THE CITIZEN LAB

Mobile Surveillance Monitor

NEW TRICKS AND OLD NETWORKS

Monitoring Repression Activity In Centralized Telecom Networks

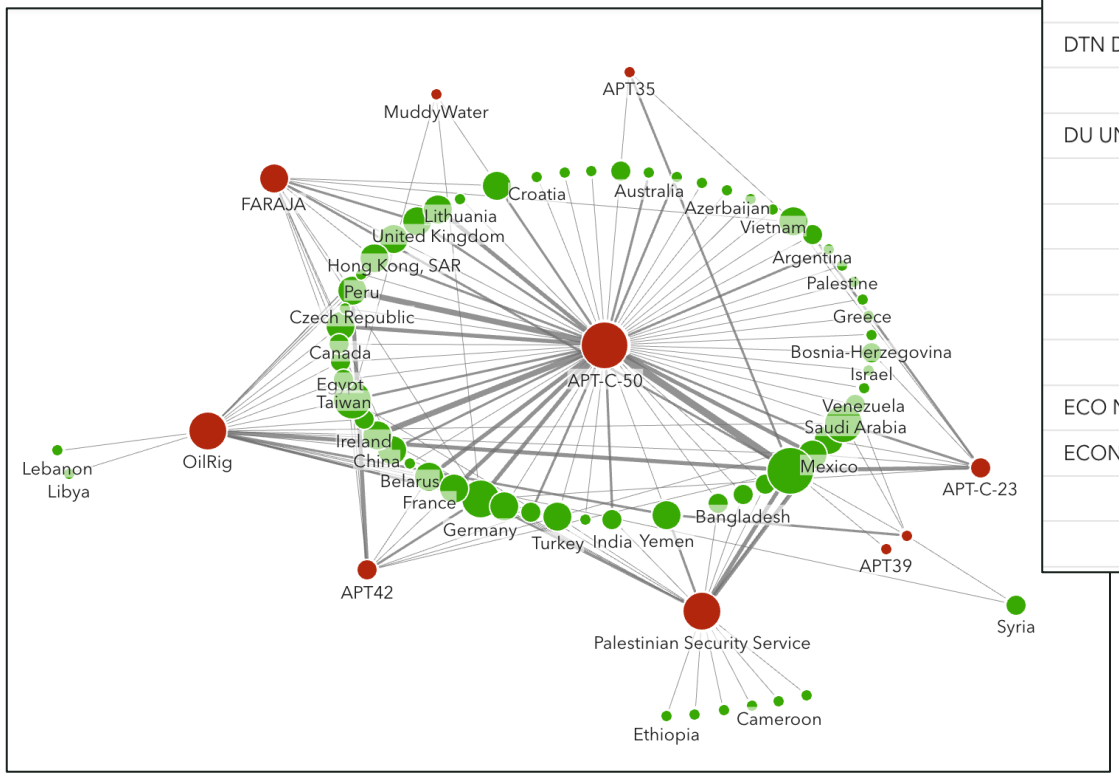
Splintercon Montreal 2023

Surveillance Data Sources – Mobile Surveillance Monitor

Spyware and Mobile Network Telemetry Data for Threat Intelligence and Investigating Adversaries

- **Device Malware** – 2 Million Attacks from 100 Threat Groups
- **Network Attacks** – 15 Million Targeted Attacks from over 200 Networks

