August 2025

ddunn@cape.co
whallisey@cape.co

Cape is America's privacy-first mobile carrier. We are a software defined telecom offering premium cellular connectivity while protecting our customer's sensitive and personal information.

We are a venture-backed team with multiple successful startup exits and decades of deep tech and telco experience, deploying cutting edge IP to offer privacy, security, and resilience-focused communications over commercial cellular networks.

Cape

The Problem & Solution

The most powerful network on Earth is more important than ever and dangerously vulnerable

SEPTEMBER 2023

COMPANY T-MOBILE
USERS 100
USER TYPE CUSTOMER
BREACH ORIGIN T-MOBILE SYSTEMS
SEVERITY OF INFO PII

DECEMBER 2023

COMPANY MINT MOBILE
(NOW ACQUIRED BY T-MOBILE)
USERS UNKNOWN
USER TYPE CUSTOMER
BREACH ORIGIN MINT MOBILE SYSTEMS
SEVERITY OF INFO PII

FEBRUARY 2024

COMPANY VERIZON
USERS 63,000
USER TYPE EMPLOYEES
BREACH ORIGIN VERIZON SYSTEMS
SEVERITY OF INFO HIGHLY SENSITIVE PII

MARCH 2024

COMPANY AT&T
USERS 73,000,000
USER TYPE CUSTOMER
BREACH ORIGIN UNDISCLOSED 3RD PARTY VENDORS
SEVERITY OF INFO HIGHLY SENSITIVE PII

JULY 2024

COMPANY AT&T
USERS 109M
USER TYPE CUSTOMER
BREACH ORIGIN THIRD PARTY
SEVERITY OF INFO CONSUMER COMMUNICATION RECORDS

OCTOBER 2024

COMPANY AT&T, VERIZON, LUMIN
USERS IMPACTED UNKNOWN
USER TYPE UNKNOWN
BREACH ORIGIN SPECULATED TO BE SALT TYPHOON, A CHINESE FOREIGN SPY SERVICE
SEVERITY OF INFO NATIONAL SECURITY

OCTOBER 2024

COMPANY VERIZON
USERS IMPACTED UNKNOWN
USER TYPE VERIZON'S PTT CUSTOMERS
BREACH ORIGIN SHACKERS CYBERPHANTOM AND JUDISCHE
SEVERITY OF INFO CALL LOGS AND PII

American Phone-Tracking Firm Demonstrates Surveillance Powers by Spying on CIA and NSA

SIM swapping: the simple way that hackers took over the SEC's X Account

Experts say SIM swap attacks will continue happening until mobile phone carriers change how they operate—or are forced to do so with stronger rules and regulations.

T-Mobile announces another data breach, impacting 37 million accounts / The attacker obtained customer names, billing addresses, emails, phone numbers, and birth dates through an internal API.

Data of nearly all AT&T customers downloaded from a third-party platform in security breach

SPY BALLOON

Chinese spy balloon carried 'multiple antennas' for collecting signals intelligence, State Dept. says

Photos by U-2 planes confirmed the presence of the equipment, and debris collected so far includes electronics. An official said what's collected is cumulatively the size of a small car.

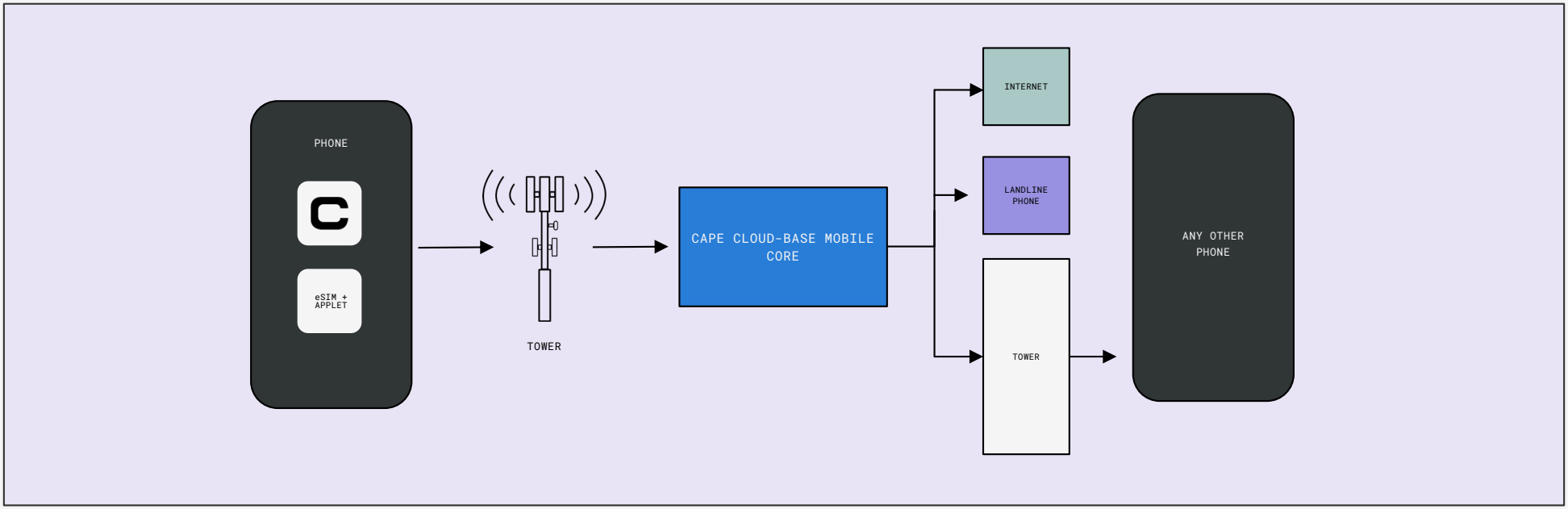
CHINA INFORMATION TECHNOLOGY SECURITY EVALUATION CENTER, MINISTRY OF STATE SECURITY,
PEOPLE'S REPUBLIC OF CHINA

