

# IMSI catchers in the age of 5G

*IMSI-catchers, SMS blasters, and the mobile security gap nobody's closed*

**Past**

Once upon a time

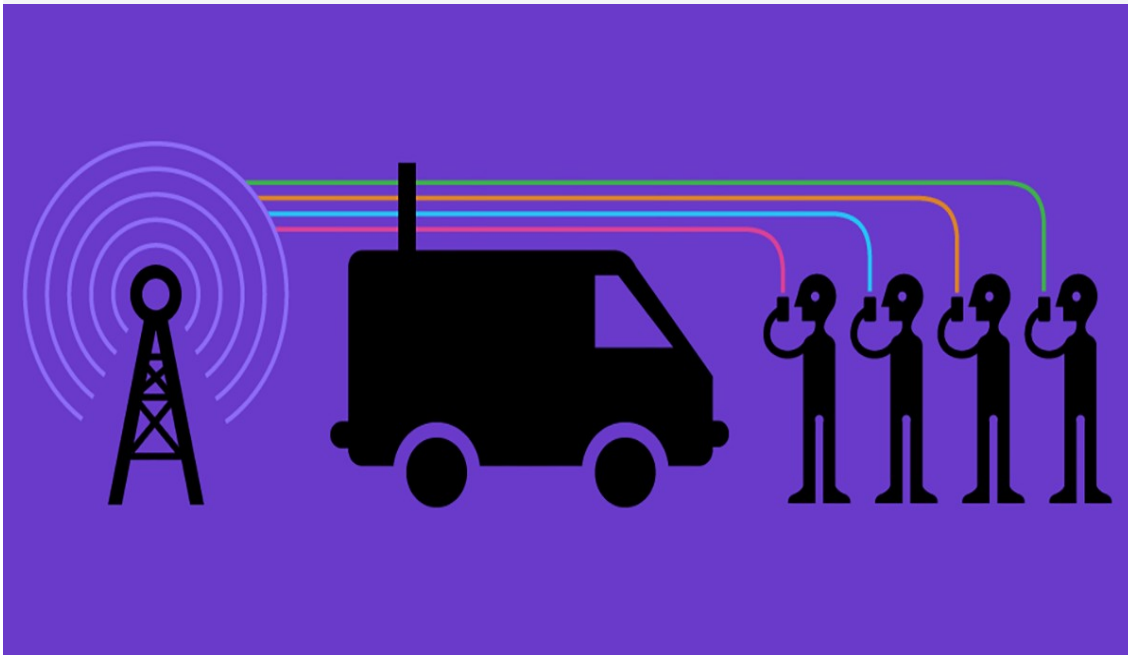
2013



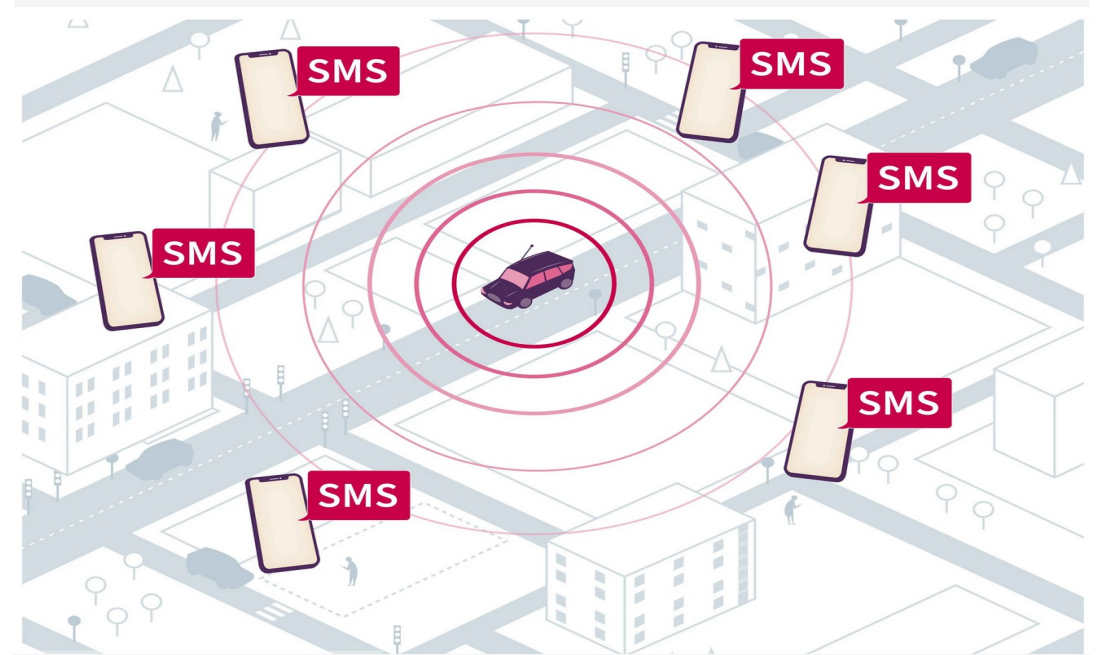
**Present**

# Two devices, one trick

## IMSI-catcher



## SMS blaster



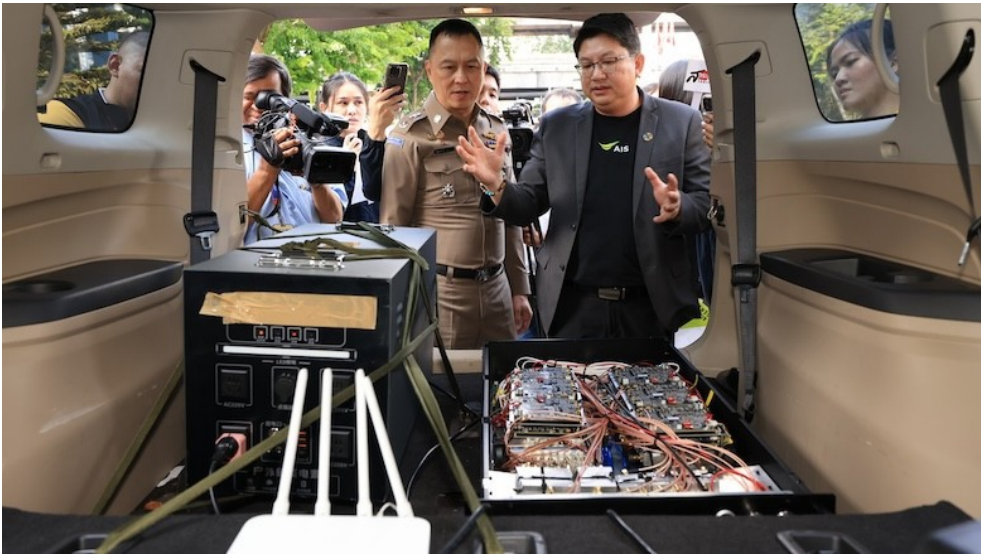
## NOT A REGIONAL PROBLEM

## Cases across several continents



Source: Commsrisk [Global Fraud Dashboard](#)

# SMS Blasters: The Fraud Machine Anyone Can Buy Online



## Three jailed for hijacking mobile signals in Dubai Marina



Image used for illustrative purpose. Photo: File

The digital trail eventually led police to a vehicle in Palm Jumeirah, containing jamming devices, a signal receiver, and equipment used to send fabricated SMS messages

## THE UNCOMFORTABLE PART

# Who's actually behind them?

## Criminal gangs



## State actors



## COWs (Cell-on-Wheels)



Source: [Japan Radio Co. LTD](#)

## Emergency Management





**FIELD TESTED!**



**GUARDIAN IMSI CATCHER**

- Polyfunctional & Innovative cellular scheduler
- Full SDR Device
- Multiple Configurations



Russian Army's RB-341V  
Leer-3 EW system

## Spy ring plotted to obtain details from phones of Ukrainians at US airbase in Germany, UK court hears

Group made plans in late 2022 to obtain information and pass on anything that could benefit Russia in its invasion of Ukraine