Cellusys® VIRUSTOTAL Lookout™

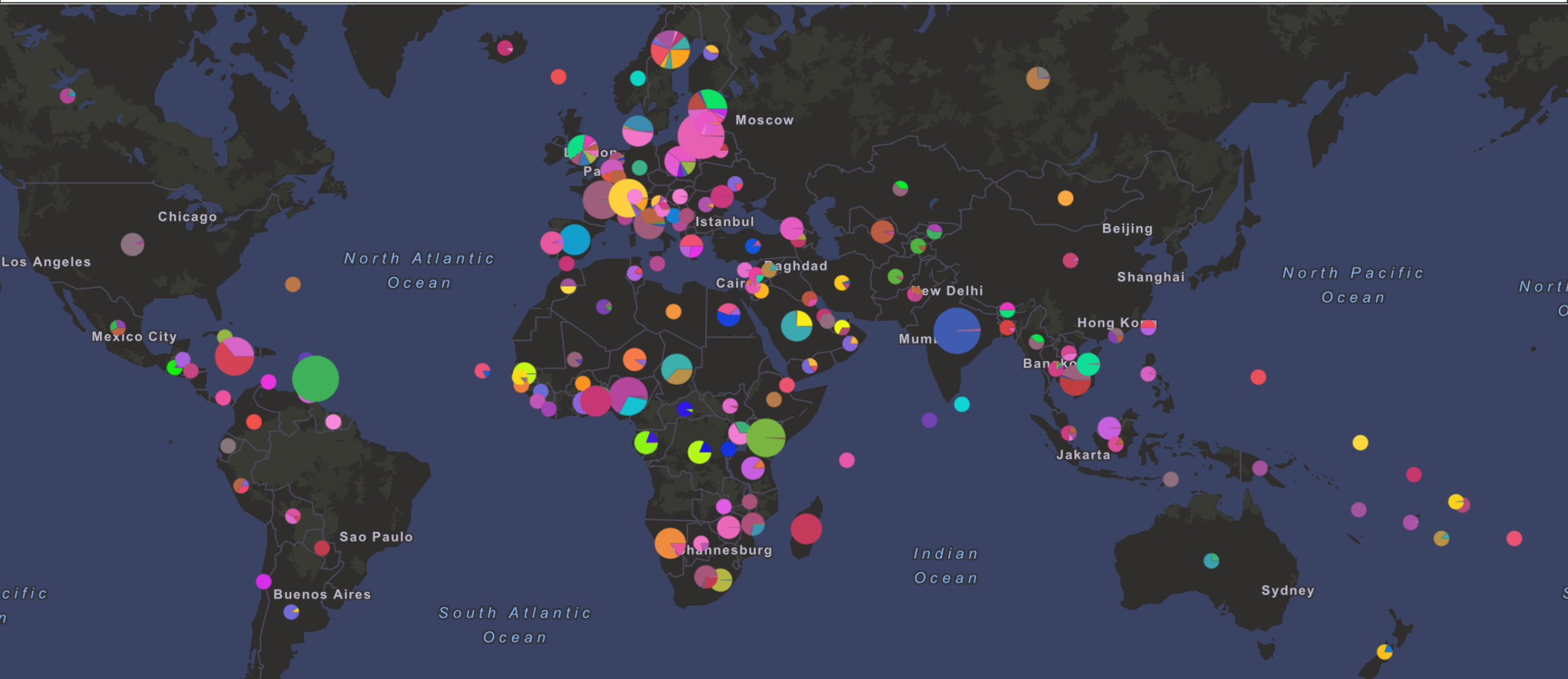


Source Network	Source Node	Threat Type	Operation	Network
DOCOMO PACIFIC	mme01.epc.mnc370.mcc310.3gp…	Communications Intercept	Authentication-Information-…	4G
		Location Discovery	Insert-Subscriber-Data-Requ…	4G
DTN DTAC NETWORK COMPANY	mme01.epc.mnc005.mcc520.3gp…	Communications Intercept	Authentication-Information-…	4G
		Location Discovery	Insert-Subscriber-Data-Requ…	4G
DU UNITED ARAB EMIRATES	971555515518		provideSubscriberInfo	3G
	971555515519			3G
	hss01.epc.mnc003.mcc424.3gppn…		Insert-Subscriber-Data-Requ…	4G
	hss1.epc.mnc003.mcc424.3gppne…			4G
	mme01.epc.mnc003.mcc424.3gp…	Communications Intercept	Authentication-Information-…	4G
		Location Discovery	Insert-Subscriber-Data-Requ…	4G
ECO NETWORKS	79560000100		sendRoutingInfo	3G
ECONET EZI-CEL	2666000010	Denial of Service	processUnstructuredSS-Data	3G
			processUnstructuredSS-Req…	3G
	hss.epc.mnc002.mcc651.3gppnet…	Location Discovery	Insert-Subscriber-Data-Requ…	4G