"Telecommunications network operating personnel do not have an accumulation of knowledge about information security.

Their vigilance is not high…

they lack the necessary awareness of the consequences that may result from attacks."

Private, secure, and resilient communications over commercial cellular networks, enabled by our own mobile core and associated software.



Pushing the edge of telecom innovation

Cape Strategic MVNOs

Maximum protection where it's most needed

Direct network access and administration offers unparalleled flexibility, privacy, and security.

Cape Obscura

Encompassing identity obfuscation

Obfuscated network identities in simulated hostage rescue vs close technical surveillance and compromised telco

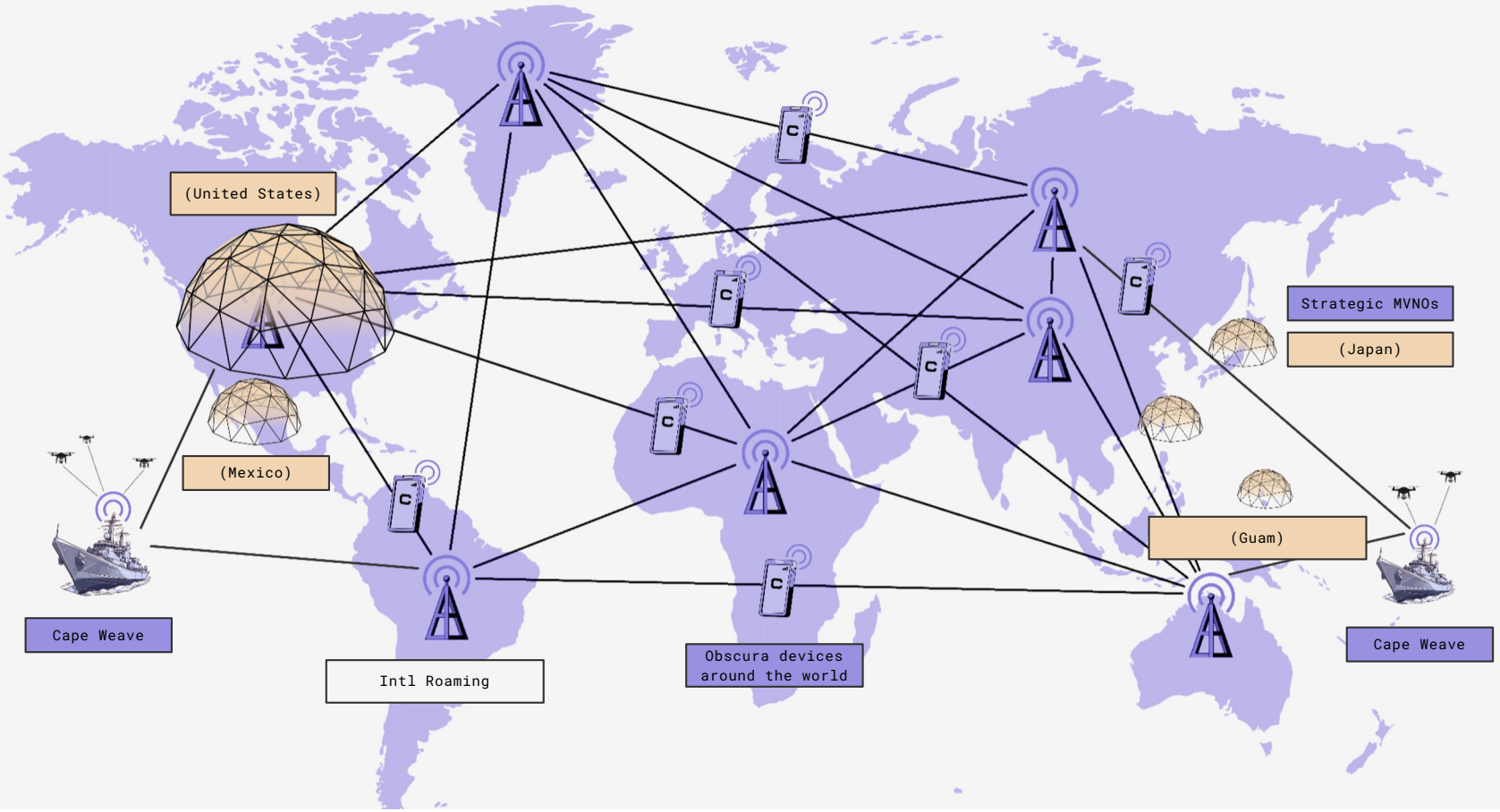
Cape Weave

First seamless Hybrid Network on a single SIM

Proved out what telecom giants failed to deliver for DIU despite millions invested