Airborne interception

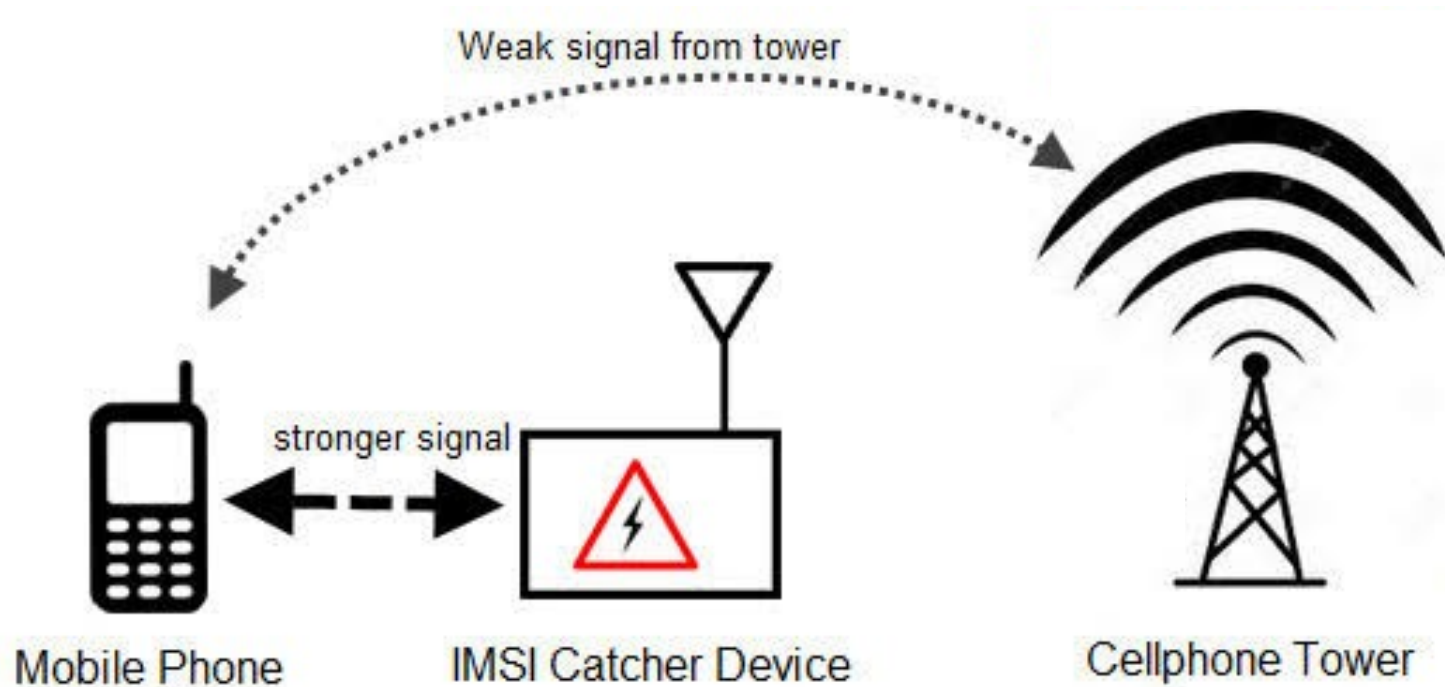


Troop & movement tracking



Diplomat & political  
targeting

## Trust happens before security does



- 1 A phone picks which tower to trust based only on what it broadcasts.
- 2 That step happens before any authentication or encryption runs.
- 3 It has never been protected – in any generation.

NOT A 2G PROBLEM

## Same gap, every generation since

**2G**

tower-trust step:

**unprotected**

**3G**

tower-trust step:

**unprotected**

**4G**

tower-trust step:

**unprotected**

**5G**

tower-trust step:

**unprotected**

*5G added real protections — encrypted subscriber IDs, stronger auth. None of it touches this first step.*

## **“We turned off 2G” doesn't fix it**

### **The assumption**

Carriers shut off 2G, so the old attack surface goes away.

### **The reality**

Phones still carry the old radio hardware, and disabling it is a setting most people don't know exists.