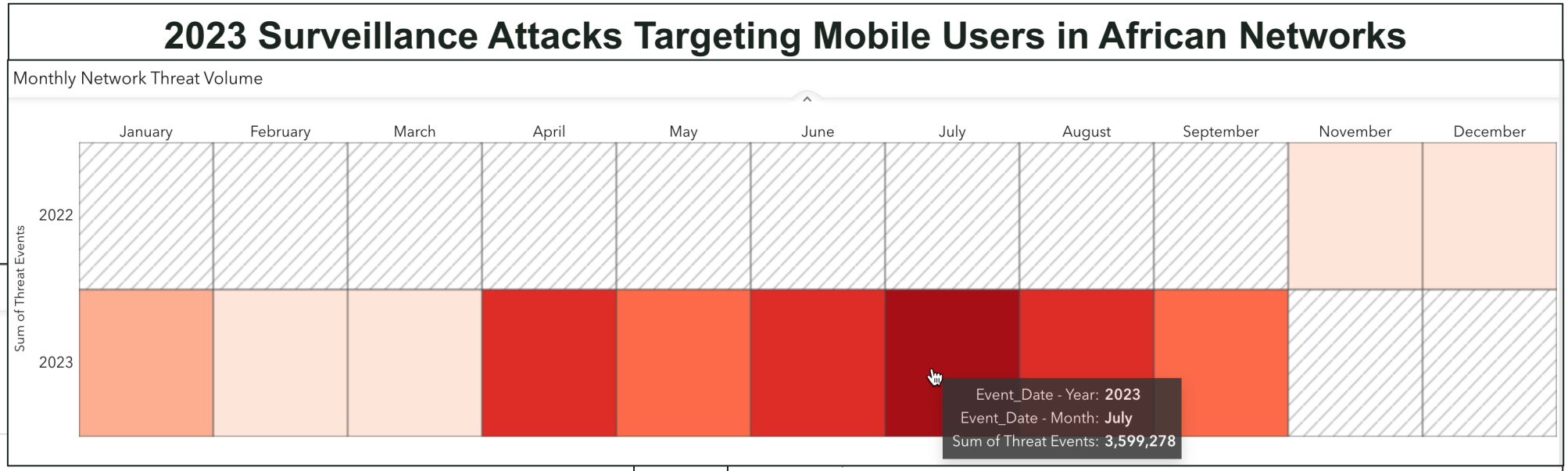
Operators are shutting down 3G service. Aren't mobile network attacks old news?

