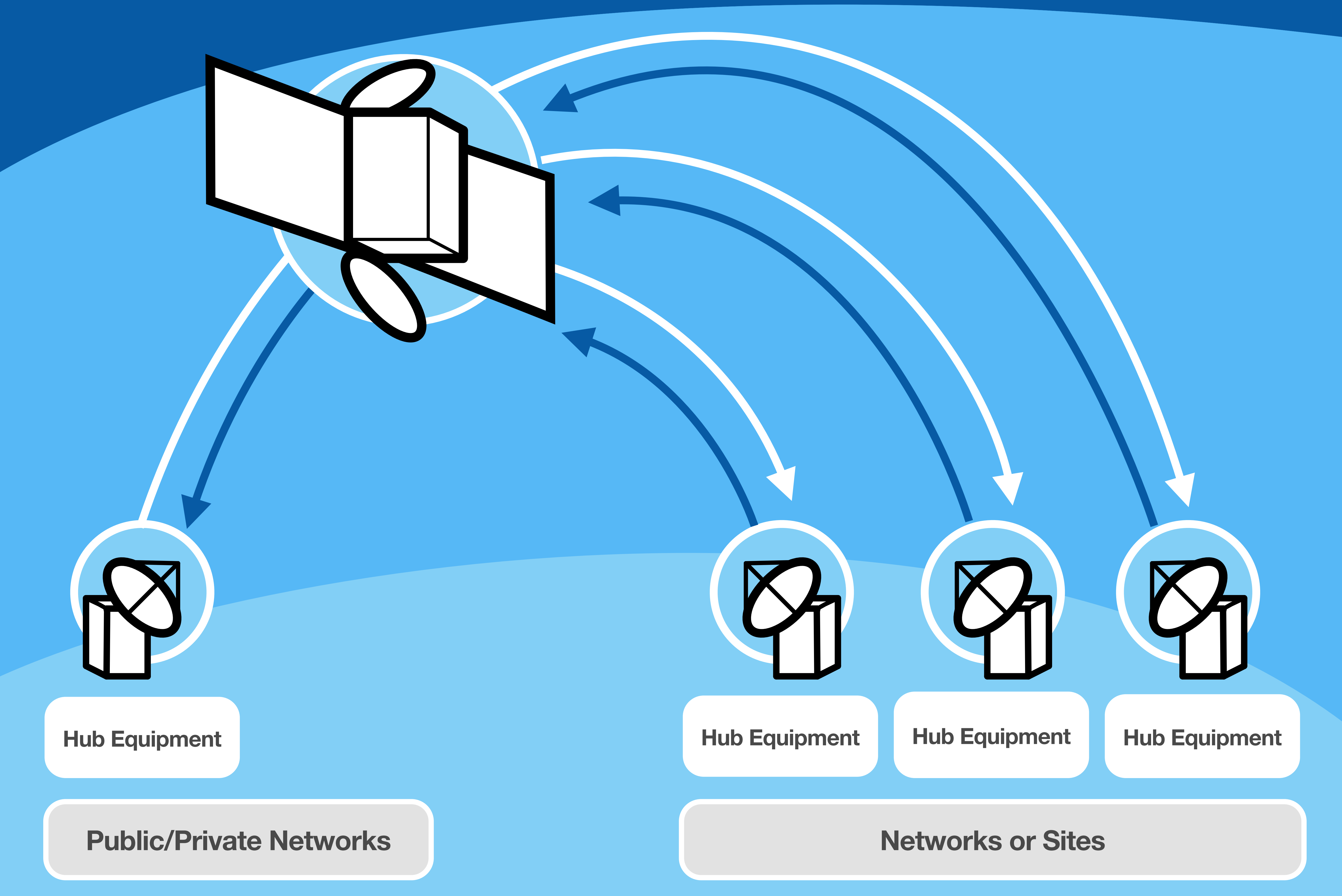
Hub Equipment

Public Network

Private Network

Customer Site

VSAT Network Topologies / Star Network



Hub Equipment

Hub Equipment

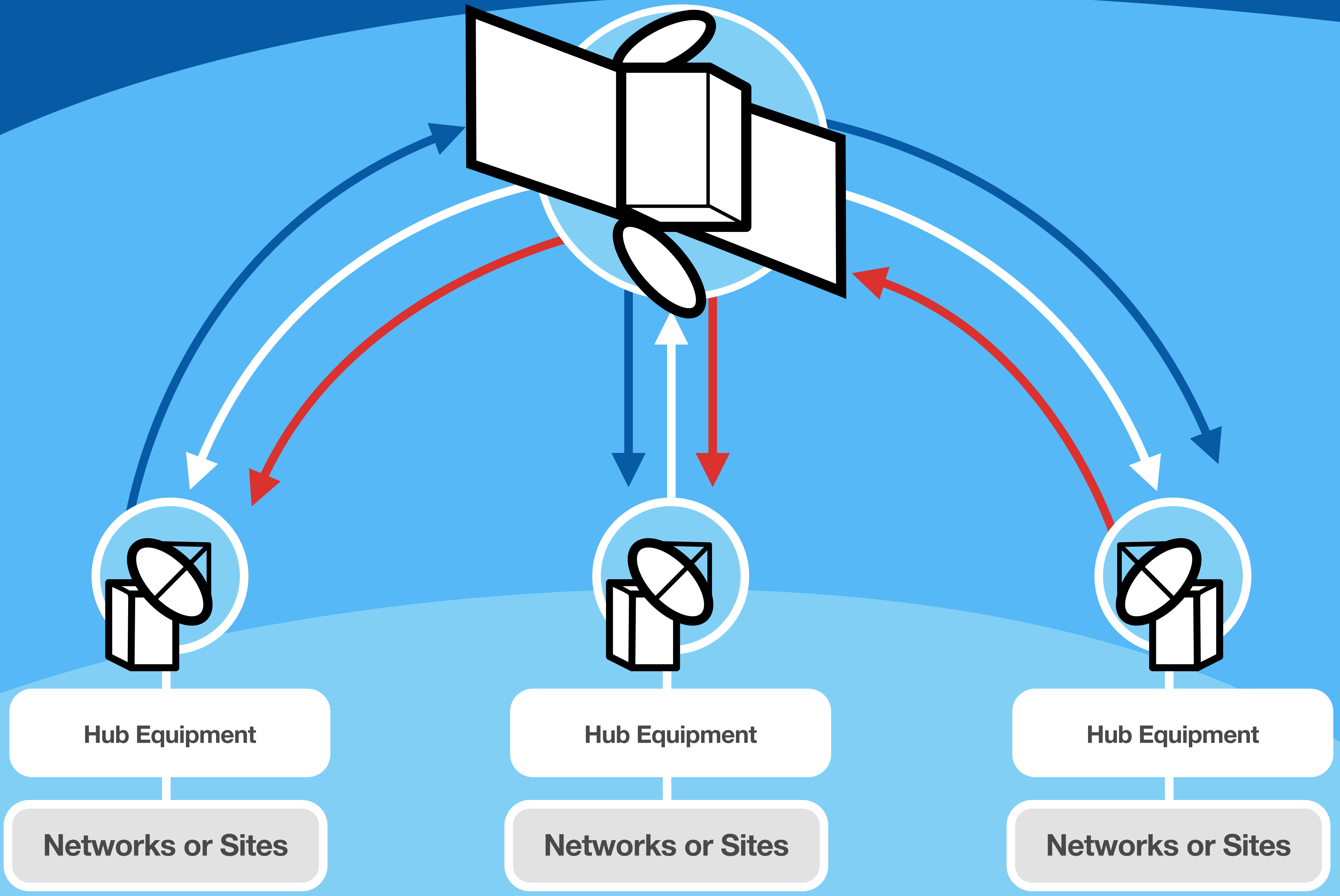
Hub Equipment

Hub Equipment

Public/Private Networks

Networks or Sites

VSAT Network Topologies / Mesh Network



Hub Equipment

Networks or Sites

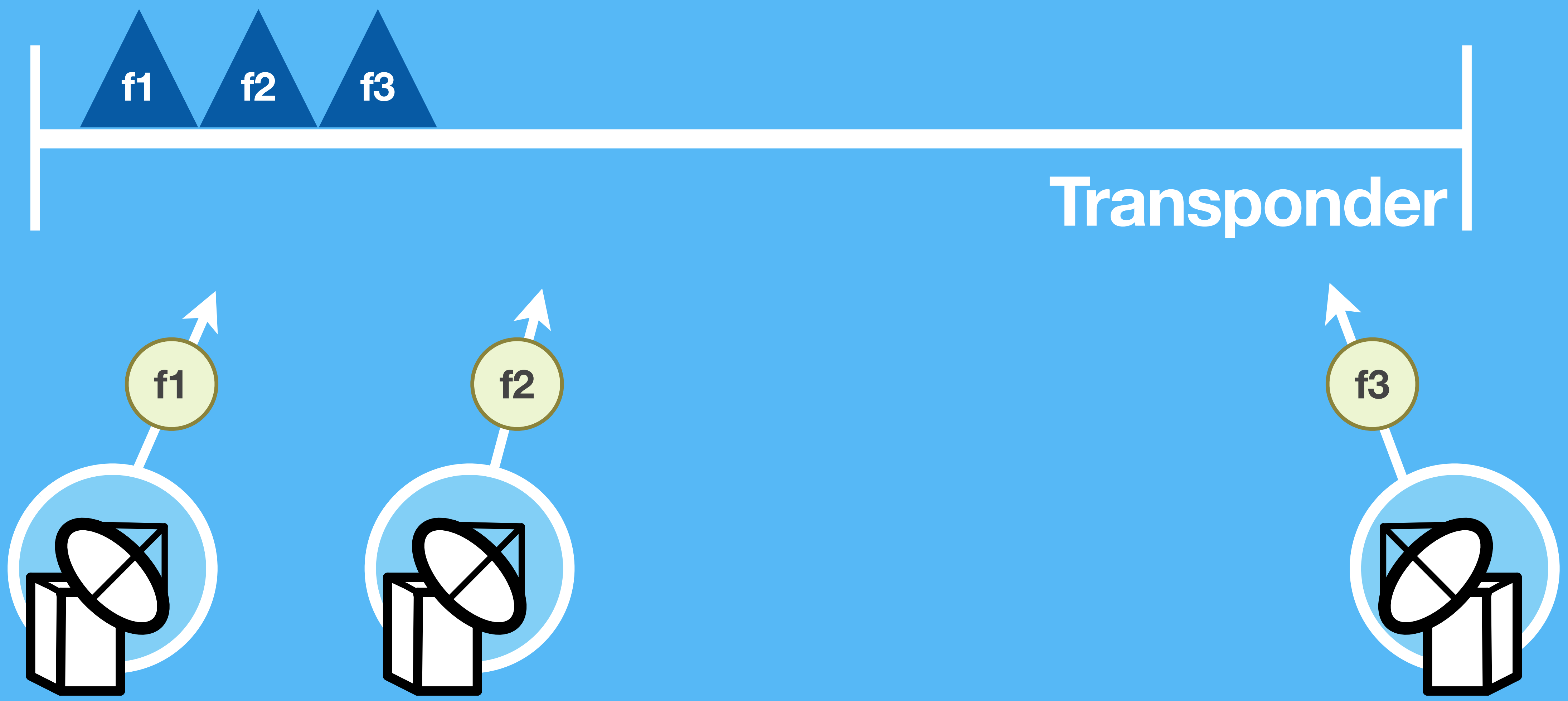
Hub Equipment

Networks or Sites

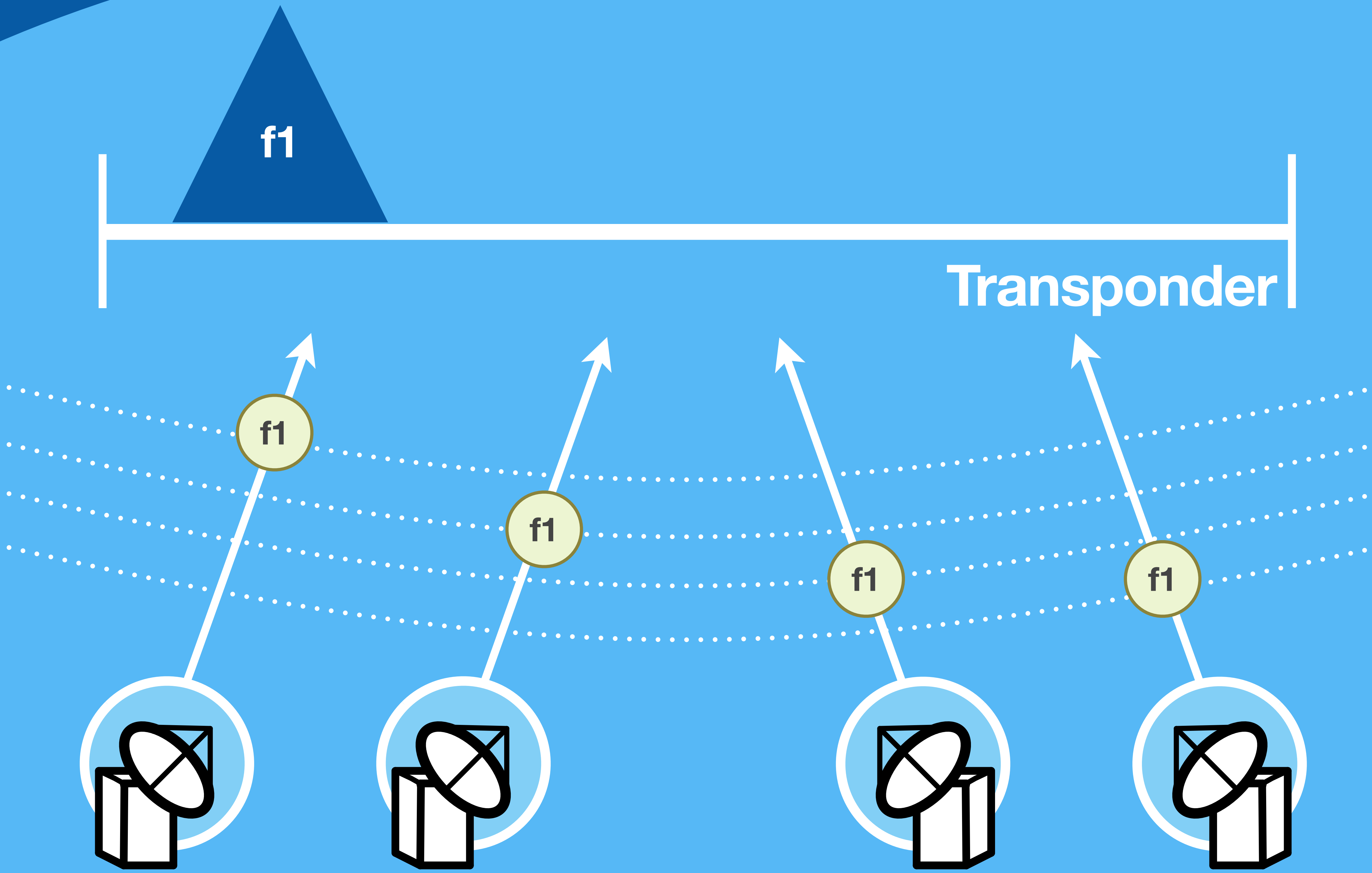
Hub Equipment

Networks or Sites

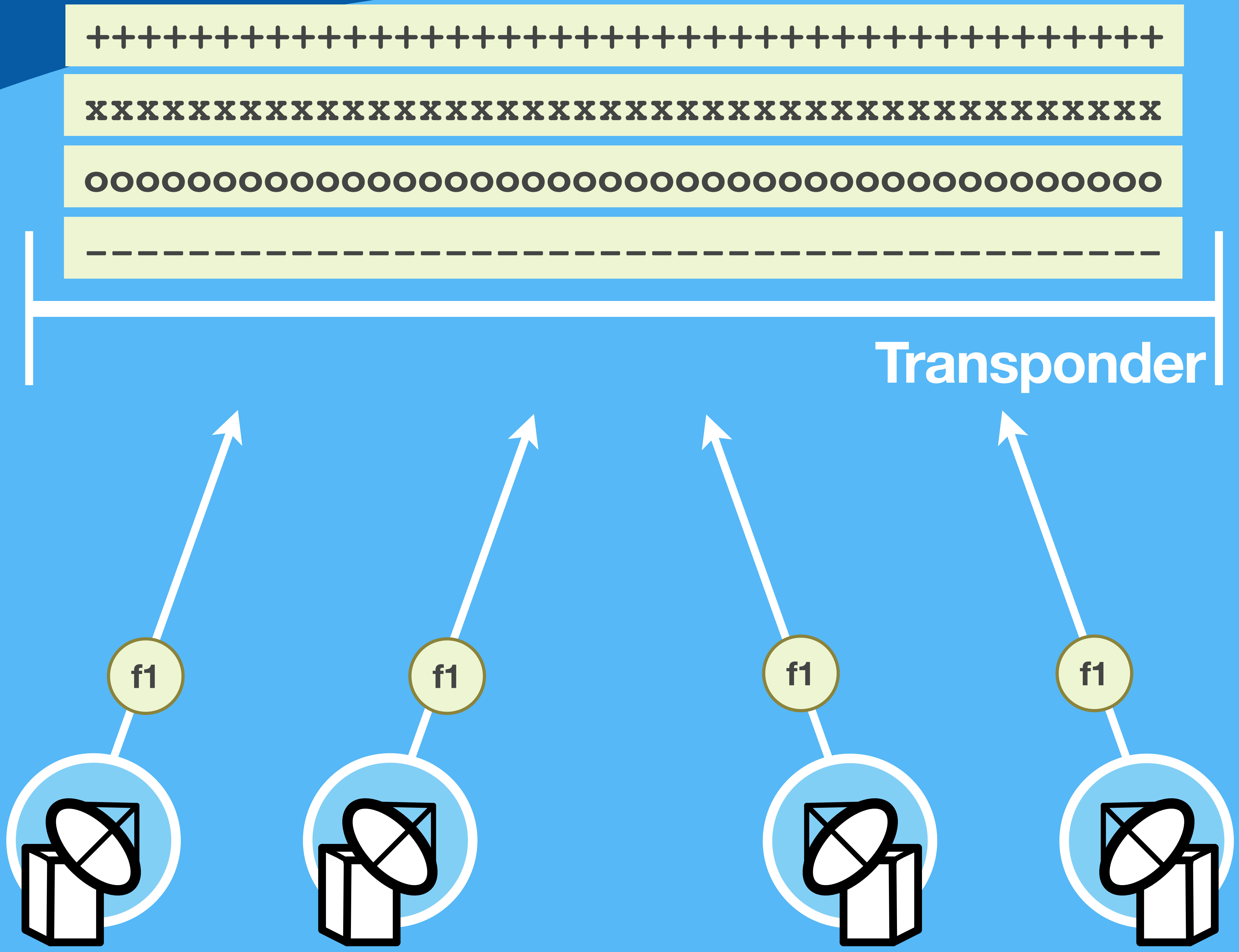
Access Methods / FDMA (Frequency Division Multiple Access)



