ENEA
AdaptiveMobile Security

Mobile Networks – The Hidden Global Battlefield

Rowland Corr

Director of National Security Intelligence

29/06/2022

About Enea

Publicly Listed

NASDAQ

Stockholm

Revenue (MUSD)

~110

No. of Employees

~770

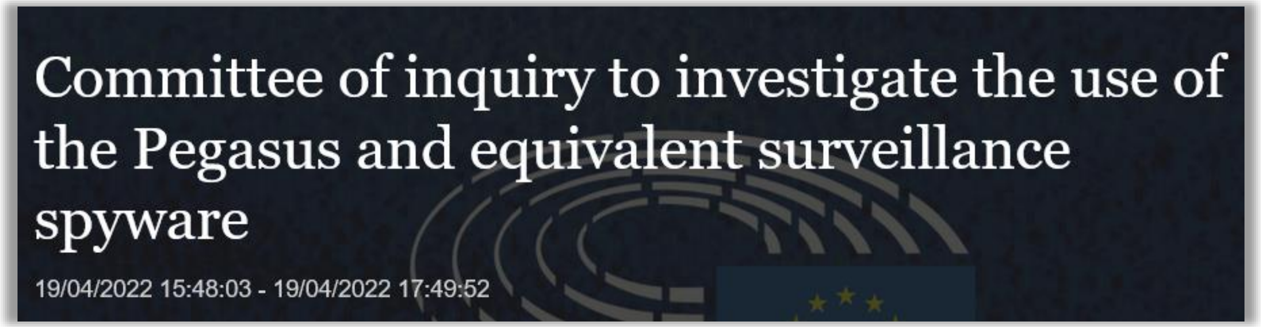
No. of Operator Customers

~100

Enea is one of the world's leading **specialists in software for telecommunications and cybersecurity.**

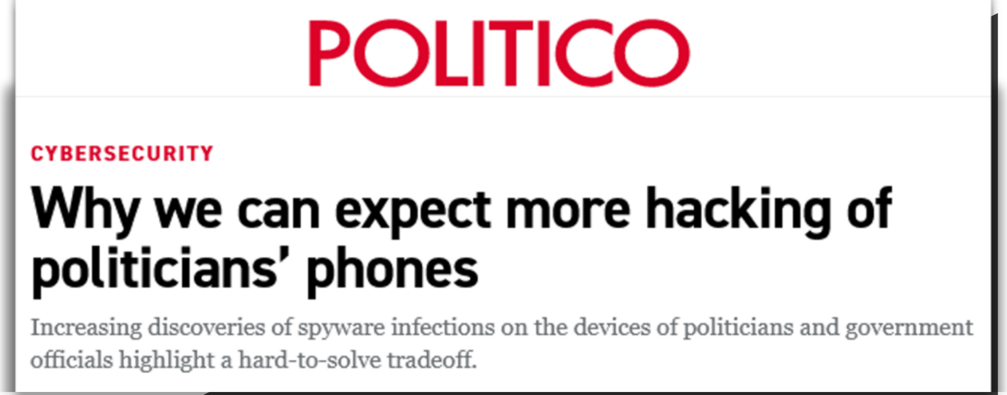
More than 4.5 billion people rely on Enea technologies in their daily lives.