You can only do this if you're a global telco...which Cape is.

Cape's global connectivity is augmented by strategic MVNO agreements across the world with counterparties in countries including Japan, Mexico, and Guam. Cape is incorporated in Mexico, Japan, and other regions with additional roaming reach via international hub partners.



Cape

Obscura

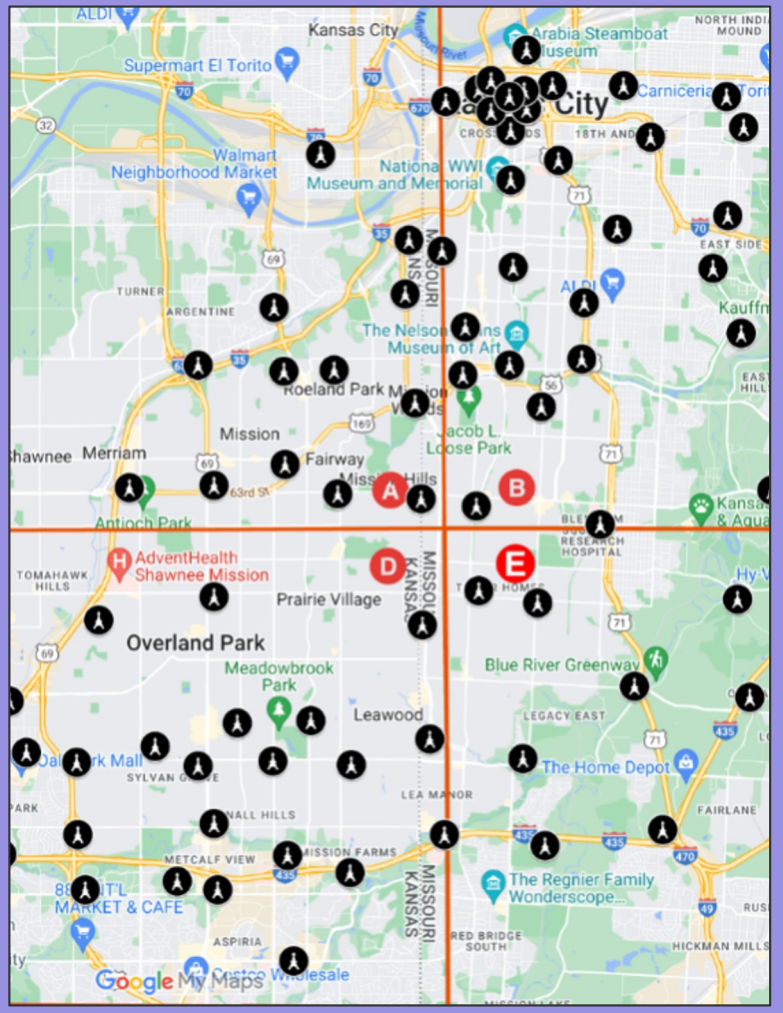
Obfuscation of identity on public networks.

Kansas City Red Team Exercise
(Sept 2023)

Supported a 10 day simulated hostage rescue exercise via our network on partner towers. Red team had technical surveillance gear and insider access to service provider, simulating a compromised telco.

"[Cape] made it nearly impossible for the ground-based technicians to conduct direction finding operations[...] Ultimately, Cape offers a product currently in a class of its own."