Access Methods / TDMA (Time Division Multiple Access)



Access Methods / CDMA (Code Division Multiple Access)



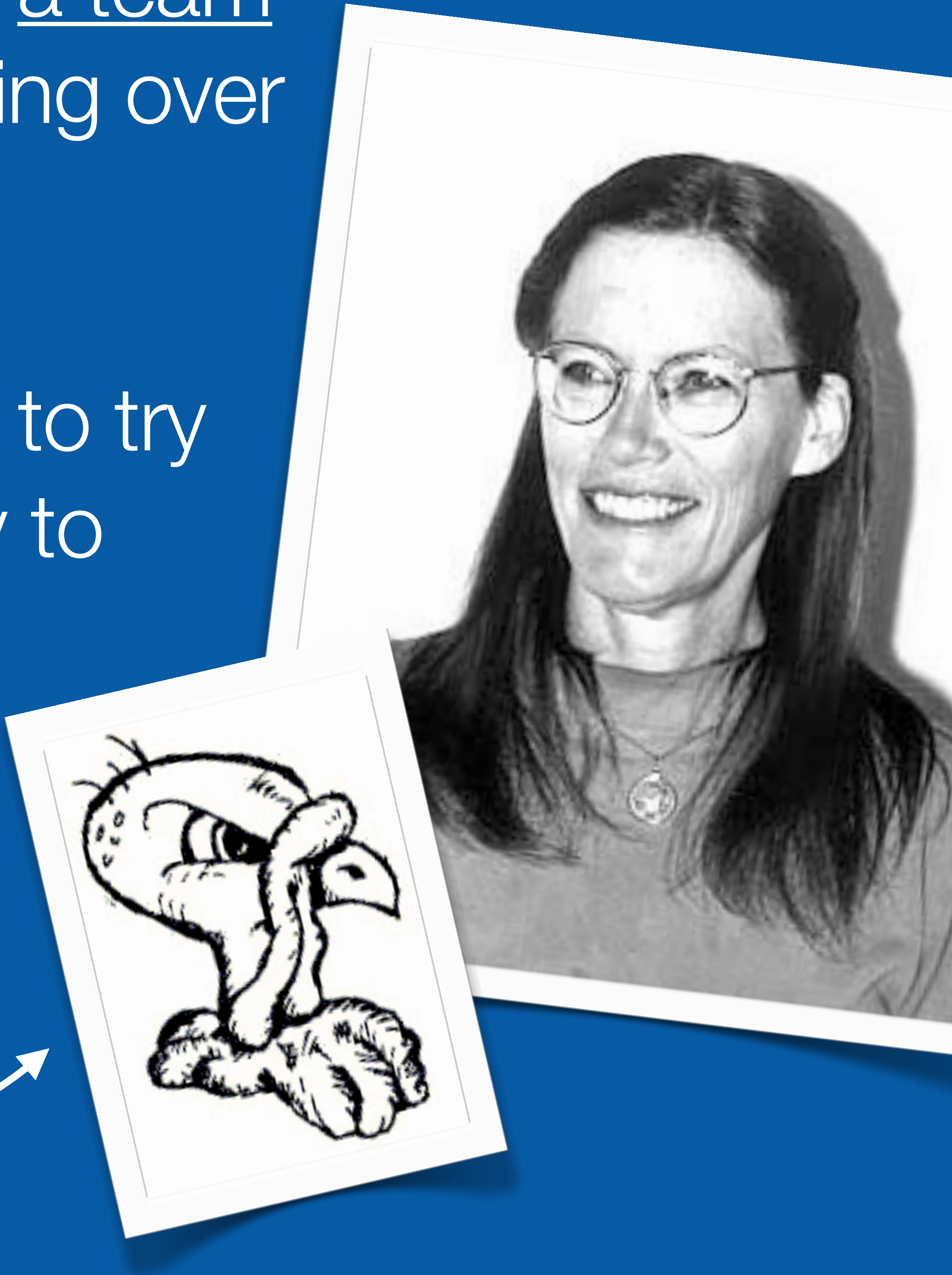
Satellite Vulnerabilities

Current systems are **vulnerable** to a variety of attacks, and future systems **promise little improvement**.

Unless you have millions of dollars and a team of engineers, you have **no hope** of taking over commercial or governmental satellites.

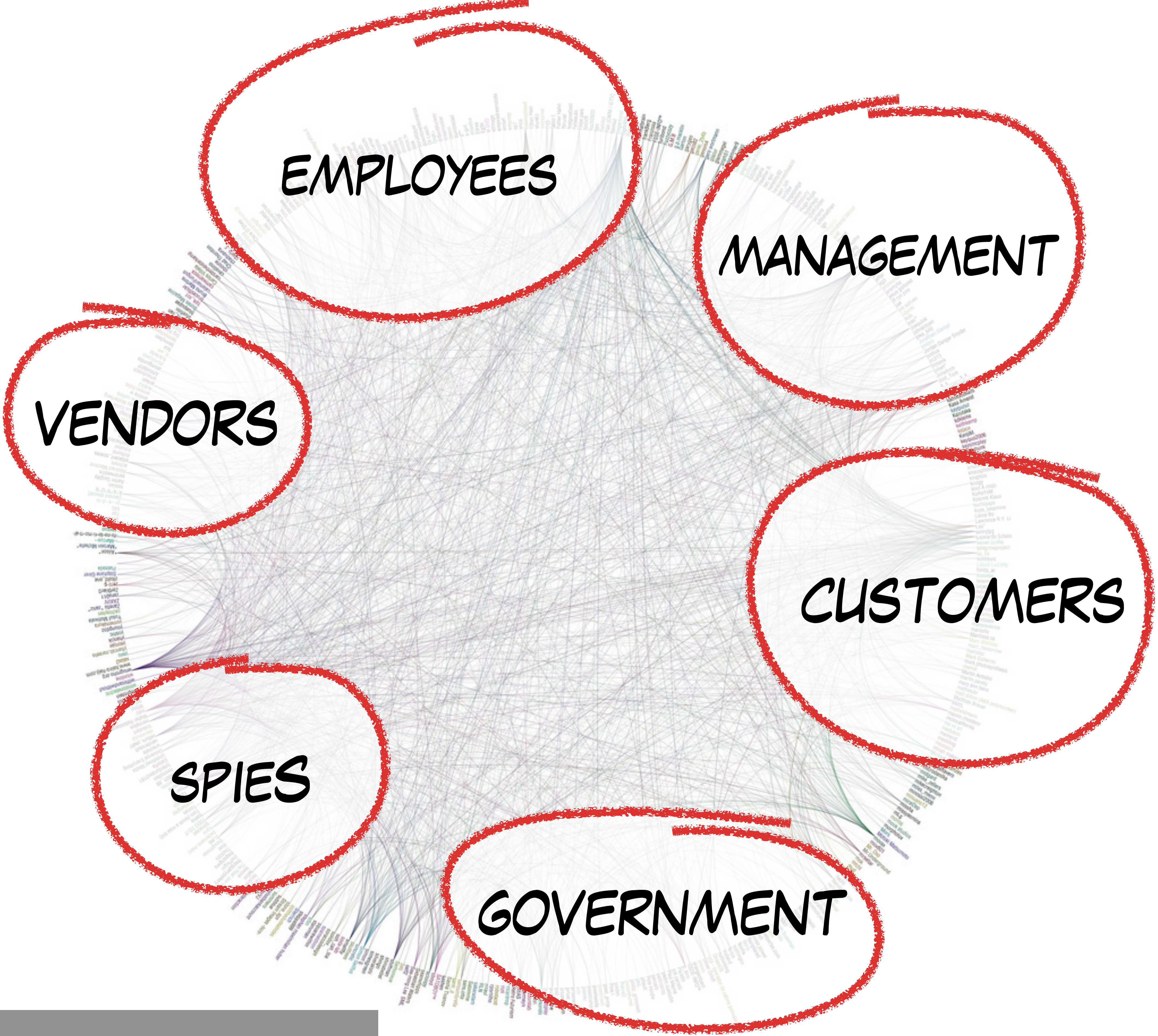
If someone did put together the power to try such a stunt, they would be more likely to **damage** a satellite than take it over.