Mobile Device-focused Attacks are Increasingly in the News



Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware

19/04/2022 15:48:03 - 19/04/2022 17:49:52

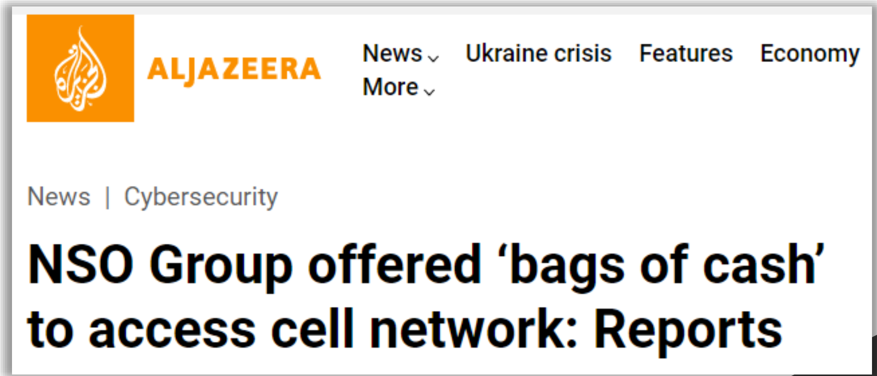


POLITICO

CYBERSECURITY

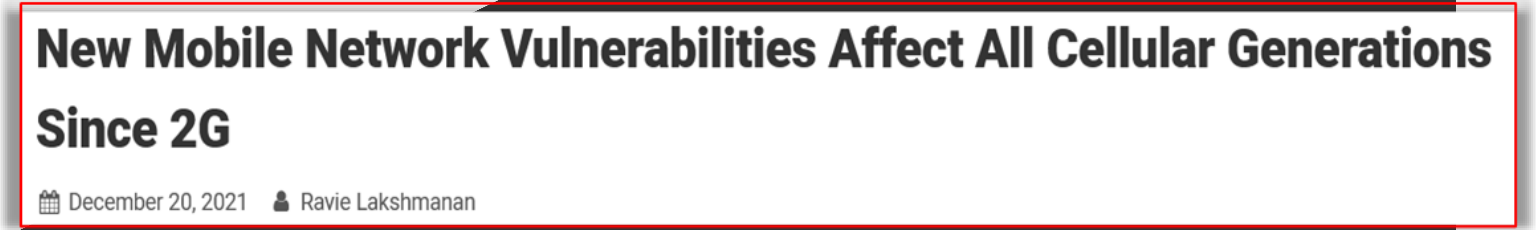
Why we can expect more hacking of politicians' phones

Increasing discoveries of spyware infections on the devices of politicians and government officials highlight a hard-to-solve tradeoff.



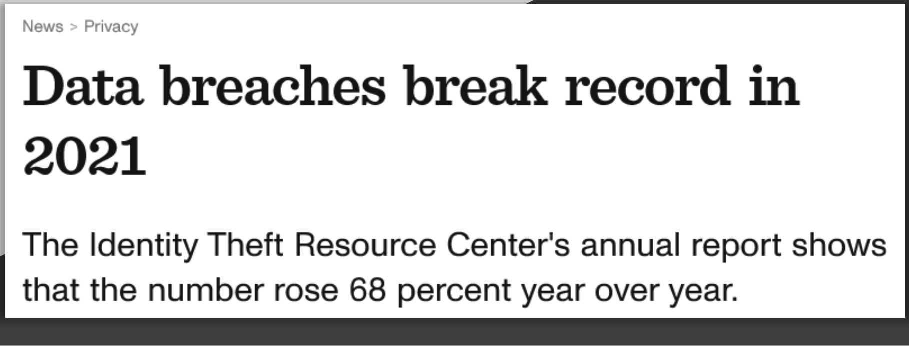
News | Cybersecurity

NSO Group offered 'bags of cash' to access cell network: Reports



New Mobile Network Vulnerabilities Affect All Cellular Generations Since 2G

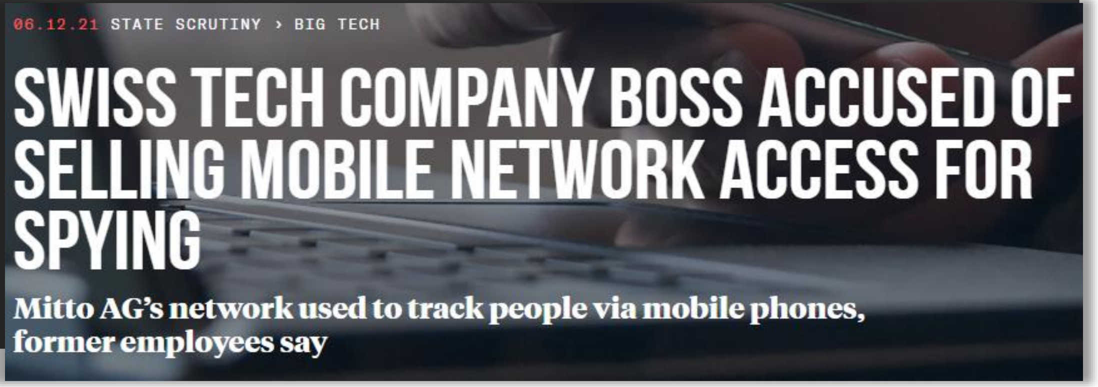
December 20, 2021 Ravie Lakshmanan



News > Privacy

Data breaches break record in 2021

The Identity Theft Resource Center's annual report shows that the number rose 68 percent year over year.