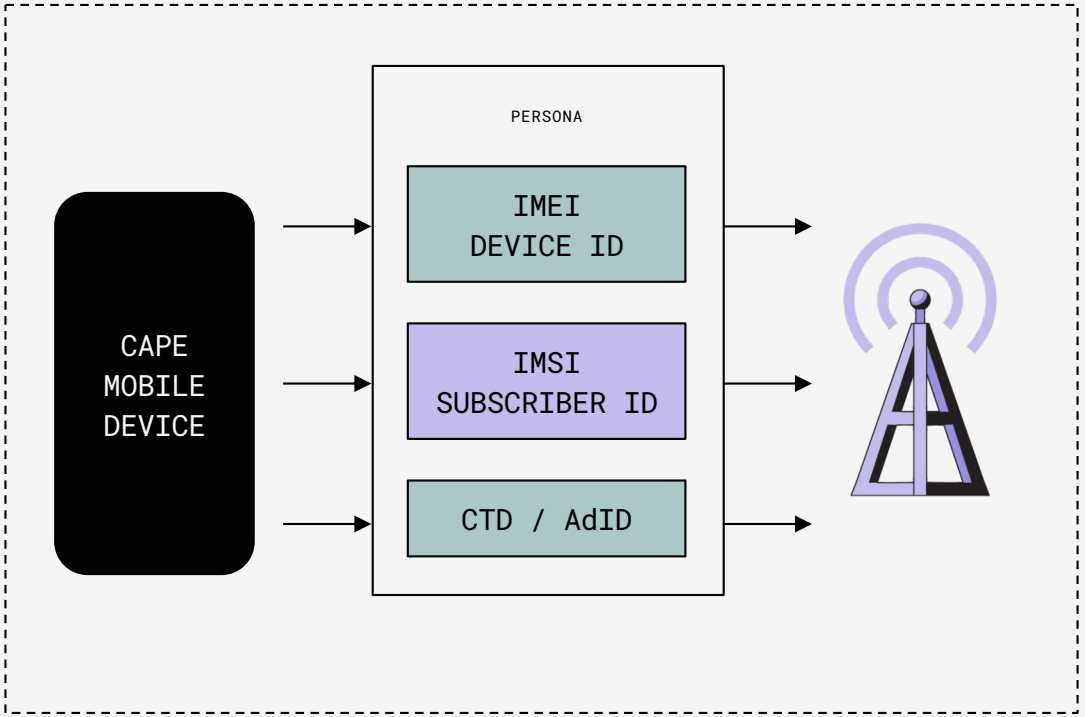
After Action Review of Cape's Kansas City Exercise



Cape

Cape Obscura – Identity Obfuscation & Management

- The root of many vulnerabilities in telco is that the identifiers on our phones are all static and observable.
- Cape decouples the mobile phone from these identifiers by rotating them in bundles via a concept we call “Personas”.
- IMSI, IMEI & AdID on Cape android mobile device.

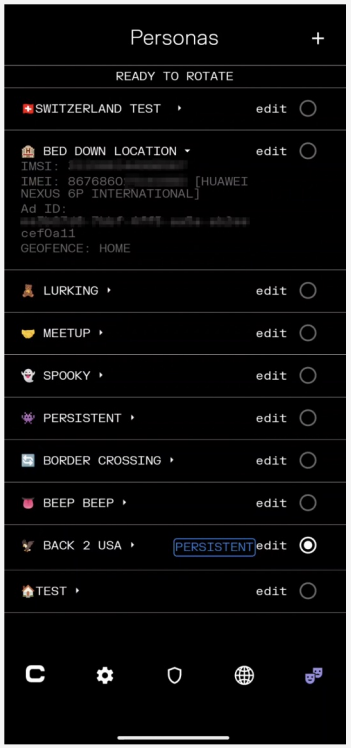


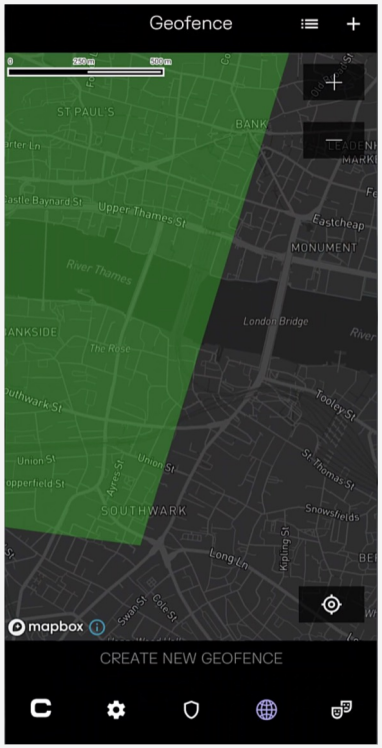
Cape Handsets

Cape addresses this by decoupling devices from those identifiers. We rotate them in grouped sets of properties using a construct we call “Personas.”