How to Break into Satellites: Not!
Carolyn Meinel's GUIDE TO (mostly) HARMLESS HACKING



GOBBLES! →

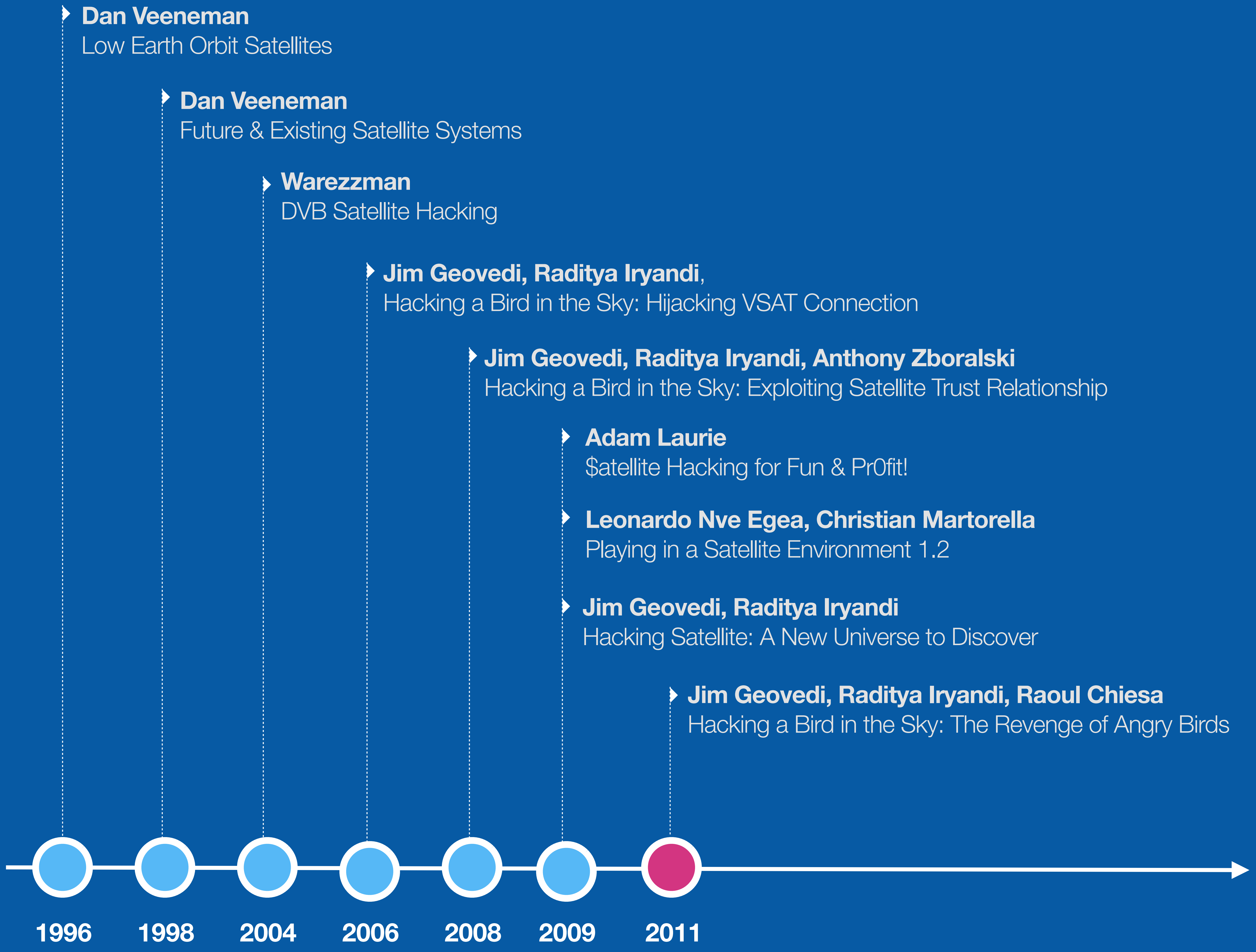
hackers will **eventually** find a way to hack



network of trust

It is worth noting that **the most likely cause of damage** to or loss of service from a satellite **is the actual operator**.

Dan Veeneman



Dan Veeneman
Low Earth Orbit Satellites

Dan Veeneman
Future & Existing Satellite Systems

Warezzman
DVB Satellite Hacking

Jim Geovedi, Raditya Iryandi,
Hacking a Bird in the Sky: Hijacking VSAT Connection

Jim Geovedi, Raditya Iryandi, Anthony Zboralski
Hacking a Bird in the Sky: Exploiting Satellite Trust Relationship

Adam Laurie
$atellite Hacking for Fun & Pr0fit!

Leonardo Nve Egea, Christian Martorella
Playing in a Satellite Environment 1.2

Jim Geovedi, Raditya Iryandi
Hacking Satellite: A New Universe to Discover

Jim Geovedi, Raditya Iryandi, Raoul Chiesa
Hacking a Bird in the Sky: The Revenge of Angry Birds

1996 **1998** **2004** **2006** **2008** **2009** **2011**

Veeneman’s Satellite Hypothetical Attacks

Denial of Service

Jam Uplink

Overpower Uplink

Jam Downlink

Orbital Positioning

Raging Transponder Spoofing

Direct Commanding

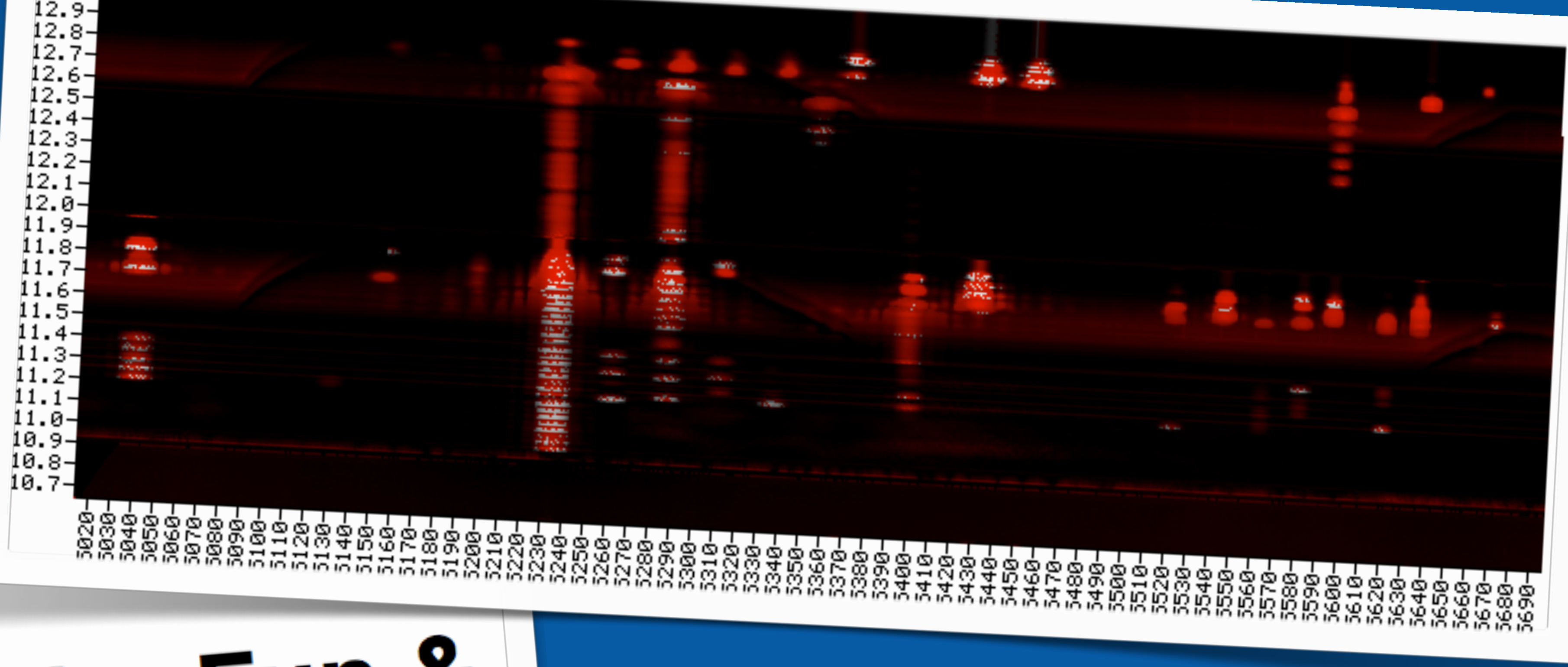
Command Replay

Insertion

Takeover Spare Satellite

?

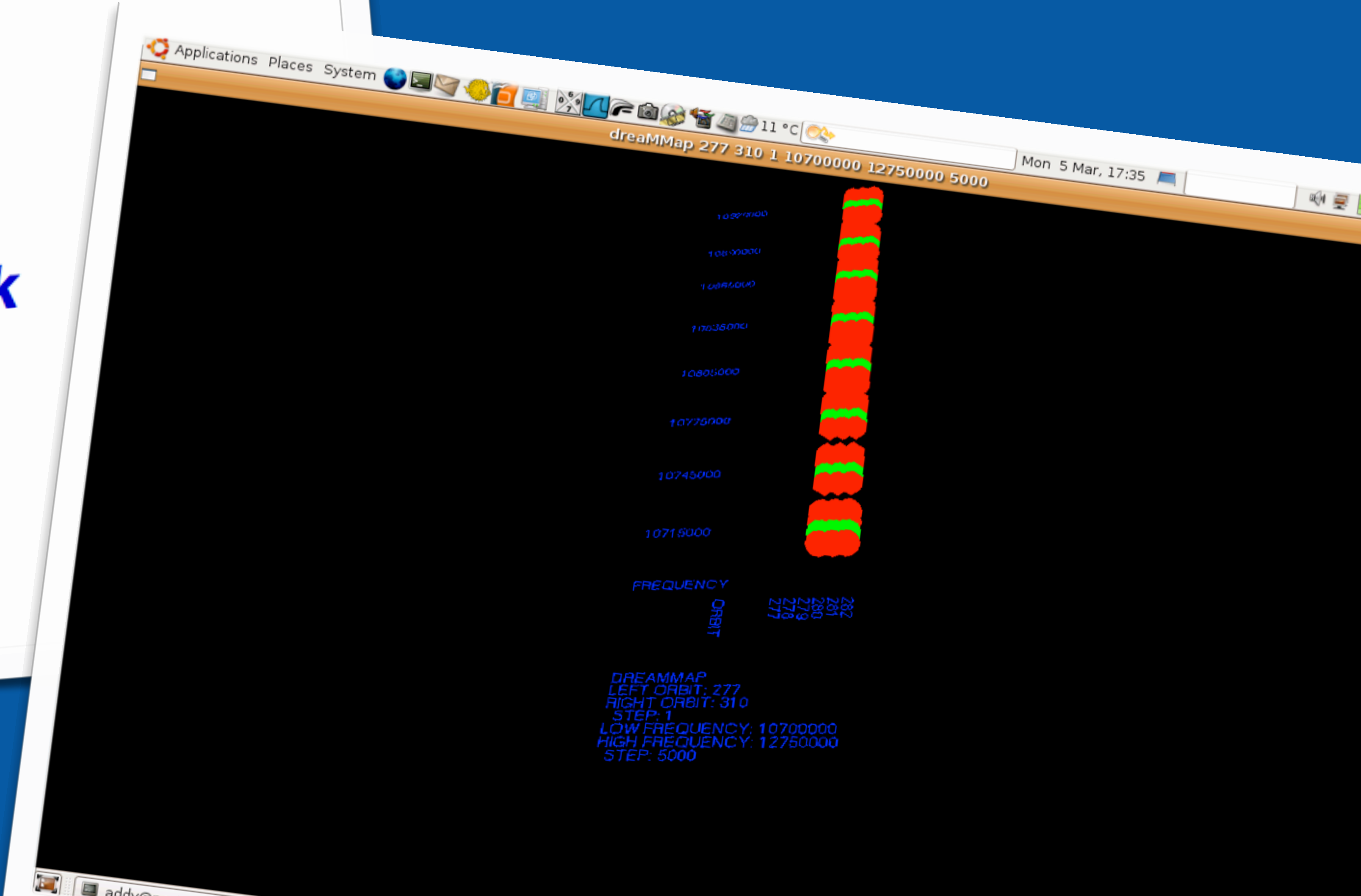
Satellite Operation Centre



$atellite Hacking for Fun & Pr0fit!

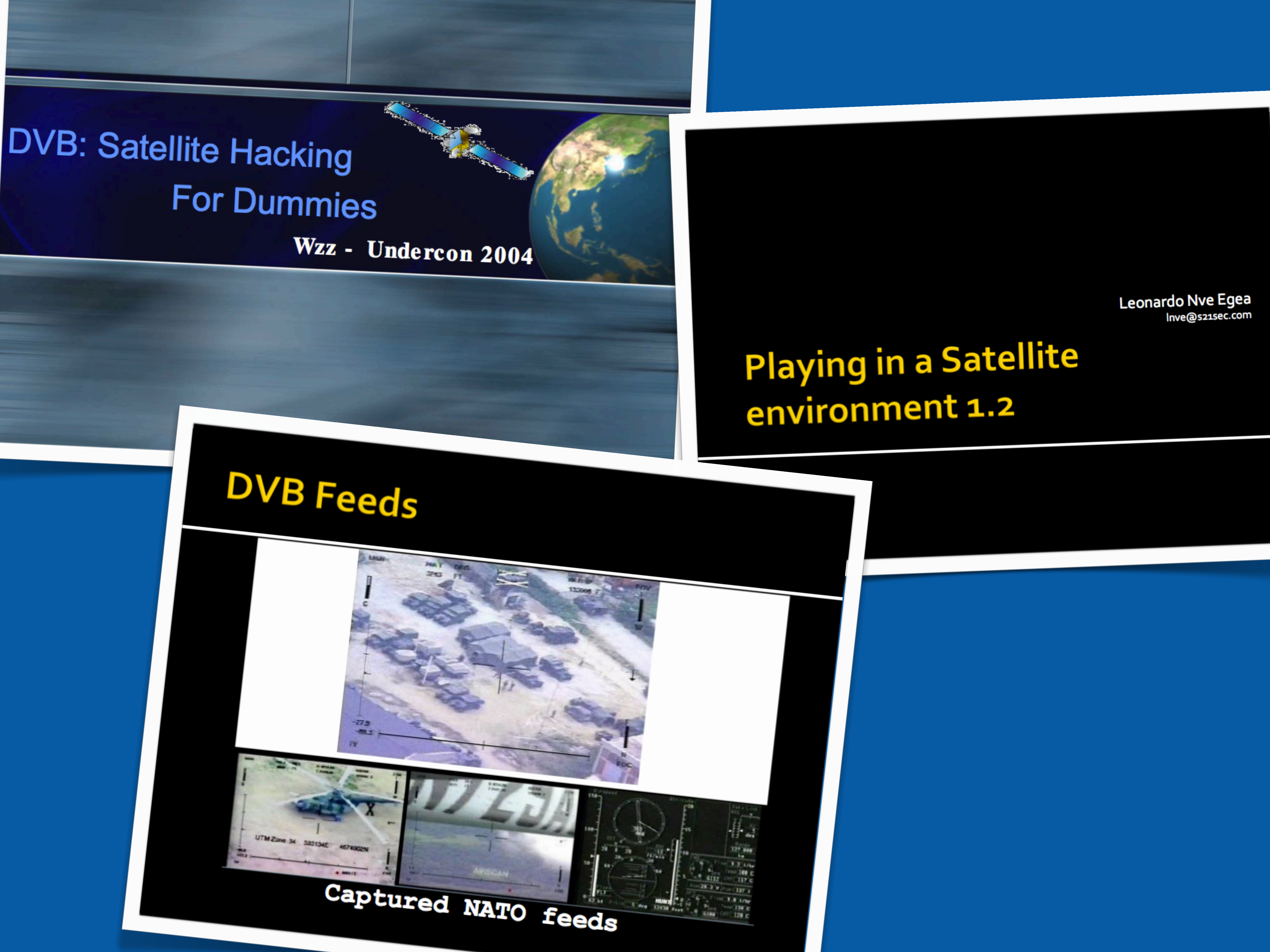
Adam Laurie
adam@algroup.co.uk

http://rfidiot.org



```
dreaMMap 277 310 1 10700000 12750000 5000
```

```
DREAMMAP
LEFT ORBIT: 277
RIGHT ORBIT: 310
 STEP: 1
LOW FREQUENCY: 10700000
HIGH FREQUENCY: 12750000
 STEP: 5000
```