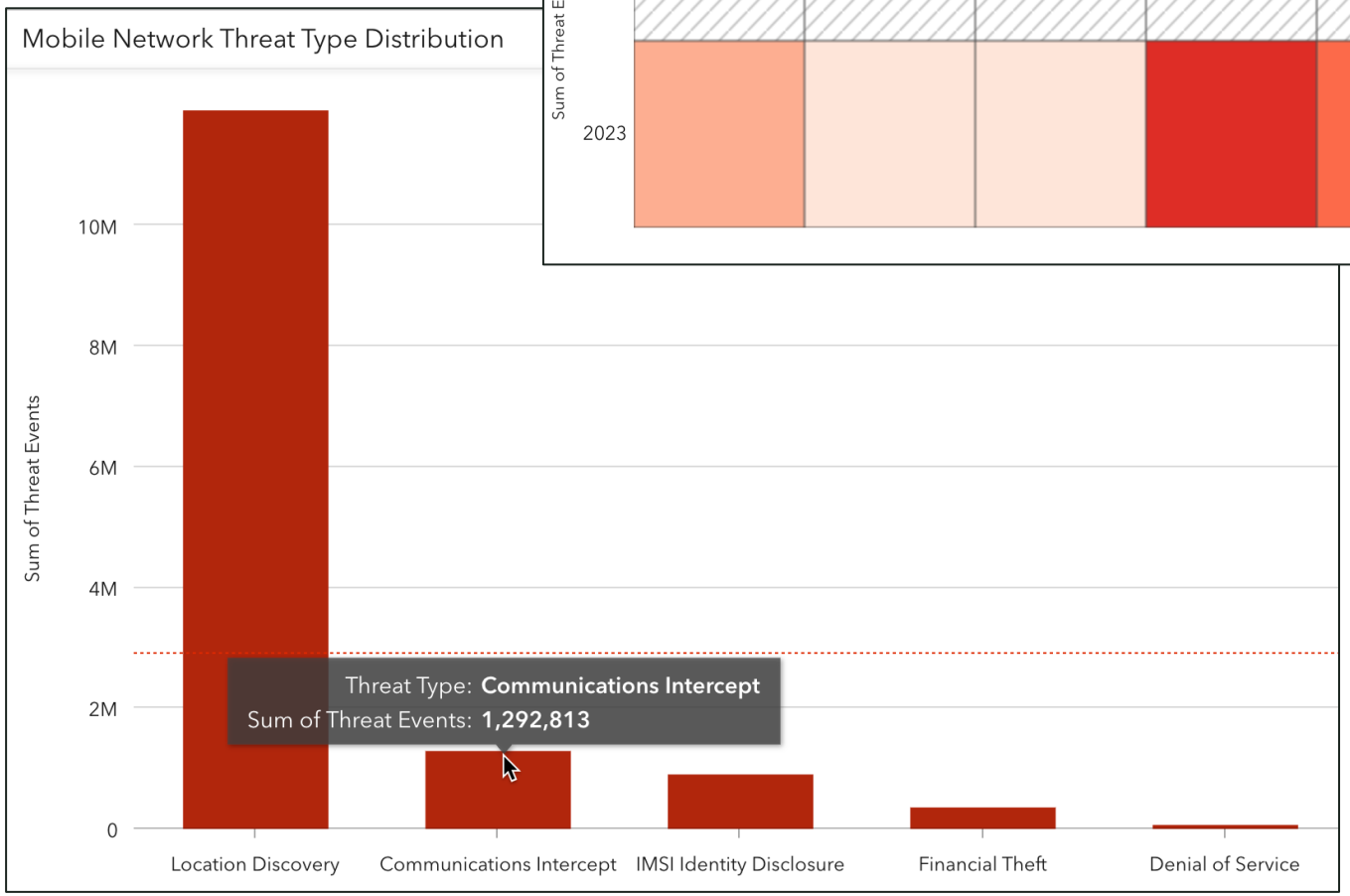
Attack telemetry data from mobile operator network firewalls suggests otherwise...