This fundamentally shifts the targeting surface. The selectors are no longer fixed—they’re dynamic and extremely difficult to track.

These are flagship devices from a major manufacturer.





Guam MVNO Project

Navy asked us to field and test a secure cellular network OCONUS, running on local towers, to replicate results from the Kansas City trial.

Partnering with regional providers, we set up a Strategic MVNO on Guam. In addition to replicating Kansas City, we trialled secure 4G / 5G connectivity at port and offshore.

We tested in August with USS Abraham Lincoln, offshore connectivity up to 30nm, with similar speeds to satellite, at port connectivity gave high speed data link, transferring 1TB in 24 hours.

US Navy Trying Experimental Tech to Help Secure Guam

- Mobile carrier Cape hired for pilot project to shield network
- Hackers tied to Chinese government accused of targeting Guam

Strategic MVNO

Cloud-based mobile core deployed in any country, improving resilience, mitigating APTs, and supporting expanded use cases.

Guam Strat MVNO Pilot Assessment (March 2025)

Third party evaluator recreated Kansas City results on 2 MNOs integrated into a single network and validated hybrid network interoperability.

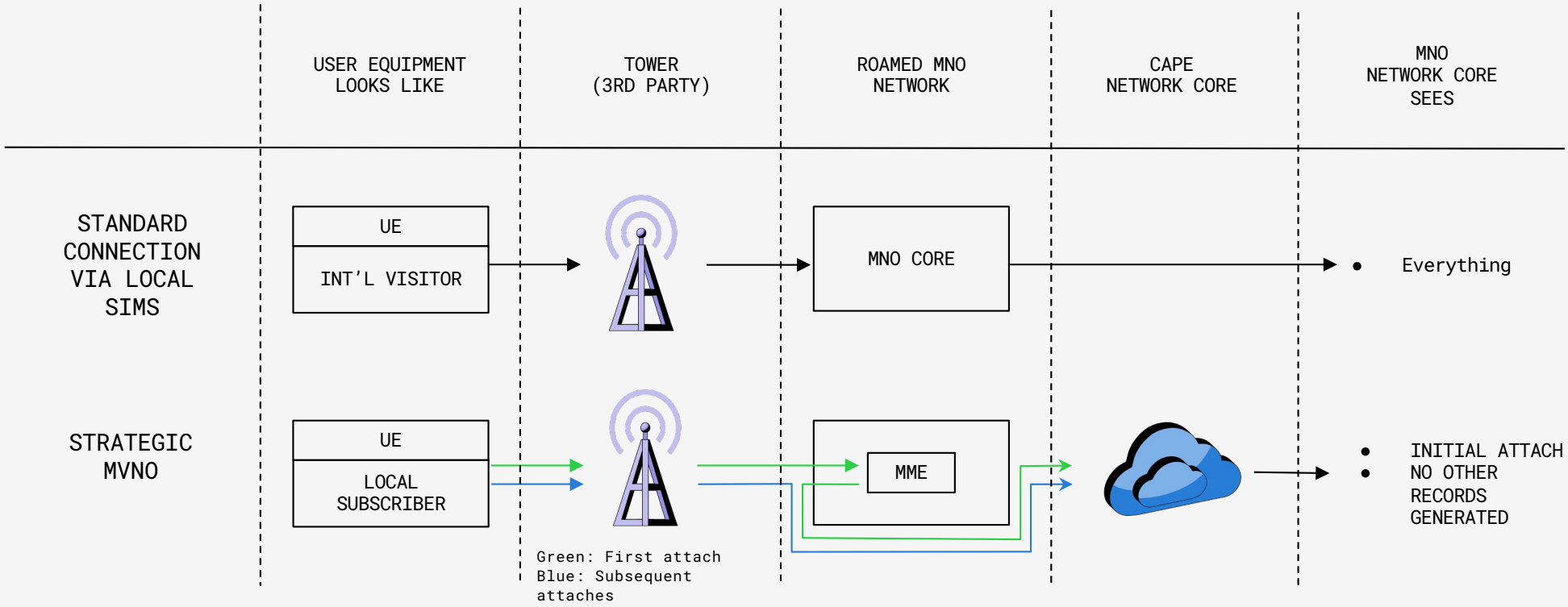
USS Abraham Lincoln Test (Oct 2024)

Provided commercial cellular ship to shore connectivity from a single SIM 130 miles offshore.