DVB: Satellite Hacking For Dummies

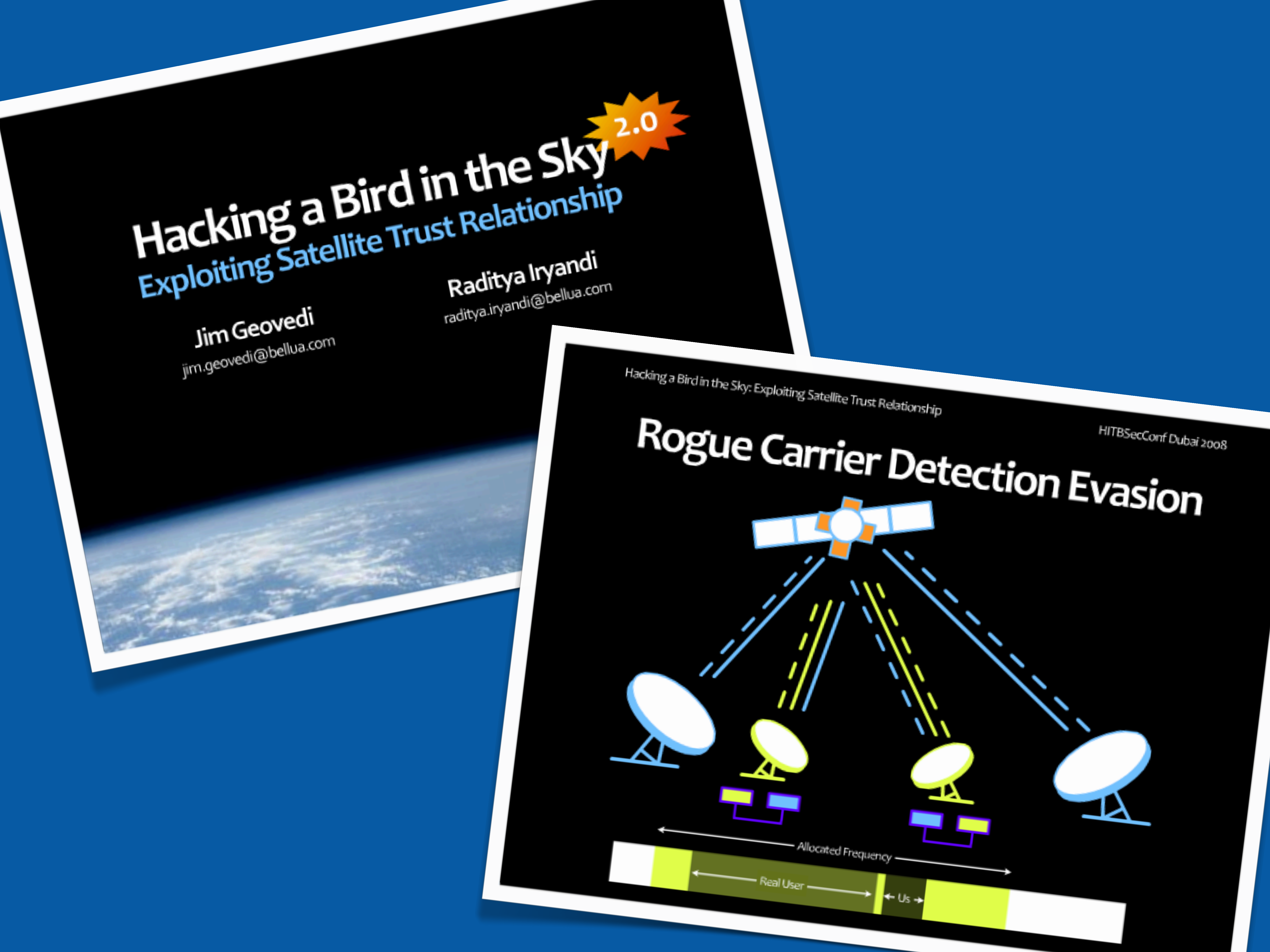
Wzz - Undercon 2004

Leonardo Nve Egea
lnve@s21sec.com

Playing in a Satellite environment 1.2

DVB Feeds

Captured NATO feeds



Hacking a Bird in the Sky 2.0

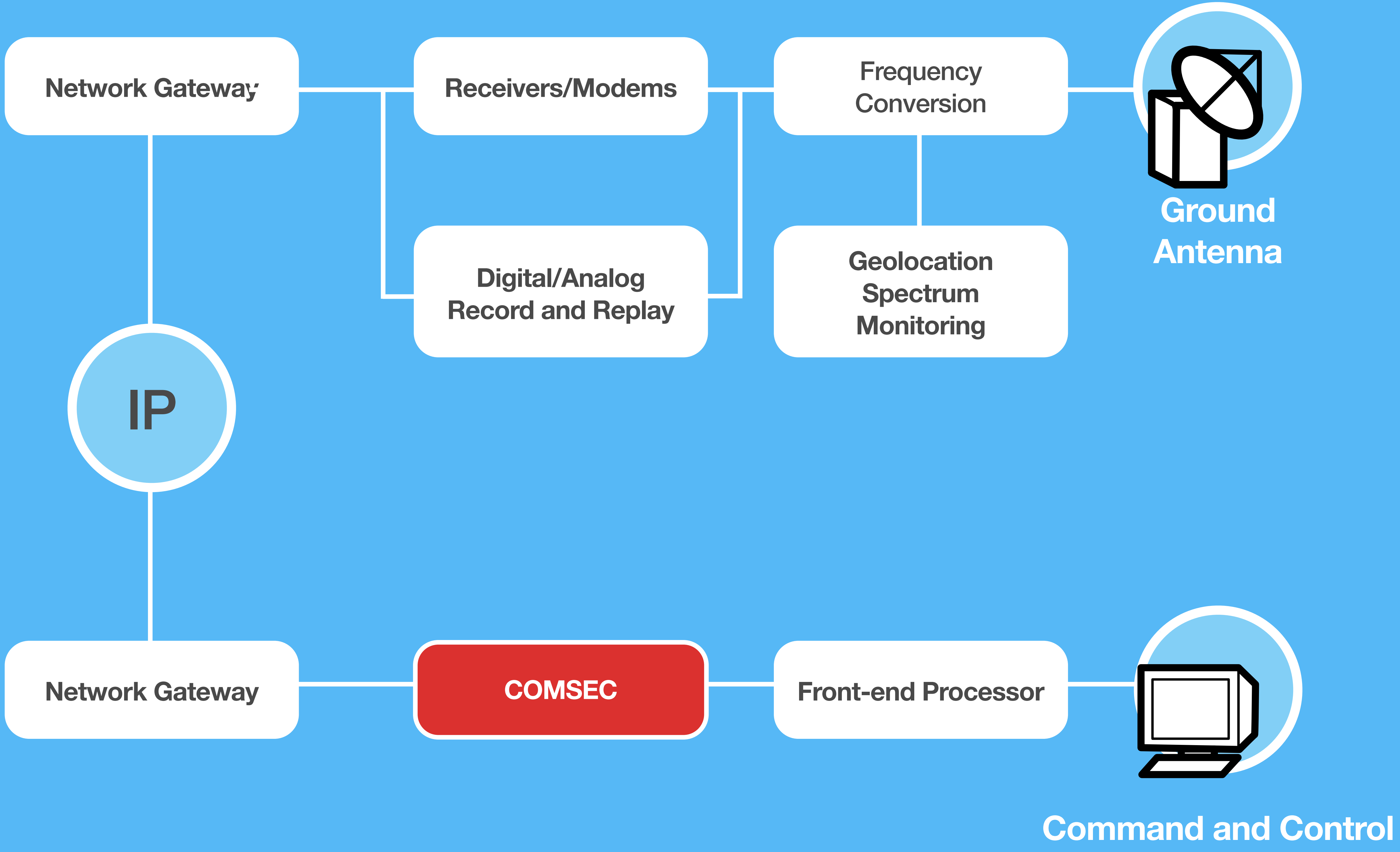
Exploiting Satellite Trust Relationship

Jim Geovedi
jim.geovedi@bellua.com

Raditya Iryandi
raditya.iryandi@bellua.com

Rogue Carrier Detection Evasion

Satellite TT&C Ground Networks



Network Gateway

Receivers/Modems

Frequency Conversion

Ground Antenna

Digital/Analog Record and Replay

Geolocation Spectrum Monitoring

IP

Network Gateway

COMSEC

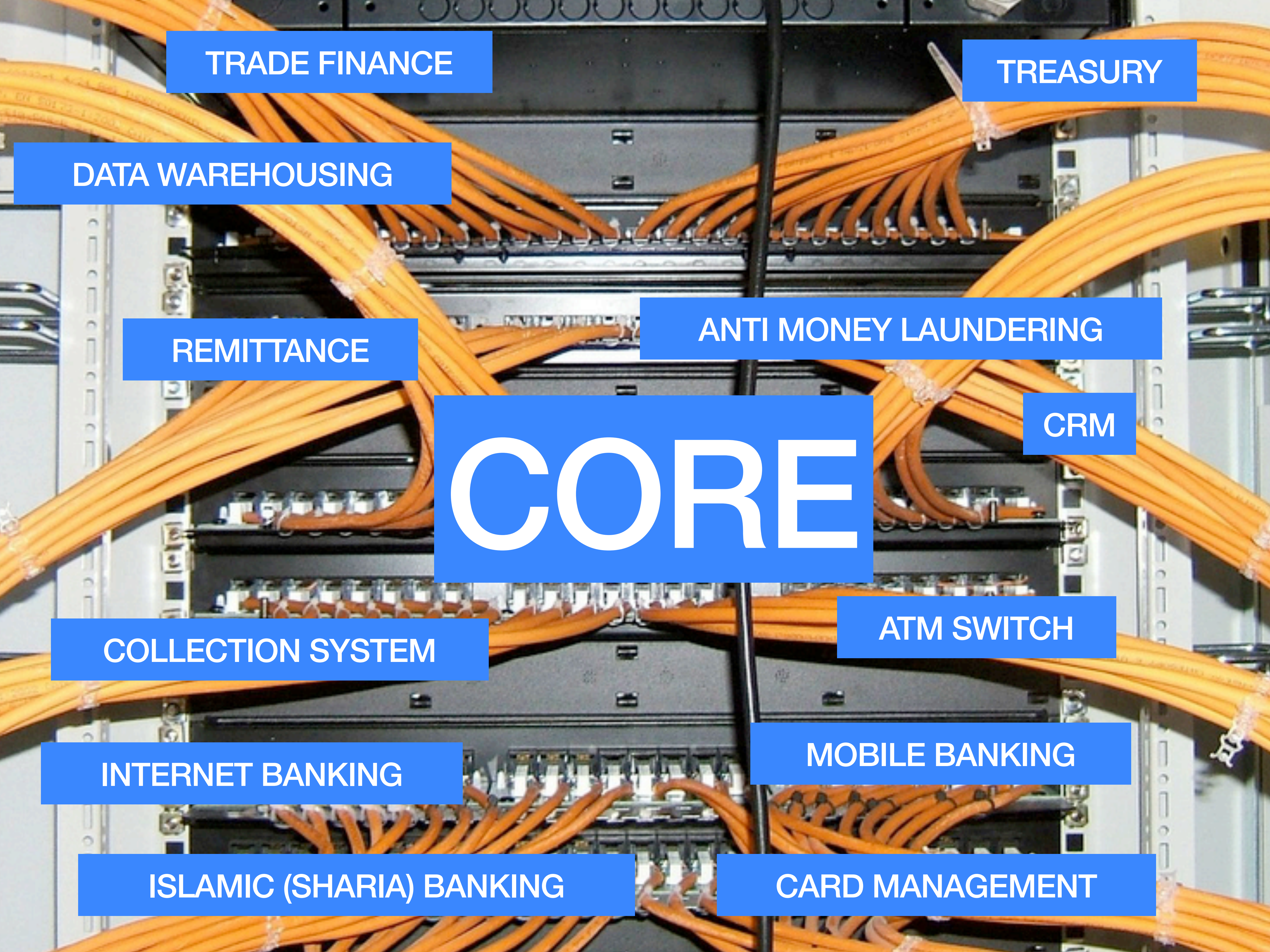
Front-end Processor

Command and Control

Land Earth Station Attacks

Satellite-based Attacks Against ATMs and Bank Networks

It's not a big truck. **It's a series of tubes**.