Over 200 Networks Are Seen Targeting African Mobile Network Users



Telecom networks are massively exploited in regions of repression and conflict

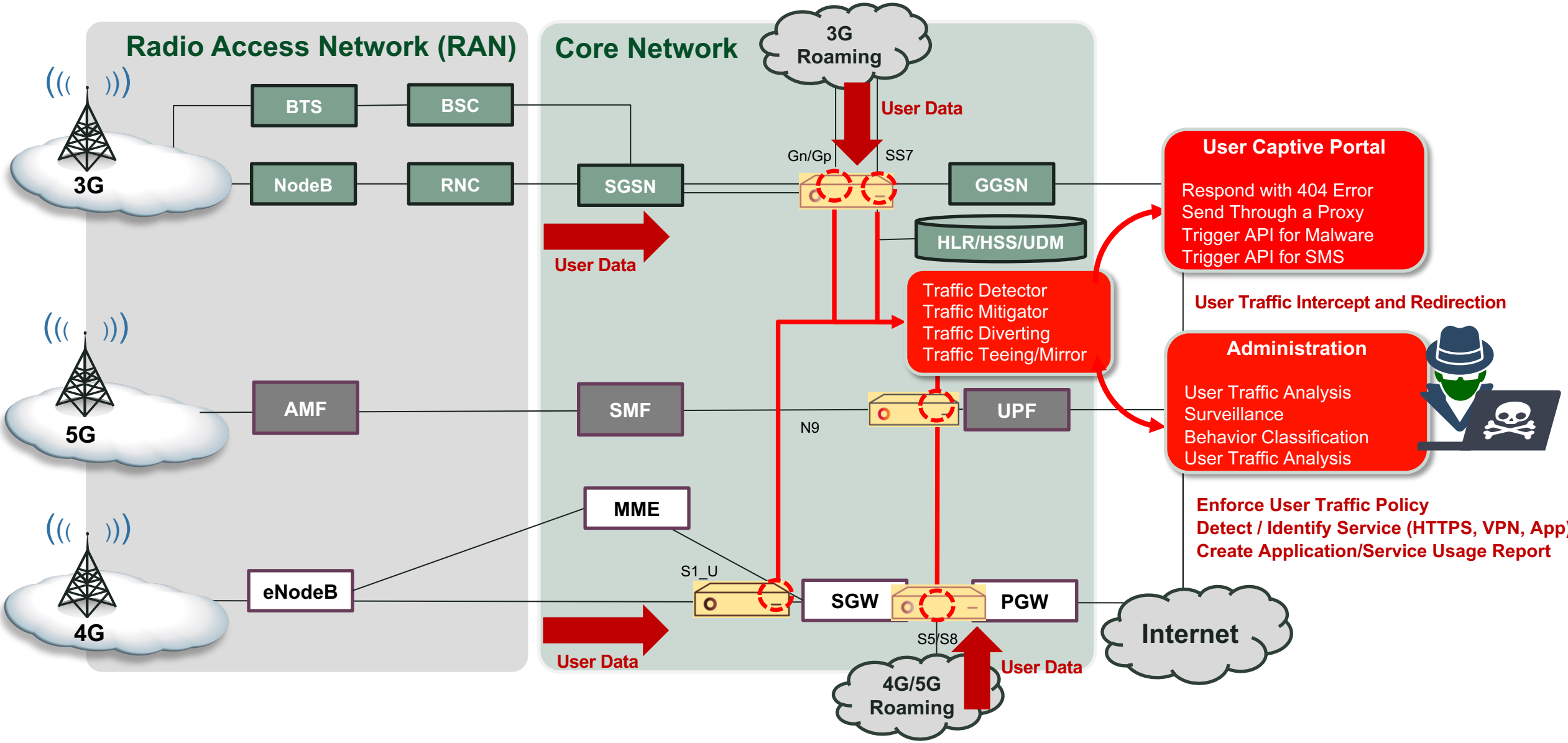




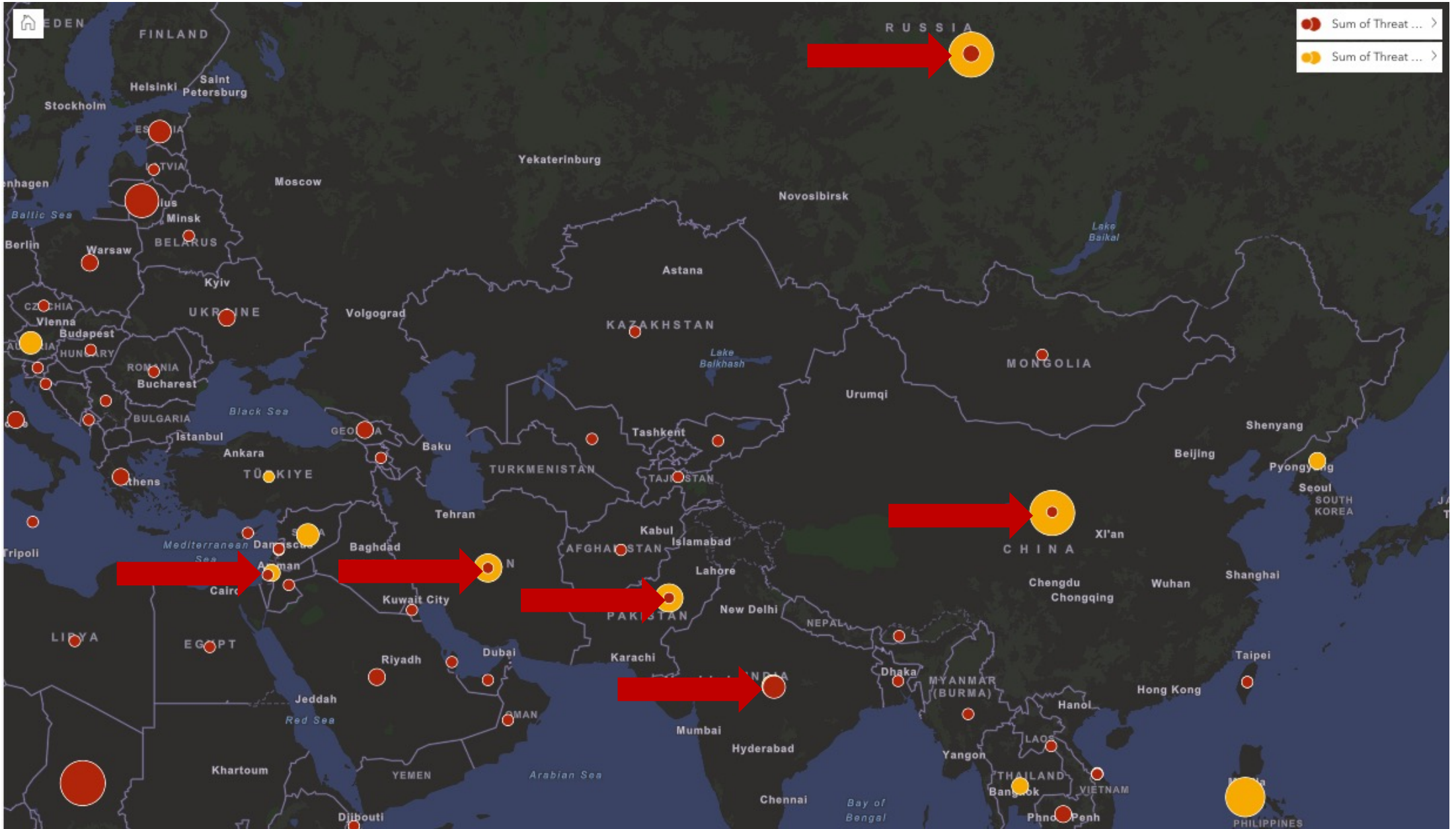
- **Niger** – Presidential coup d'etat
- **Sudan** – War between rival military groups
- **Botswana** – Anti same-sex marriage bill protests
- **Congo DRC** – Congolese and Rwandan clashes
- **Sierra Leone** – Legislative elections
- **Kenya** – Widespread economic demonstrations and al-Shabaab attacks

They also monitor and manipulate usage centrally with DPI technology

Centralized telecom systems capture all service interfaces, enabling reconnaissance and targeted spyware distribution



Spyware and network surveillance attacks appear from sources we expect



How a Swiss telecom provider runs a global surveillance system

An obscure telecommunications company based in Basel, Switzerland operates a surveillance system sold to government agencies with licenses from the ITU, Switzerland, Sweden, and Antarctica, using networks from Cambodia, South Pacific Islands, Italy, Madagascar, Russia, UK, Iceland, and Vietnam.