"...Cape effectively masks user and session information [from the underlying carrier]"

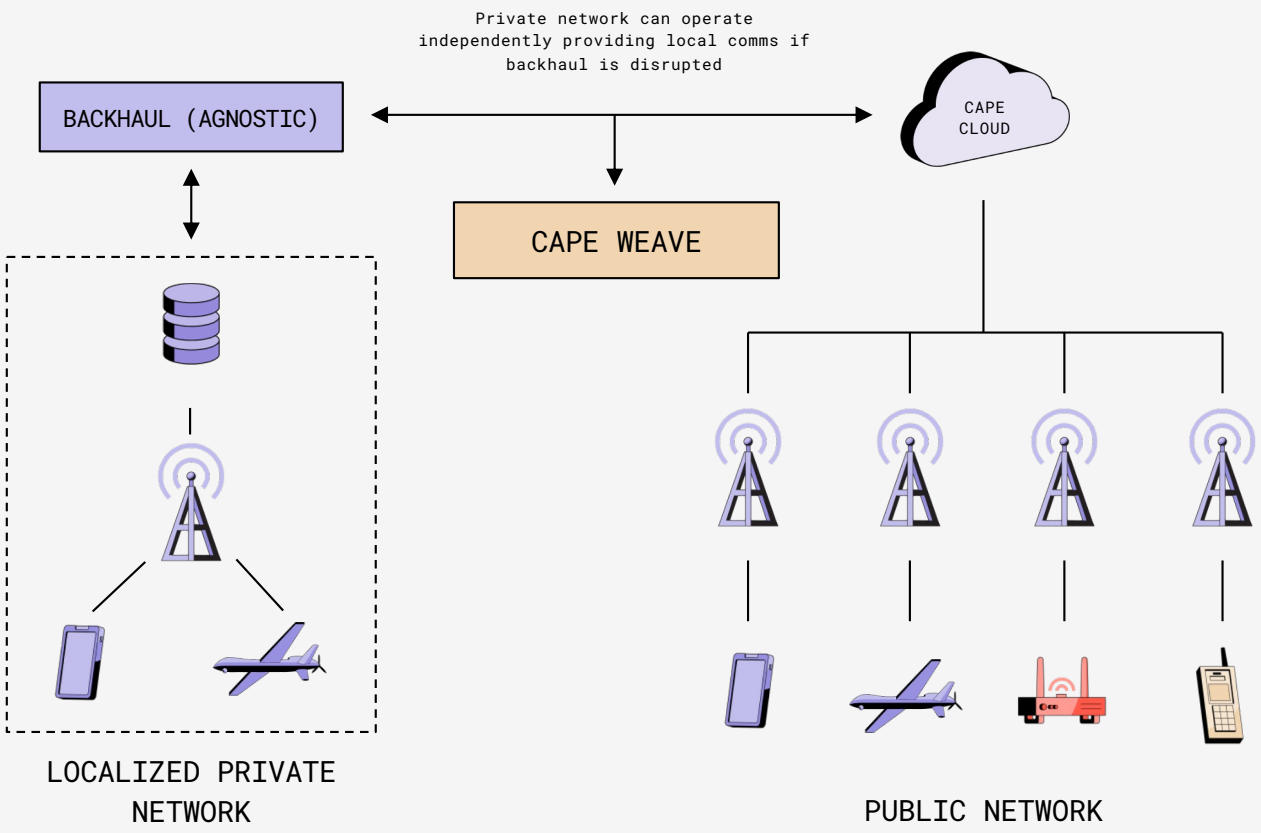
– Third party evaluator, Guam Pilot

Cape



- Ease of use, no special equipment required
- Fast, cost effective, ubiquitous, uses existing assets
- Connectivity to IoT devices via cellular modems
- Able to transmit encrypted tactical data
- Easily extended if required using private 5G network
- Roam seamlessly between public and private networks

Hybrid Networks: Meshing Public & Private Cellular



Capabilities:

Seamlessly roam between localized private & public commercial networks with managed and synced credentials

Extend coverage as needed by deploying additional RAN as needed

Federation of subscribers and integration with government networks

Advantages:

Leverage existing commercial infrastructure where possible

Isolate tactical assets from commercial infrastructure as required

Enable connectivity for a wide variety of IoT devices

Discussion

CONTACTS
ddunn@cape.co
whallisey@cape.co

SECTION 04

Appendix

Case Study: Operation Spider Web – Ukraine

BLUF: In June 2025, Ukraine conducted Operation Spider Web deep in Russian territory. The SBU used small, inexpensive drones equipped with cellular SIM cards to destroy over a third of Russia's strategic bomber fleet. **Operators relied on improvised C2 using open-source software running on Russian mobile cellular networks.**

WHAT: Cellular networks provided a low-profile data channel, **blending in with normal civilian traffic and avoiding detection by Russian electronic warfare systems.**