TRADE FINANCE

TREASURY

DATA WAREHOUSING

ANTI MONEY LAUNDERING

REMITTANCE

CRM

CORE

ATM SWITCH

COLLECTION SYSTEM

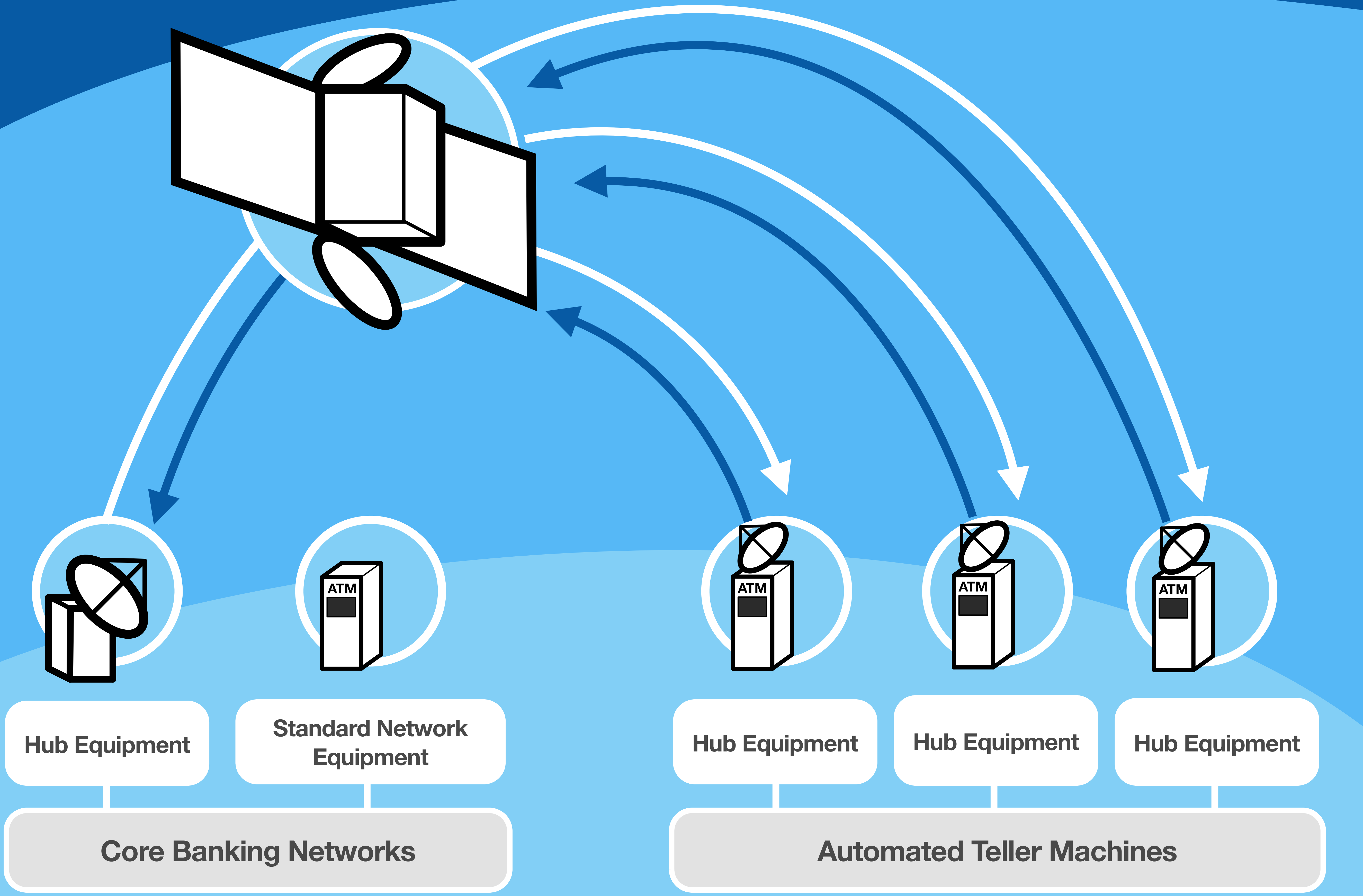
MOBILE BANKING

INTERNET BANKING

ISLAMIC (SHARIA) BANKING

CARD MANAGEMENT

VSAT / Automated Teller Machine Networks



Hub Equipment

Standard Network Equipment

Hub Equipment

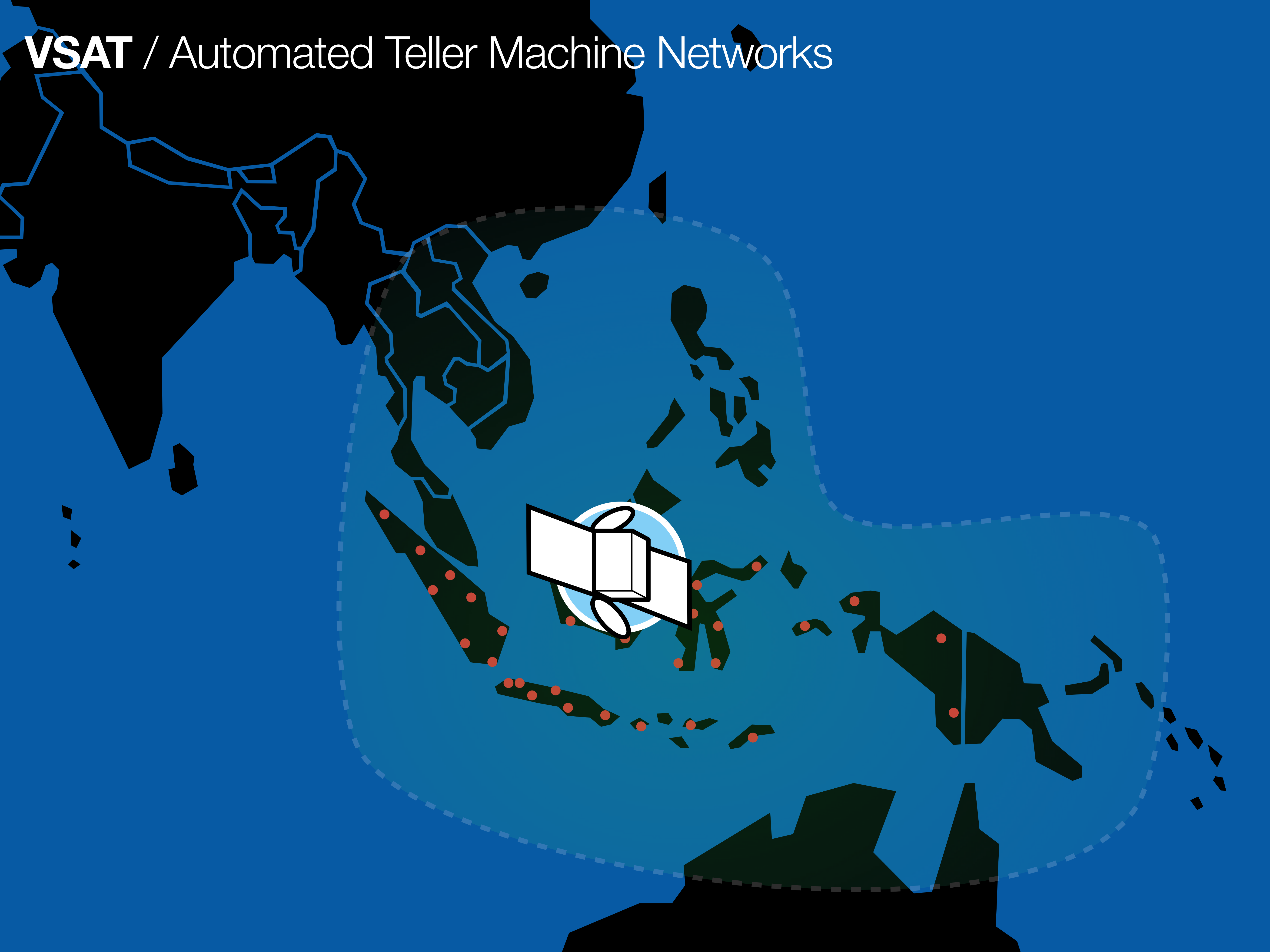
Hub Equipment

Hub Equipment

Core Banking Networks

Automated Teller Machines

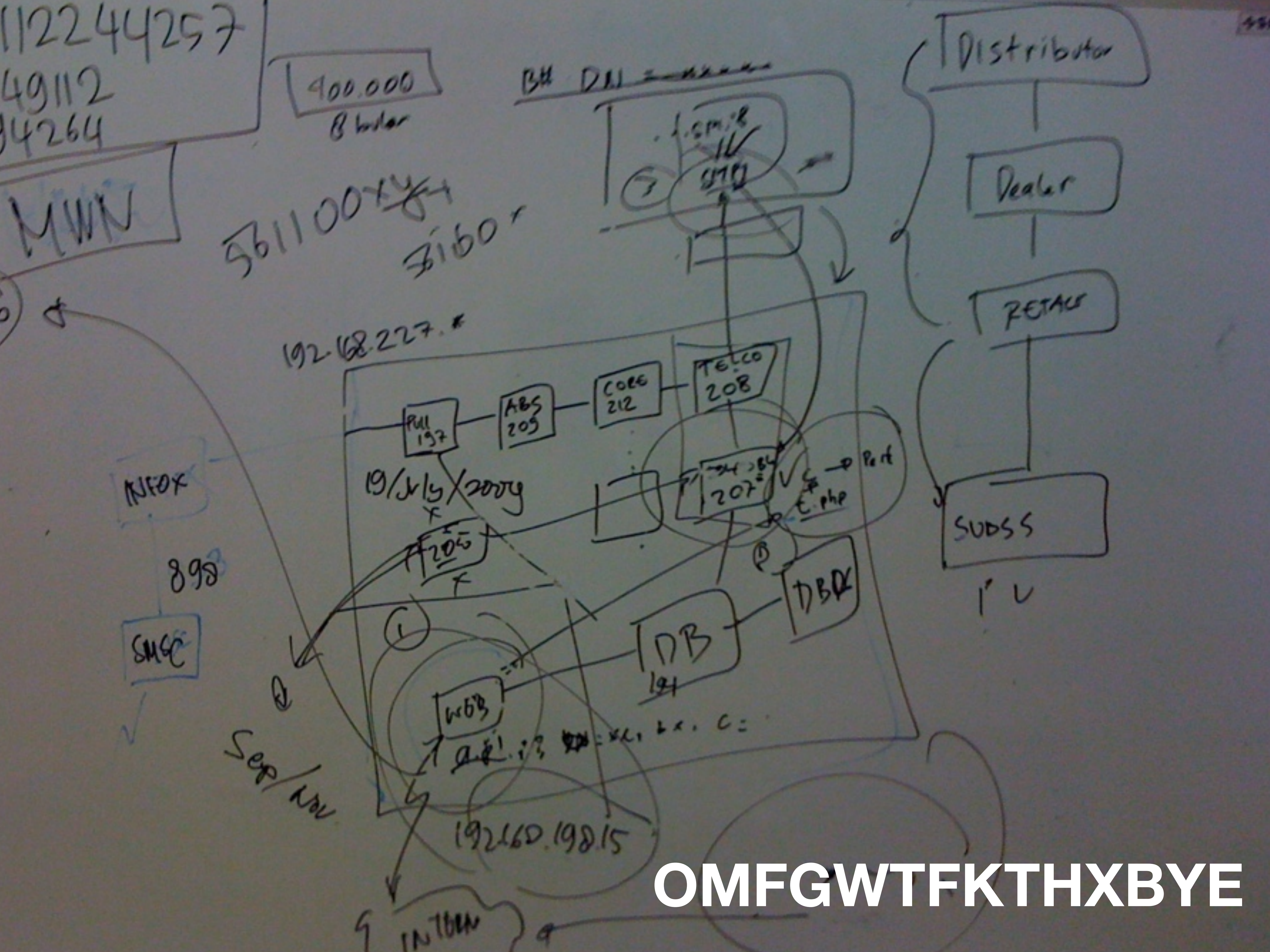
VSAT / Automated Teller Machine Networks