LIGHTHOUSE REPORTS

Fink Telecom Surveillance in Africa Exceeded 18,000 Attacks

Fink Telecom "Corporate HQ"

Cadcomms - Cambodia
Mobile license revoked in 2020

Fink Telecom and SMS Relay
both owned by Andreas Fink

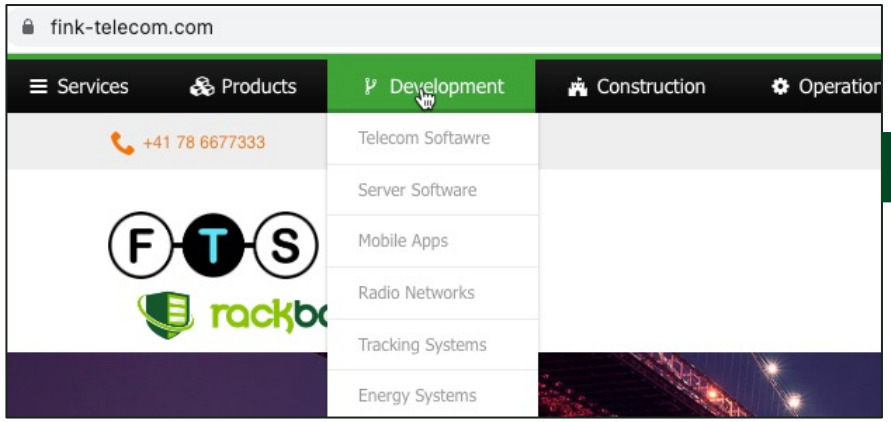
Operator Unknown – GT number in OFCOM "Protected" range

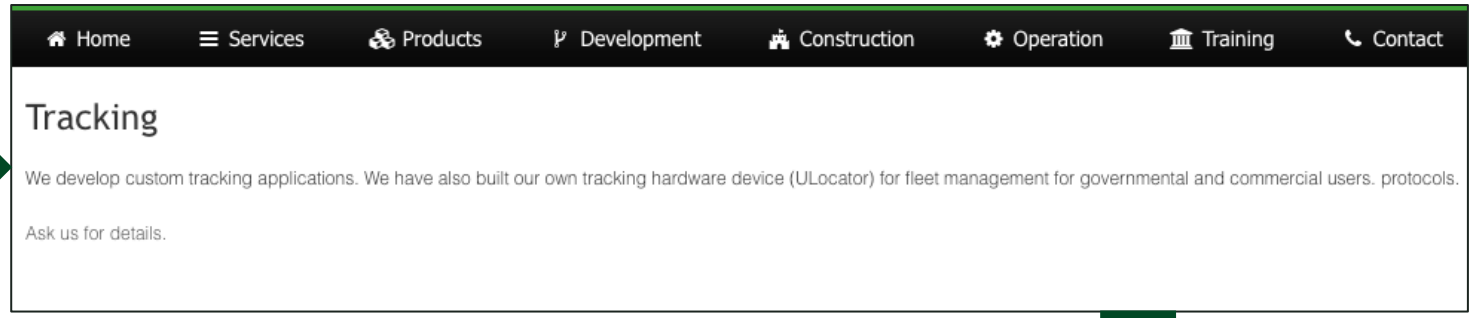
Gmobile – **Vietnam** – Owned by the **Ministry of Public Security**

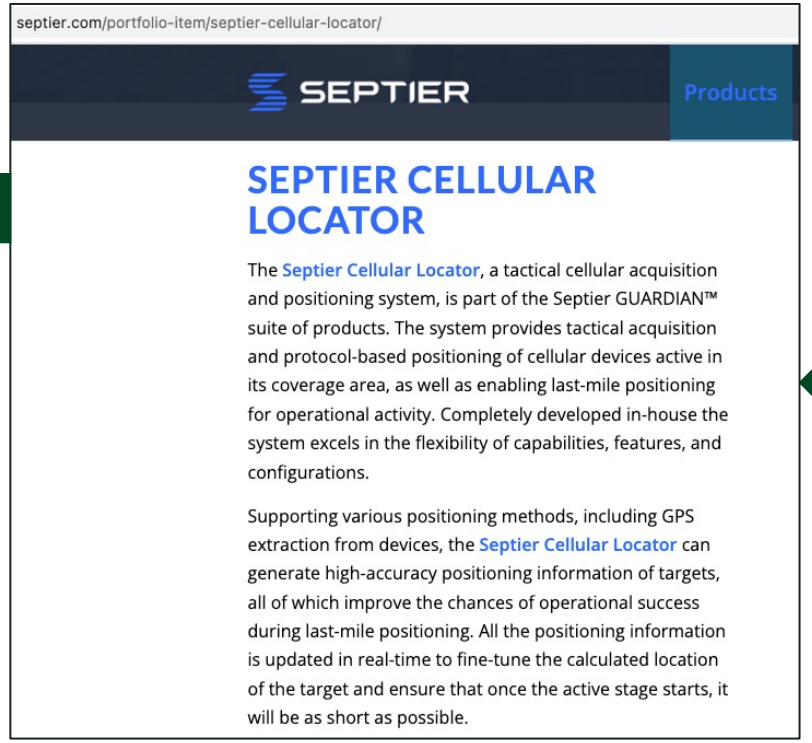
Fink Telecom Surveillance Network Cluster