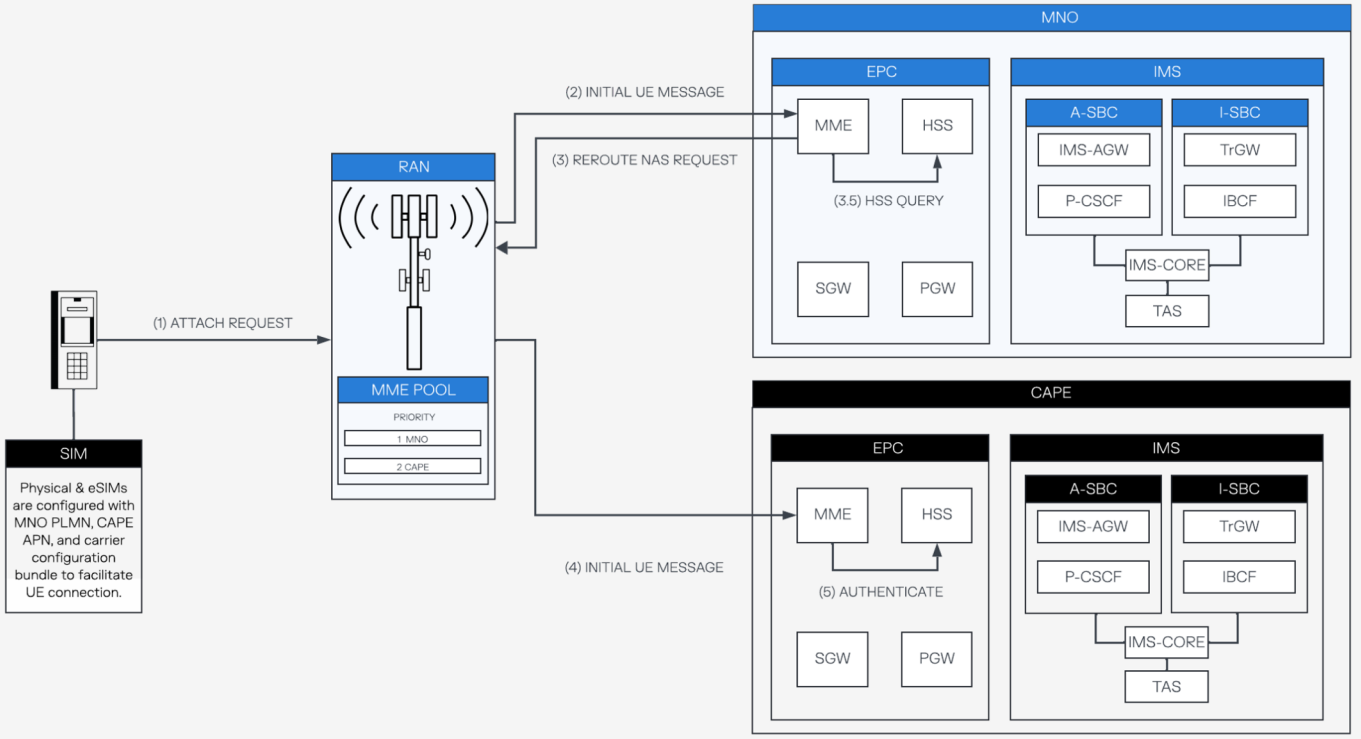
HOW: **By using local mobile networks, Ukrainian operators avoided cross-border RF transmissions, reducing traceability and attribution risk.** Russian air defenses typically look for high-power, long-range comms or GPS spoofing/jamming—**these drones avoided both by behaving like ordinary IoT devices or smartphones.**

WHY: **Ukraine's success relied on the ability to coordinate unmanned systems at scale using Russian commercial cellular networks.** The drones used in the operation were equipped with SIM cards that allowed them to connect to local Russian mobile networks, enabling beyond-line-of-sight (BLOS) C2 w/out relying on vulnerable satellite or long-range radio links.