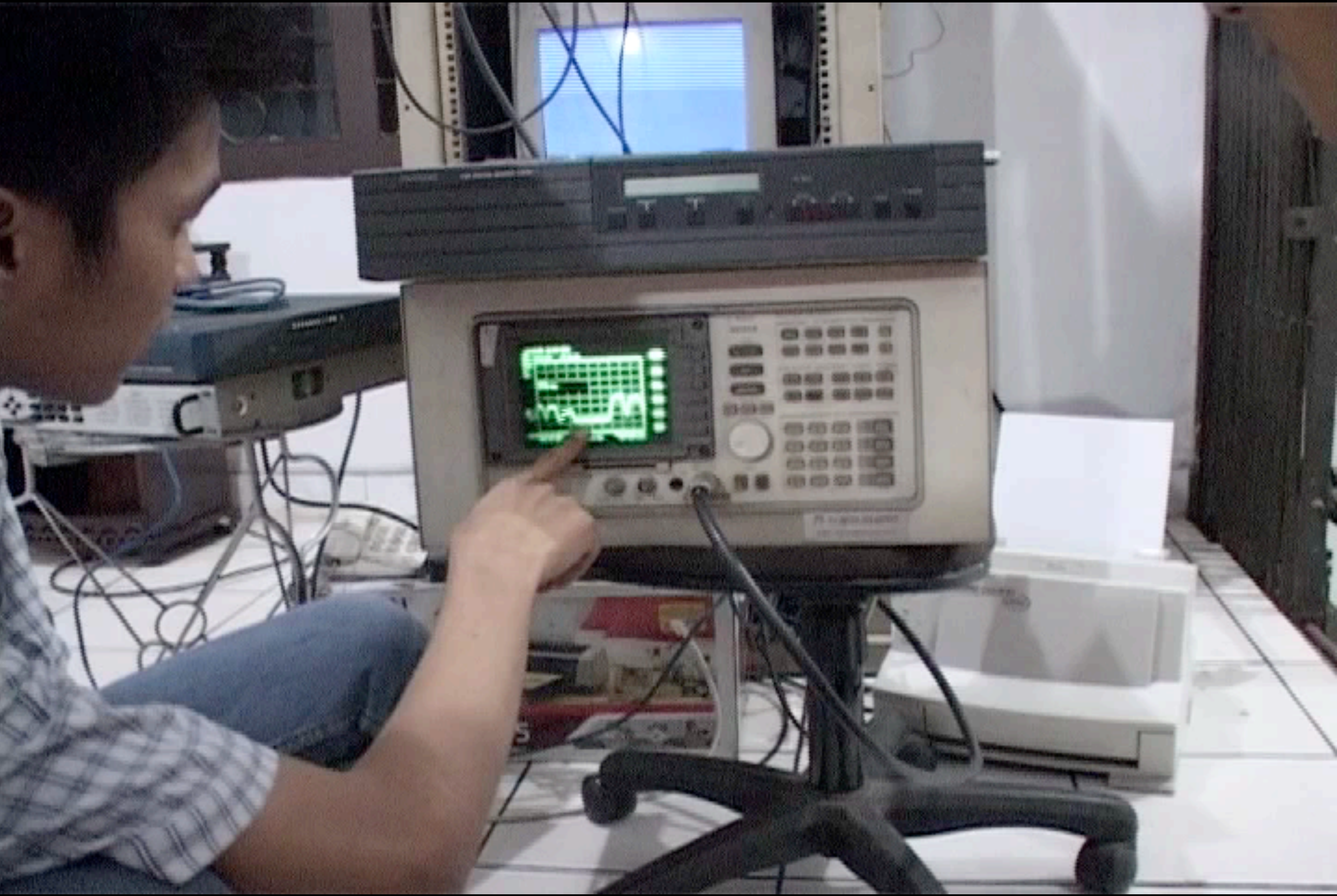
ATM
ATM

Automated Teller Machine

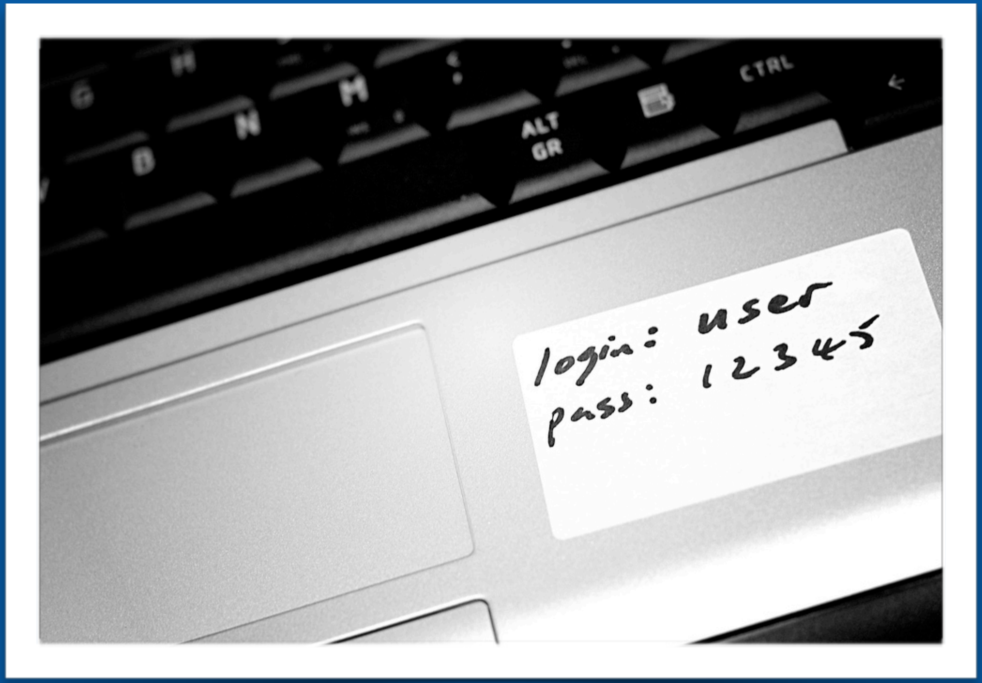
Automated Teller Machine



OMFGWTFKTHXBYE



The Usual Culprits



People Problems

Weak Passwords
Lack of Awareness
Lack of Skills

System Problems

Outdated Systems
Insecure Configurations
Insecure Protocols

MANAGEMENT PROBLEMS

Distributed Satellite Scanning Framework

Identify **potential problems** at an early stage.

Framework Goals

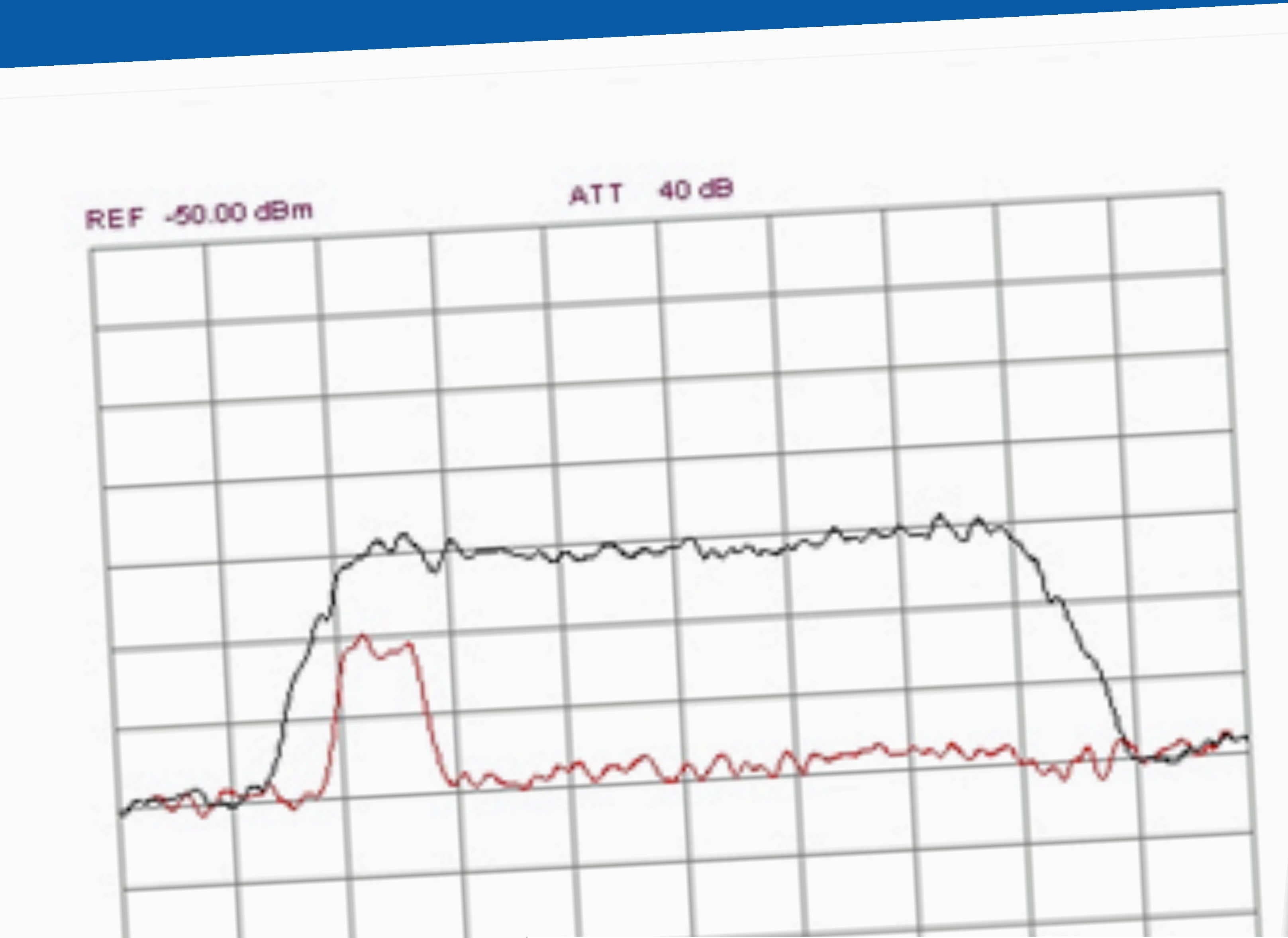
- *Dead or Alive* status / checking if the bird is still alive
- Protocols / understand which protocols the target is running
- Service type / knowing which service we can (ab)use
- Distributed IP C&C / widening the coverage

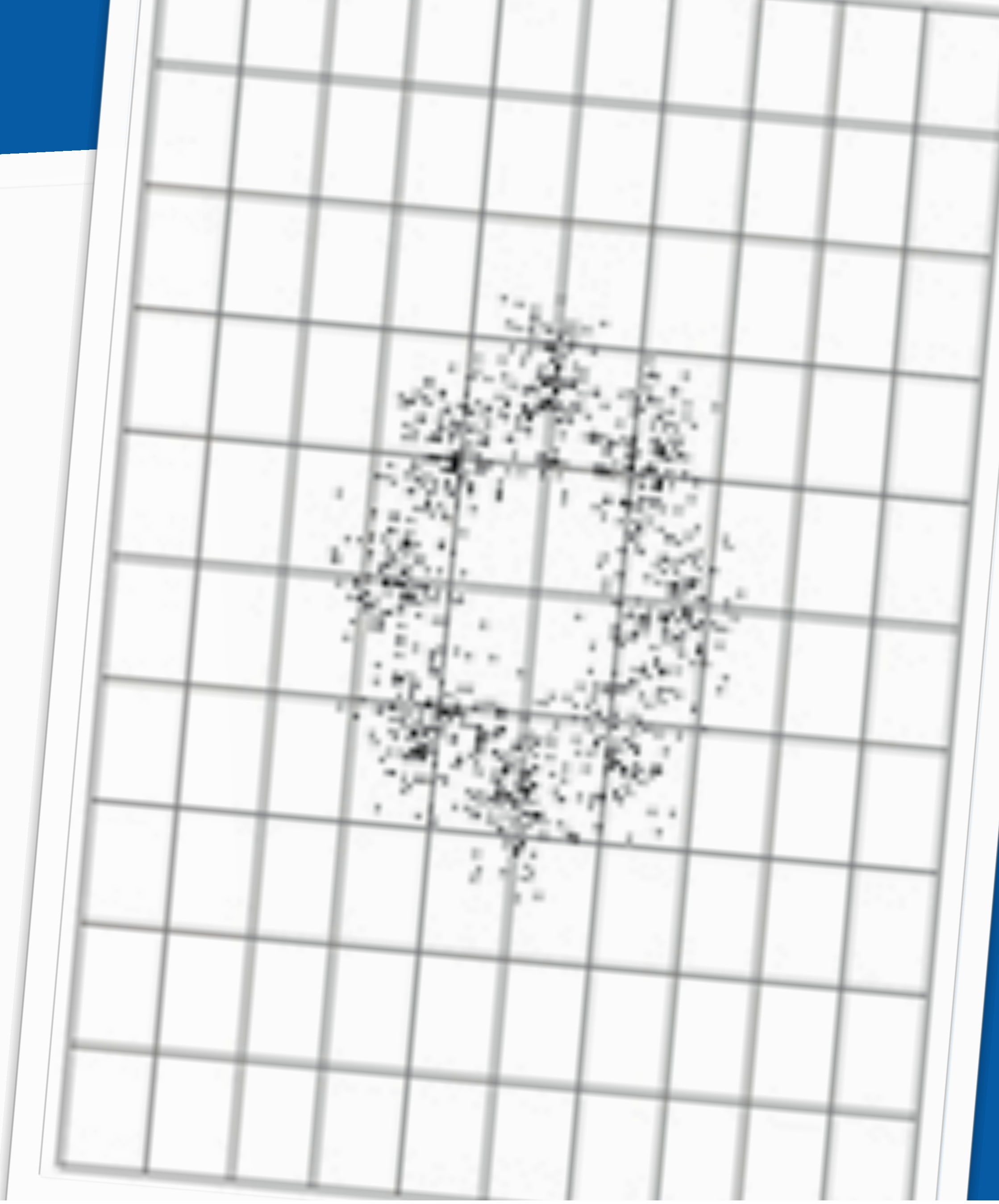
Distributed IP C&C

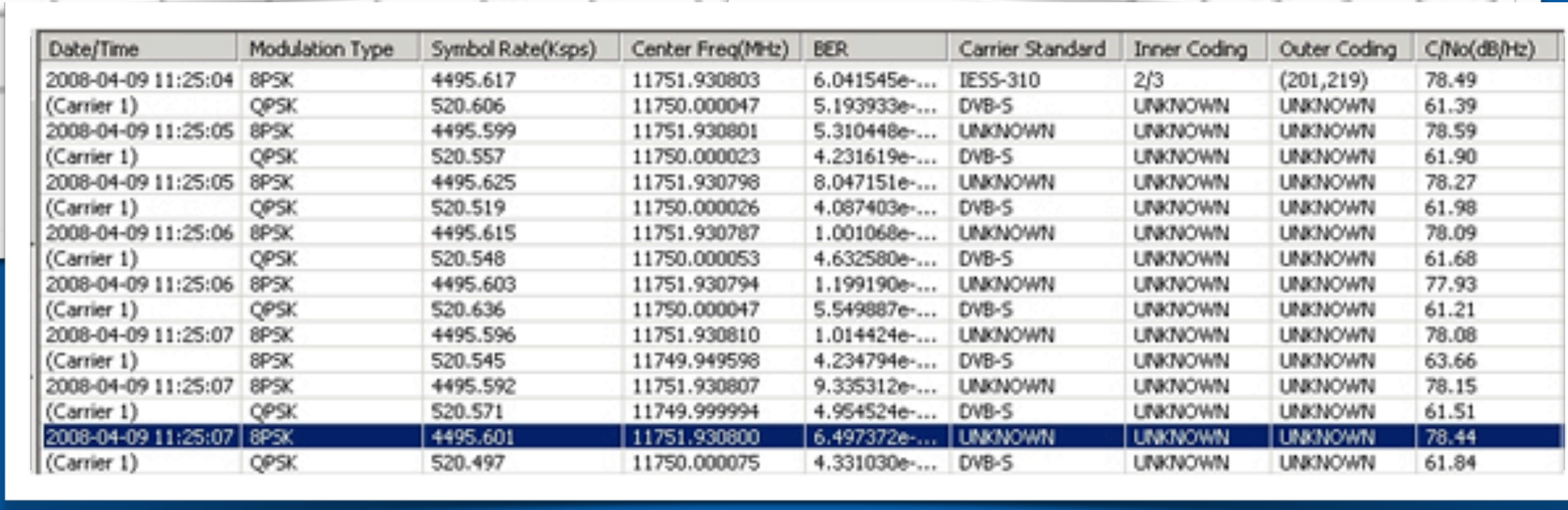
Satellite Carrier Monitoring System

- Spectrum Analyser and Digital Spectrum Processor analysis
- Reference trace and measurement
- Automatic alerts for abnormal and missing carriers