Source Country	Source Network	Calling GT
Cambodia	CADCOMMS	85513000222
Fiji	DIGICEL FIJI	6797001057
Iceland	IMC ISLAND	3546500493
Italy	Unknown	390760000039
Madagascar	MADACOM CELTEL	261331111201
Papua New Guinea	DIGICEL PAPUA NEW GUINEA	67572210444
Russian Federation	MIATEL LLC	79588879810
Samoa	DIGICEL SAMOA	6857700095
Switzerland	FINK TELECOM SERVICES	4158707123456
Switzerland	FINK TELECOM SERVICES	41587070188
Switzerland	SMSRELAY	4144596008
Switzerland	FINK TELECOM SERVICES	4186044596008
Tonga	DIGICEL TONGA	6768900003
United Kingdom	Unknown	44753259780
United Kingdom	LIMITLESS MOBILE2	447458810177
United Kingdom	Unknown	44753252780
United Kingdom	Unknown	44753250080
Vanuatu	DIGICEL VANUATU	6785330094
Vietnam	GTEL MOBILE	841993973021
Vietnam	GTEL MOBILE	841993973022

A surveillance "suite" is sold– with Global Title addresses, a cloud-hosted platform, and access to the private global telecom intercarrier IPX network







How can decentralized networks help?

Courtesy of FACTION NETWORKS

Eliminate cloud-based vulnerabilities and centralized control by empowering users to create secure and private networks

No Visibility or Access by Admins or Staff

End User Authentication

Network Owner

Creates and controls the key

... and is the ...Certificate Authority

No User Data or Metadata

Encrypted with your key

No VPN Server

Network

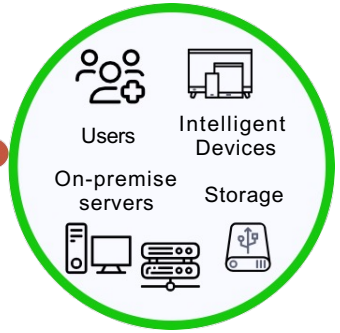
Invisible and inaccessible on the Internet

Private Web Browsing

Web exit nodes are known only to you- or BYO server

LANs and WANs

Ensure network path to LANs & WANs is private and secure



Users and Personal Devices

Replace LANs and WANs with a Personal Private Network (PPN) organized into unlimited Groups

Cloud Servers & VMs

Add them and manage access for user groups in your PPN

Smart and Dumb Devices

Extend your PPN to securely connect devices not smart enough to encrypt

Network Pods

No Credentials

No External Certificate Authorities

No IAM & Authentication Servers

E2E Data Encryption

Encrypt data on endpoints, in transit, and in the Cloud - with your keys

What we know and what we can do

Centralized telecom networks create a hidden surveillance economy

Network surveillance and spyware are different, but achieve the same objectives

As a mobile user, there's little you can do to protect yourself in repressive countries

Action from regulators is long overdue and should not be expected

HELP CHART A NEW PATH FORWARD

- Decentralized Networks
- Decentralized Security
- Attack Transparency
- Response From Like-Minded Governments


Thank You