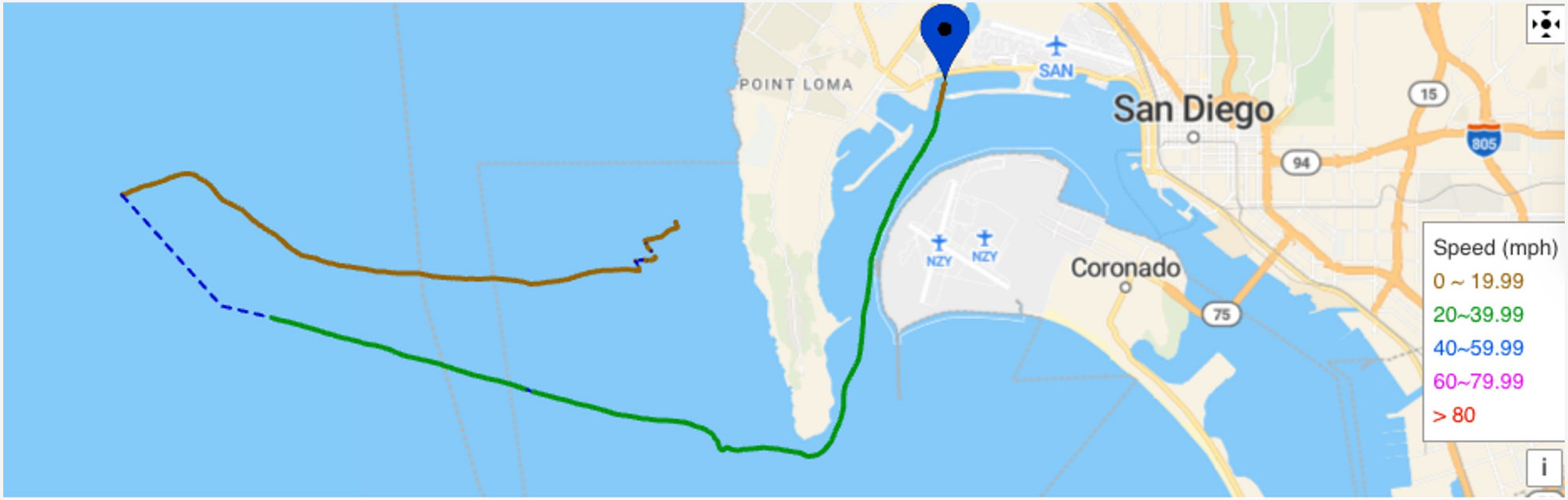
SO WHAT: The operation revealed the need for low-latency, multi-path comms that can survive degraded infrastructure, GPS denial, and network latency—especially when operating distributed unmanned assets. **Cape's DECOR network would enable obfuscated high-throughput, low latency tactical C2 of unmanned systems via Cape's global cellular network**

DECOR Architecture: Looking Local by Being Local and Operating Through Host-Nation Commercial Infrastructure

Primary approach is connectivity using local cell network, routing over local RAN, and using DECOR to route all network traffic to Cape cloud core



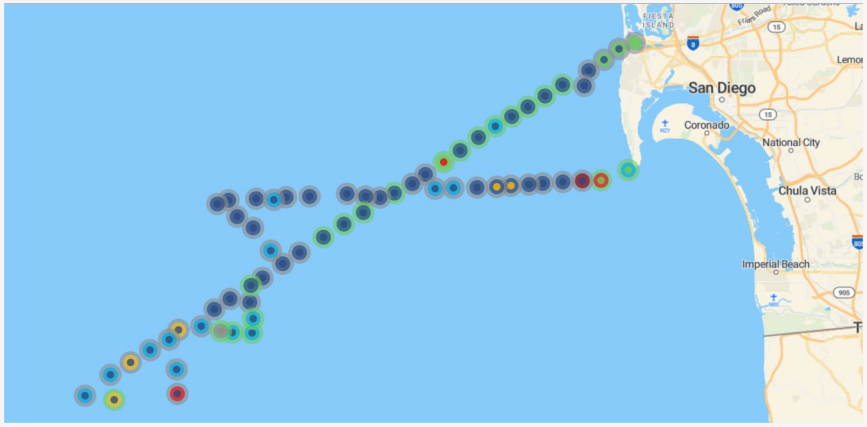
Achieved 5G connectivity up to 8 miles offshore



FILE: Attachment B_Peplink_gps_loc_2024-11-22.GPX

Offshore Public Cellular Range Testing

- Connection to public cellular networks lost at approximately ~37 standard miles offshore
- Antennas were affixed to the offshore vessel at approximately eight feet above sea level



Aft facing MIMO antenna connectivity map

Time	Strength	Quality	Latency	Cell ID	Carrier	Band
2024-12-18 18:26:02	-100 dBm (Good)	8 dB (Very good)	73 ms (≤ 500 ms)	7575	AT&T (US)	LTE Band 30 (2300 MHz)
2024-12-18 18:25:52	-99 dBm (Good)	8 dB (Very good)	118 ms (≤ 500 ms)	7575	AT&T (US)	LTE Band 30 (2300 MHz)
2024-12-18 18:25:42	-99 dBm (Good)	8 dB (Very good)	68 ms (≤ 500 ms)	7575	AT&T (US)	LTE Band 30 (2300 MHz)
2024-12-18 18:25:32	-101 dBm (Good)	8 dB (Very good)	76 ms (≤ 500 ms)	7575	AT&T (US)	LTE Band 30 (2300 MHz)
2024-12-18 18:25:22	-103 dBm (Fair)	7 dB (Very good)	67 ms (≤ 500 ms)	14231	AT&T (US)	LTE Band 30 (2300 MHz)

Connection Metrics at 36.36 standard miles from shore