Shared Data



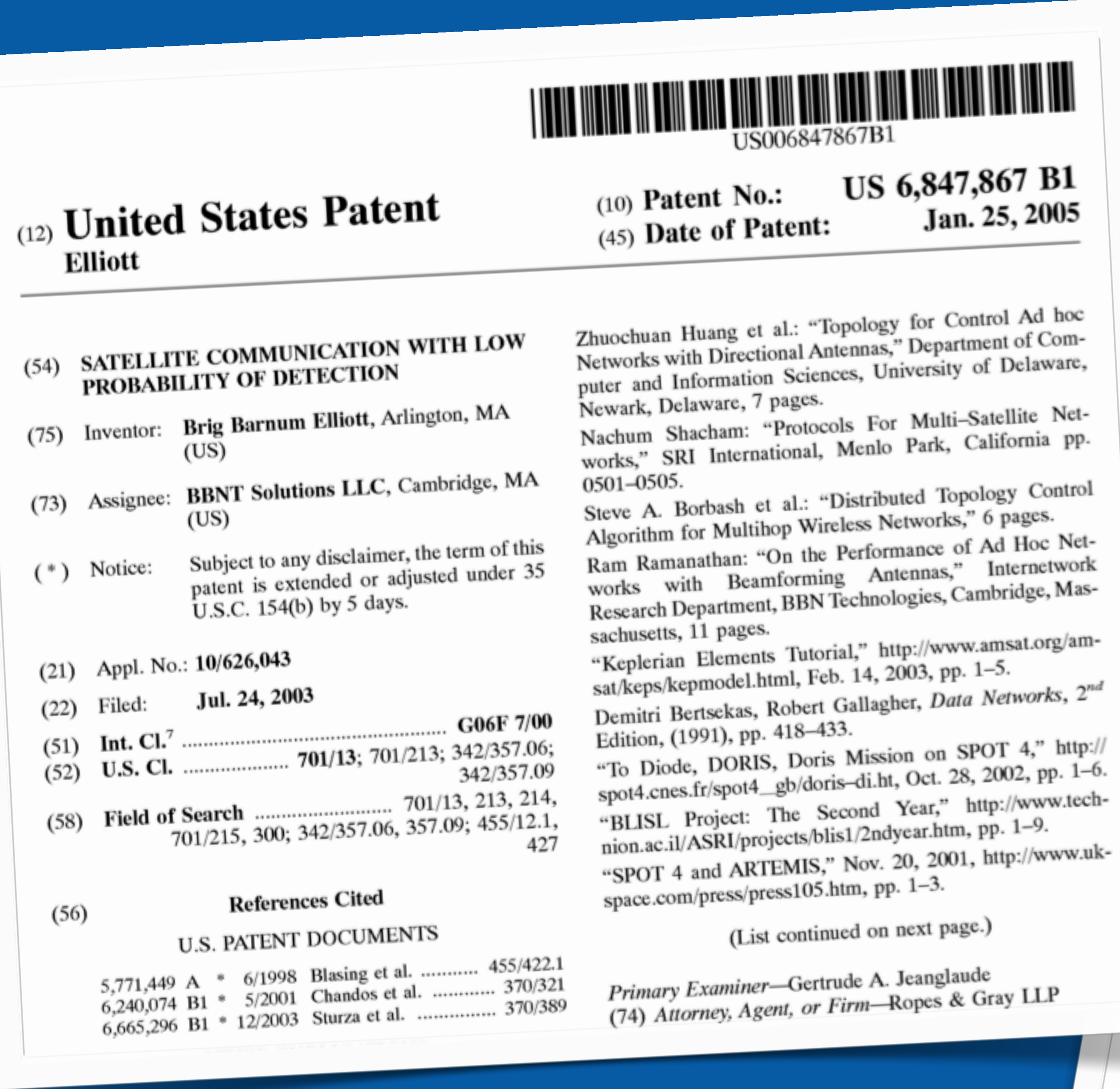




Date/Time	Modulation Type	Symbol Rate(Ksps)	Center Freq(MHz)	BER	Carrier Standard	Inner Coding	Outer Coding	C/No(dB/Hz)
2008-04-09 11:25:04	8PSK	4495.617	11751.930803	6.041545e-...	IESS-310	2/3	(201,219)	78.49
(Carrier 1)	QPSK	520.606	11750.000047	5.193933e-...	DVB-S	UNKNOWN	UNKNOWN	61.39
2008-04-09 11:25:05	8PSK	4495.599	11751.930801	5.310448e-...	UNKNOWN	UNKNOWN	UNKNOWN	78.59
(Carrier 1)	QPSK	520.557	11750.000023	4.231619e-...	DVB-S	UNKNOWN	UNKNOWN	61.90
2008-04-09 11:25:05	8PSK	4495.625	11751.930798	8.047151e-...	UNKNOWN	UNKNOWN	UNKNOWN	78.27
(Carrier 1)	QPSK	520.519	11750.000026	4.087403e-...	DVB-S	UNKNOWN	UNKNOWN	61.98
2008-04-09 11:25:06	8PSK	4495.615	11751.930787	1.001068e-...	UNKNOWN	UNKNOWN	UNKNOWN	78.09
(Carrier 1)	QPSK	520.548	11750.000053	4.632580e-...	DVB-S	UNKNOWN	UNKNOWN	61.68
2008-04-09 11:25:06	8PSK	4495.603	11751.930794	1.199190e-...	UNKNOWN	UNKNOWN	UNKNOWN	77.93
(Carrier 1)	QPSK	520.636	11750.000047	5.549887e-...	DVB-S	UNKNOWN	UNKNOWN	61.21
2008-04-09 11:25:07	8PSK	4495.596	11751.930810	1.014424e-...	UNKNOWN	UNKNOWN	UNKNOWN	78.08
(Carrier 1)	8PSK	520.545	11749.949598	4.234794e-...	DVB-S	UNKNOWN	UNKNOWN	63.66
2008-04-09 11:25:07	8PSK	4495.592	11751.930807	9.335312e-...	UNKNOWN	UNKNOWN	UNKNOWN	78.15
(Carrier 1)	QPSK	520.571	11749.999994	4.954524e-...	DVB-S	UNKNOWN	UNKNOWN	61.51
2008-04-09 11:25:07	8PSK	4495.601	11751.930800	6.497372e-...	UNKNOWN	UNKNOWN	UNKNOWN	78.44
(Carrier 1)	QPSK	520.497	11750.000075	4.331030e-...	DVB-S	UNKNOWN	UNKNOWN	61.84

What’s Next?

No, the journey doesn't end here.



US006847867B1

(12) **United States Patent**
Elliott

(10) **Patent No.:** **US 6,847,867 B1**
(45) **Date of Patent:** **Jan. 25, 2005**

(54) **SATELLITE COMMUNICATION WITH LOW PROBABILITY OF DETECTION**

(75) Inventor: **Brig Barnum Elliott**, Arlington, MA (US)

(73) Assignee: **BBNT Solutions LLC**, Cambridge, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 5 days.

(21) Appl. No.: **10/626,043**

(22) Filed: **Jul. 24, 2003**

(51) **Int. Cl.**^{7} **G06F 7/00**
(52) **U.S. Cl.** **701/13**; 701/213; 342/357.06; 342/357.09

(58) **Field of Search** 701/13, 213, 214, 701/215, 300; 342/357.06, 357.09; 455/12.1, 427

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,771,449 A	*	6/1998	Blasing et al.	455/422.1
6,240,074 B1	*	5/2001	Chandos et al.	370/321
6,665,296 B1	*	12/2003	Sturza et al.	370/389

Zhuochuan Huang et al.: "Topology for Control Ad hoc Networks with Directional Antennas," Department of Computer and Information Sciences, University of Delaware, Newark, Delaware, 7 pages.

Nachum Shacham: "Protocols For Multi–Satellite Networks," SRI International, Menlo Park, California pp. 0501–0505.

Steve A. Borbash et al.: "Distributed Topology Control Algorithm for Multihop Wireless Networks," 6 pages.

Ram Ramanathan: "On the Performance of Ad Hoc Networks with Beamforming Antennas," Internetwork Research Department, BBN Technologies, Cambridge, Massachusetts, 11 pages.

"Keplerian Elements Tutorial," http://www.amsat.org/amsat/keps/kepmodel.html, Feb. 14, 2003, pp. 1–5.

Demitri Bertsekas, Robert Gallagher, *Data Networks*, 2nd Edition, (1991), pp. 418–433.

"To Diode, DORIS, Doris Mission on SPOT 4," http://spot4.cnes.fr/spot4_gb/doris–di.ht, Oct. 28, 2002, pp. 1–6.

"BLISL Project: The Second Year," http://www.technion.ac.il/ASRI/projects/blis1/2ndyear.htm, pp. 1–9.

"SPOT 4 and ARTEMIS," Nov. 20, 2001, http://www.uk-space.com/press/press105.htm, pp. 1–3.

(List continued on next page.)

Primary Examiner—Gertrude A. Jeanglaude
(74) *Attorney, Agent, or Firm*—Ropes & Gray LLP