WHERE THIS ACTUALLY GETS FIXED

## Three places this has to move

1

**Phones**

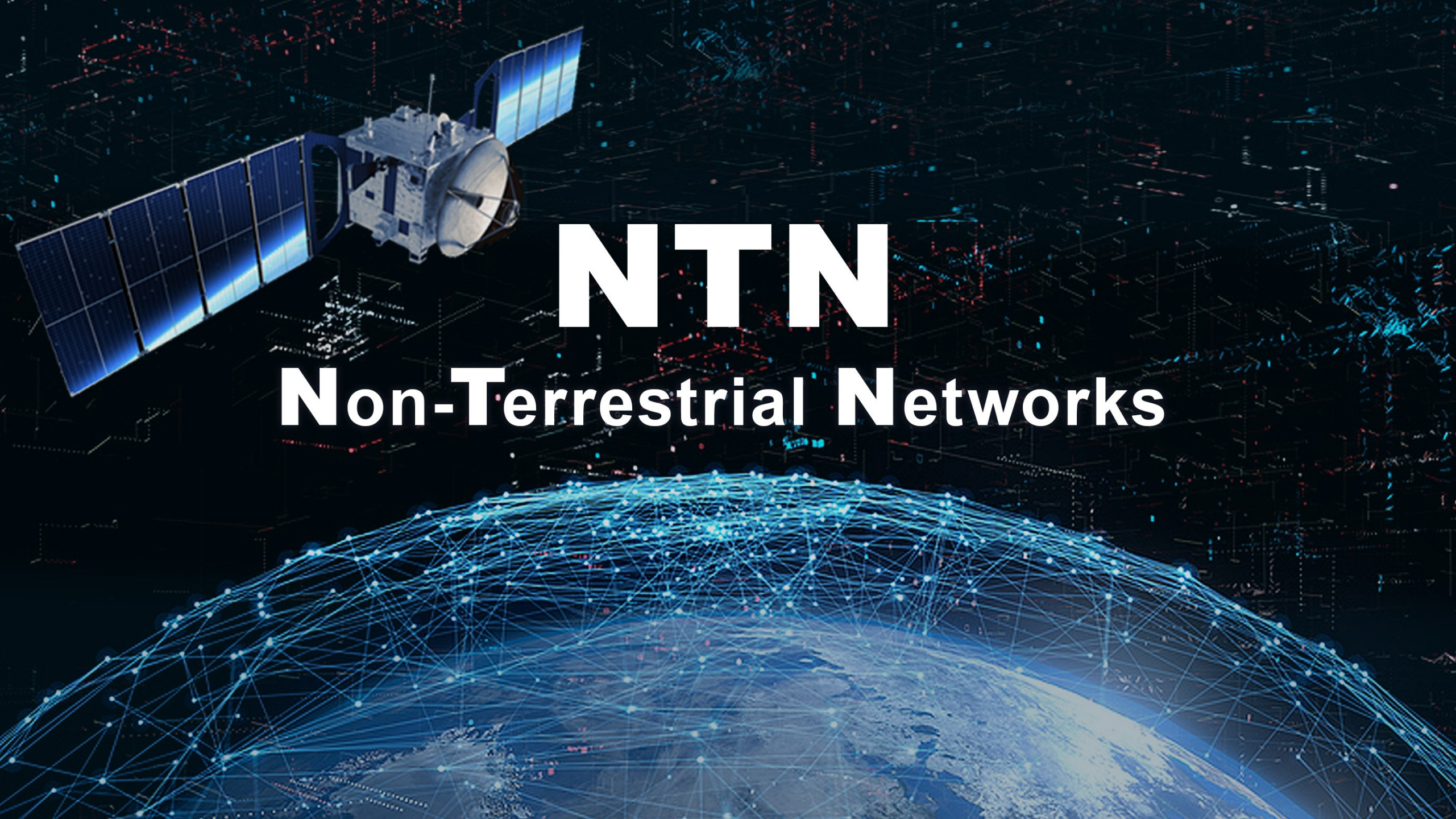
2

**Carriers**

3

**Law enforcement**

**Future**



# **NTN**

## **Non-Terrestrial Networks**

## IMSI catching in NTN era

Passive continental-scale beam sniffing

Feeder-link and gateway-side interception

Rogue small-cell exploiting NTN/TN fallback

Rogue satellite / rogue beam impersonation (long-term but real)

## Key lesson

Trust-before-auth is a 20-year debt, not a 2-year bug

Your job as the next generation is to refuse the inheritance

# Thank you

[Dr. Altaf Shaik] • [altaf.shaik@fastiot.org]

*Questions*