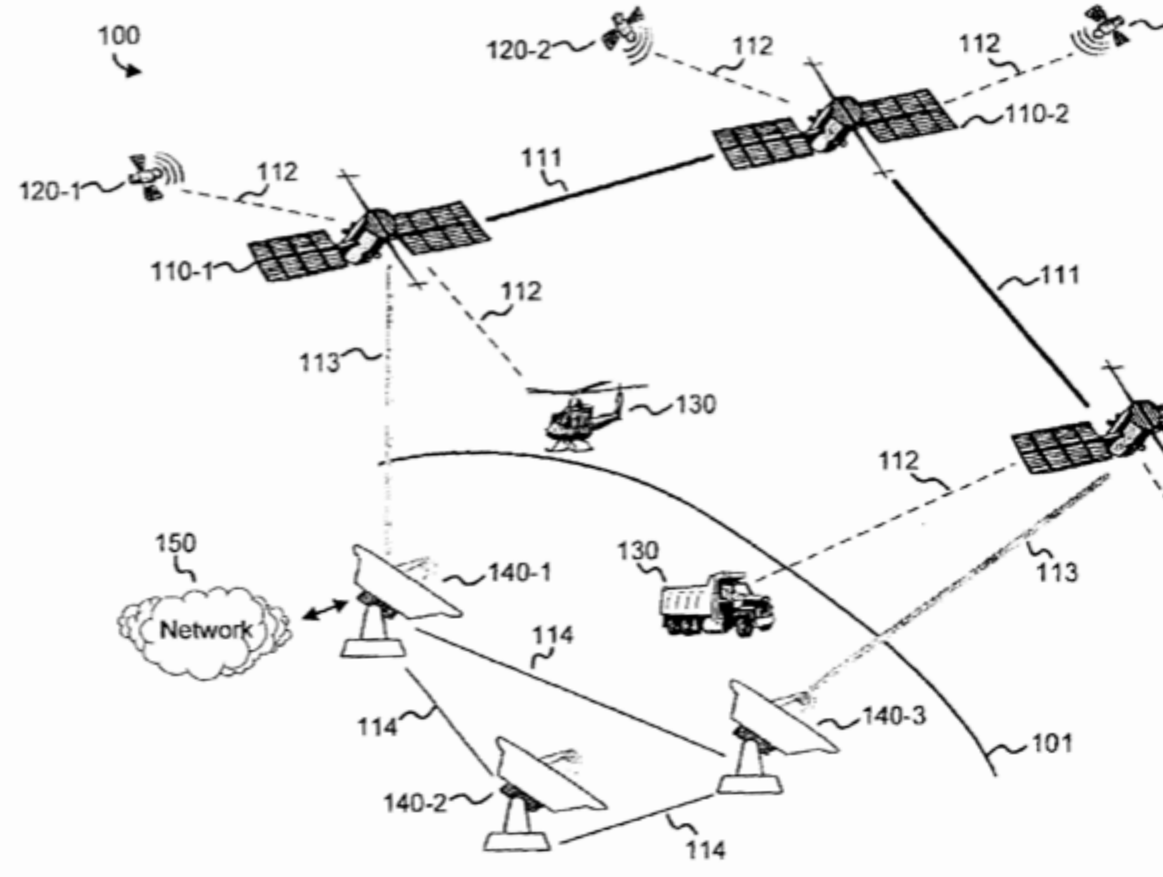


Fig. 1

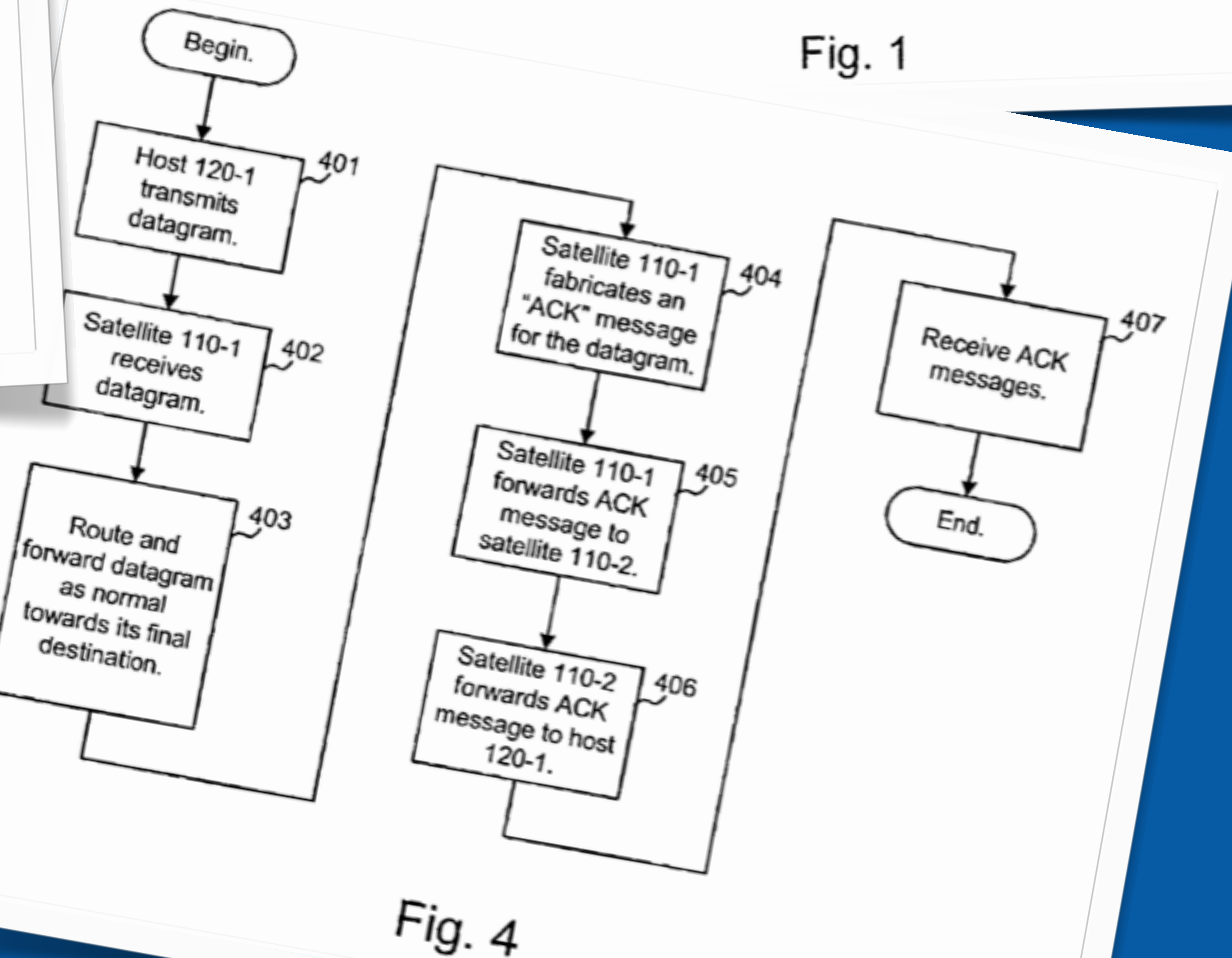
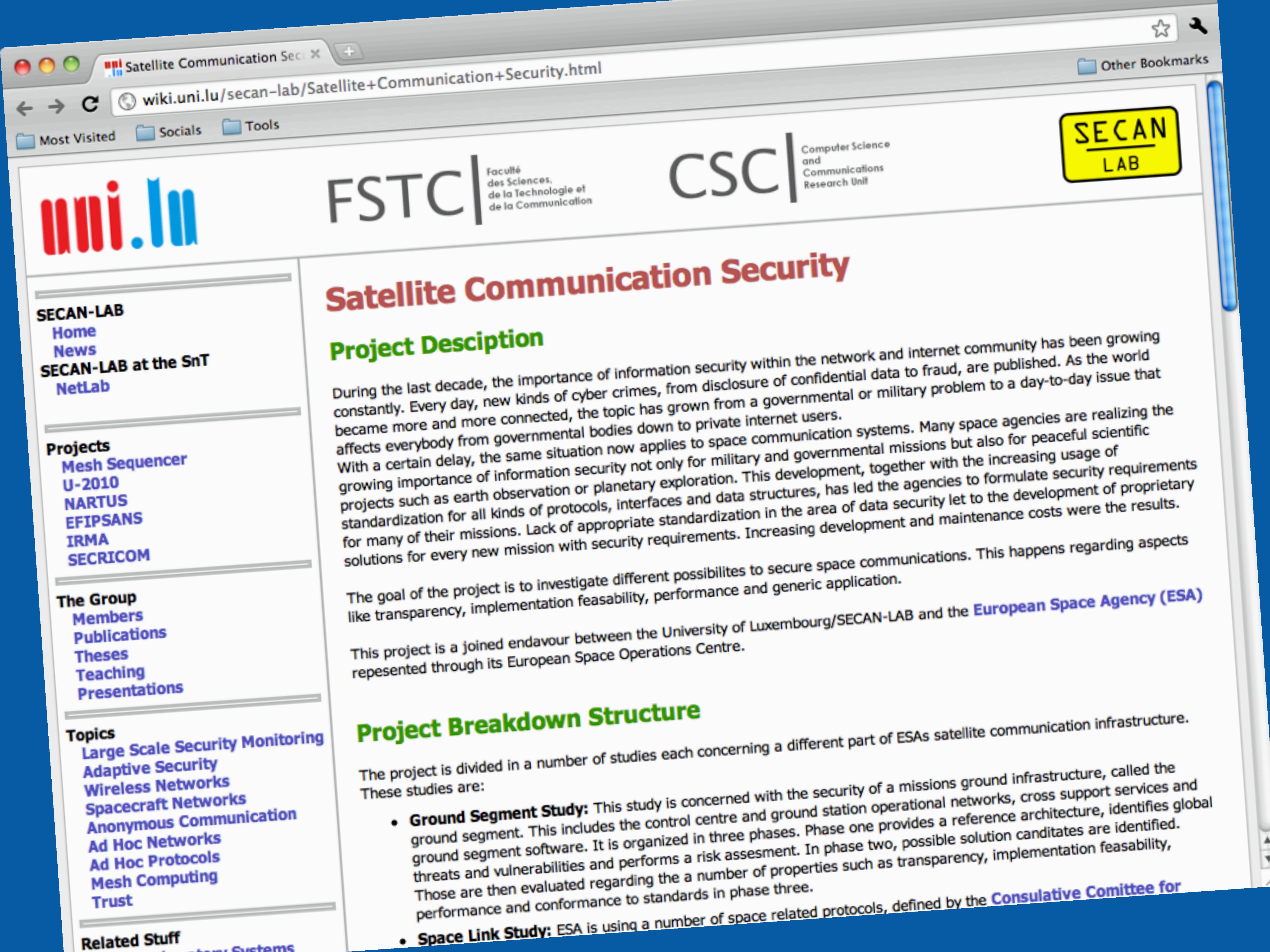

Begin.
Host 120-1 transmits datagram.
401
Satellite 110-1 receives datagram.
402
Route and forward datagram as normal towards its final destination.
403
Satellite 110-1 fabricates an "ACK" message for the datagram.
404
Satellite 110-1 forwards ACK message to satellite 110-2.
405
Satellite 110-2 forwards ACK message to host 120-1.
406
Receive ACK messages.
407
End.

Fig. 4



Satellite Communication Security

Project Description

During the last decade, the importance of information security within the network and internet community has been growing constantly. Every day, new kinds of cyber crimes, from disclosure of confidential data to fraud, are published. As the world became more and more connected, the topic has grown from a governmental or military problem to a day-to-day issue that affects everybody from governmental bodies down to private internet users.
With a certain delay, the same situation now applies to space communication systems. Many space agencies are realizing the growing importance of information security not only for military and governmental missions but also for peaceful scientific projects such as earth observation or planetary exploration. This development, together with the increasing usage of standardization for all kinds of protocols, interfaces and data structures, has led the agencies to formulate security requirements for many of their missions. Lack of appropriate standardization in the area of data security let to the development of proprietary solutions for every new mission with security requirements. Increasing development and maintenance costs were the results.

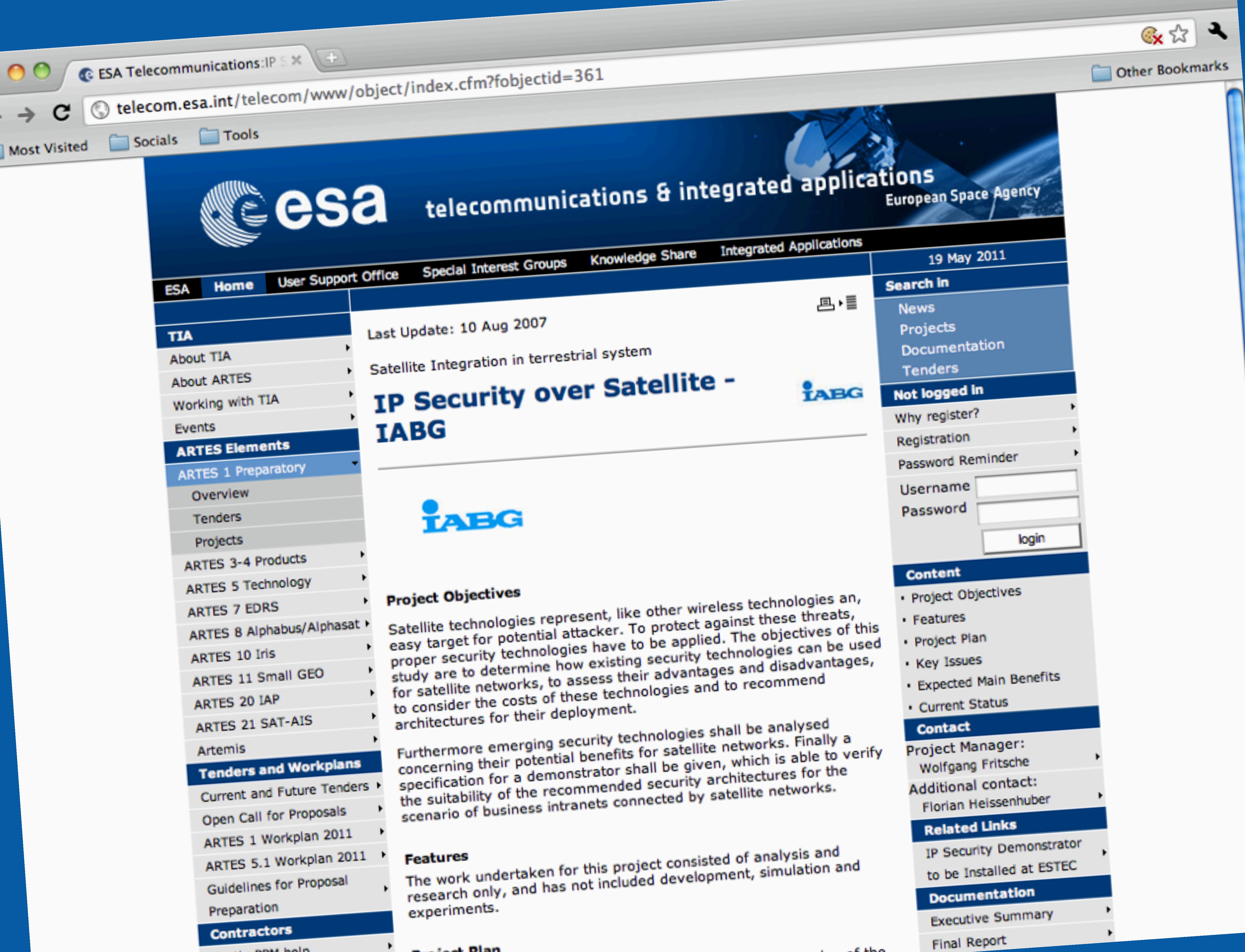
The goal of the project is to investigate different possibilites to secure space communications. This happens regarding aspects like transparency, implementation feasability, performance and generic application.

This project is a joined endavour between the University of Luxembourg/SECAN-LAB and the European Space Agency (ESA) repesented through its European Space Operations Centre.

Project Breakdown Structure

The project is divided in a number of studies each concerning a different part of ESAs satellite communication infrastructure. These studies are:

- **Ground Segment Study:** This study is concerned with the security of a missions ground infrastructure, called the ground segment. This includes the control centre and ground station operational networks, cross support services and ground segment software. It is organized in three phases. Phase one provides a reference architecture, identifies global threats and vulnerabilities and performs a risk assesment. In phase two, possible solution canditates are identified. Those are then evaluated regarding the a number of properties such as transparency, implementation feasability, performance and conformance to standards in phase three.
- **Space Link Study:** ESA is using a number of space related protocols, defined by the Consulative Comittee for



Project Manager:
Wolfgang Fritsche

Additional contact:
Florian Heissenhuber

Last Update: 10 Aug 2007

Satellite Integration in terrestrial system

IP Security over Satellite - IABG

Project Objectives

Satellite technologies represent, like other wireless technologies an, easy target for potential attacker. To protect against these threats, proper security technologies have to be applied. The objectives of this study are to determine how existing security technologies can be used for satellite networks, to assess their advantages and disadvantages, to consider the costs of these technologies and to recommend architectures for their deployment.

Furthermore emerging security technologies shall be analysed concerning their potential benefits for satellite networks. Finally a specification for a demonstrator shall be given, which is able to verify the suitability of the recommended security architectures for the scenario of business intranets connected by satellite networks.

Features

The work undertaken for this project consisted of analysis and research only, and has not included development, simulation and experiments.

Project Plan

HF-Satcom.com – The #1

www.uhf-satcom.com

Socials Tools Other Bookmarks

UHF-Satcom.com

Monitoring VHF to EHF since Y2K!

*** #Hearsat IRC chat ***
Satcom Sound Samples

*** SATCOM F.A.Q.***
*** WANTED! ***
UHF reception
L-Band reception
S-Band reception
C-Band reception
X-Band reception
Ku-Band reception
Ka-Band reception
Technical info pages
DSN tracking spreadsheet
Amateur DSN group
X-band DSN
Gonets
Sicral
Meridian / Molniya

Inma

What would you like

* IMPORTANT * U
* NEW * Get WXT
* NEW * Support th
* RIP * Remember

28/04/2011 - Surpl
01/04/2011 - UHF
24/02/2011 - The
01/01/2011 - Meri
02/11/2010 - New
07/08/2010 - The
23/05/2010 - Pla
04/03/2010 - Bri
13/11/2009 - ES
13/08/2009 - A

HITBSecConf2011 – Amsterd | Hacker News | Low Earth Or | SatBeams – Home

www.satbeams.com

Most Visited Socials Tools

SATBEAMS

Username Password

You are here: Home

Home | Satellites | Footprints | Charts | Packages | Download

News

Transponder news 18-May-11
Transponder news 17-May-11
Transponder news 15-16-May-11
Transponder news 13-14-May-11
Transponder news 12-May-11

Advertising

Features Include:
Field-replaceable F-connectors
Calibrated signal level (dBm, dBmV, or dBµV)
Holds all satellites and transponders per global region

Media Partner

http://www.dunnspace.com/leo_on_the_cheap.htm

LEO ON THE CHEAP

Methods for Achieving Drastic Reductions in Space Launch Costs

Lt Col John R. London III

Fin.

Jim Geovedi <jim@geovedi.com>, @geovedi
Raoul Chiesa <raoul.chiesa@mediaservice.net>