06.12.21 STATE SCRUTINY › BIG TECH

SWISS TECH COMPANY BOSS ACCUSED OF SELLING MOBILE NETWORK ACCESS FOR SPYING

Mitto AG's network used to track people via mobile phones, former employees say

The Hidden Battlefield – Terrain & Campaigns that go Unreported

- Reporting on Spyware – only most ‘visible’ element of the threat landscape

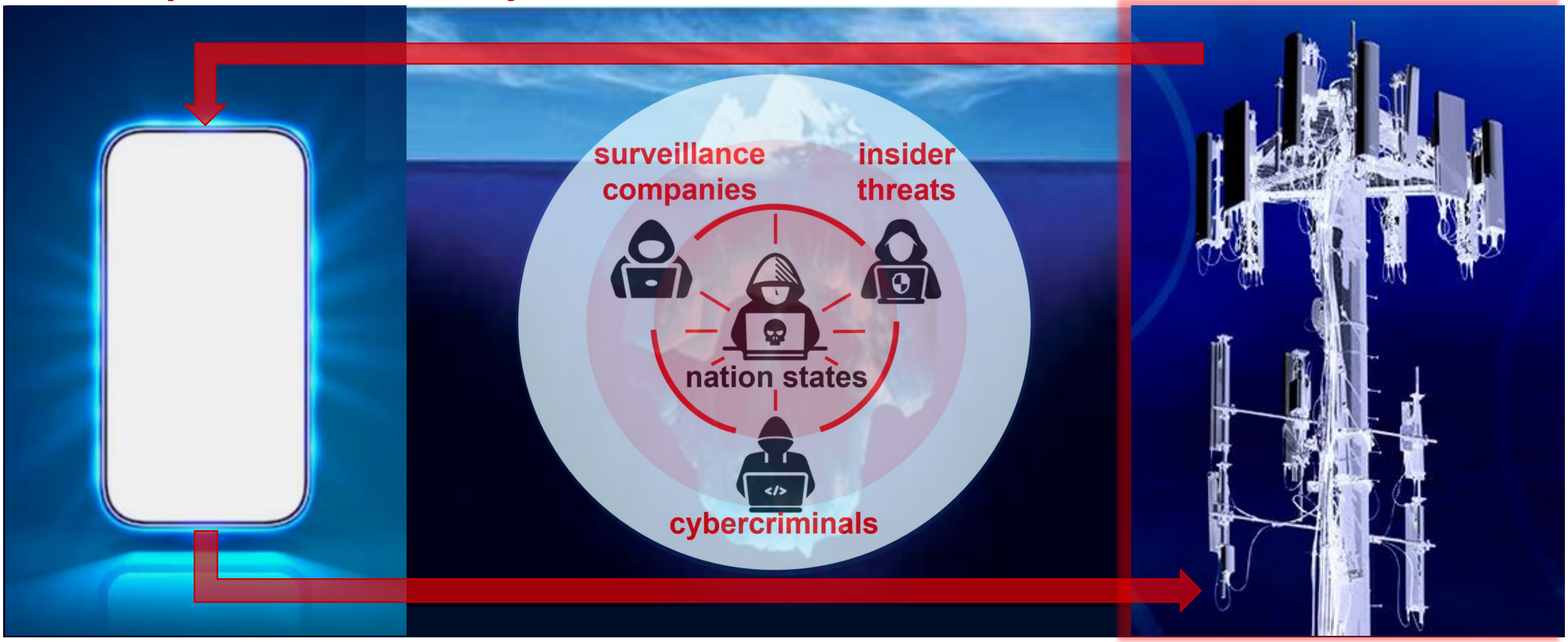
Mobile Spyware

Wider Targeting of Individuals & Networks:

- Data Exfiltration
- Location Tracking
- Communications Interception
- Network Reconnaissance
- Data Manipulation
- Denial of Service

The Hidden Battlefield – Terrain & Campaigns that go Unreported

- **Weaponization not only of devices - also of *Network Infrastructure***



Ukraine – Ahead of the Curve in Recognising Convergent Cyber Threats

S77 Attacks in context of “the first real cyberwar”

2014:

- Ukraine reported the world’s first reports of Signalling (SS7) attacks, from Russian sources.
- **Details:**
  - https://blog.adaptivemobile.com/russia-ukraine-telecom-monitoring

2022:

“We have already seen attempts to use captured telecommunications infrastructure to conduct attacks, including attacks using the Signaling System 7 (SS7)”

Source: https://therecord.media/from-the-front-lines-of-the-first-real-cyberwar/

Signalling Attack as a Hybrid ‘Force Multiplier’

- **The combined use of signalling attack with other cyber capabilities is consistent with ‘*horizonal escalation*’ described in EU Hybrid Threat modelling.**

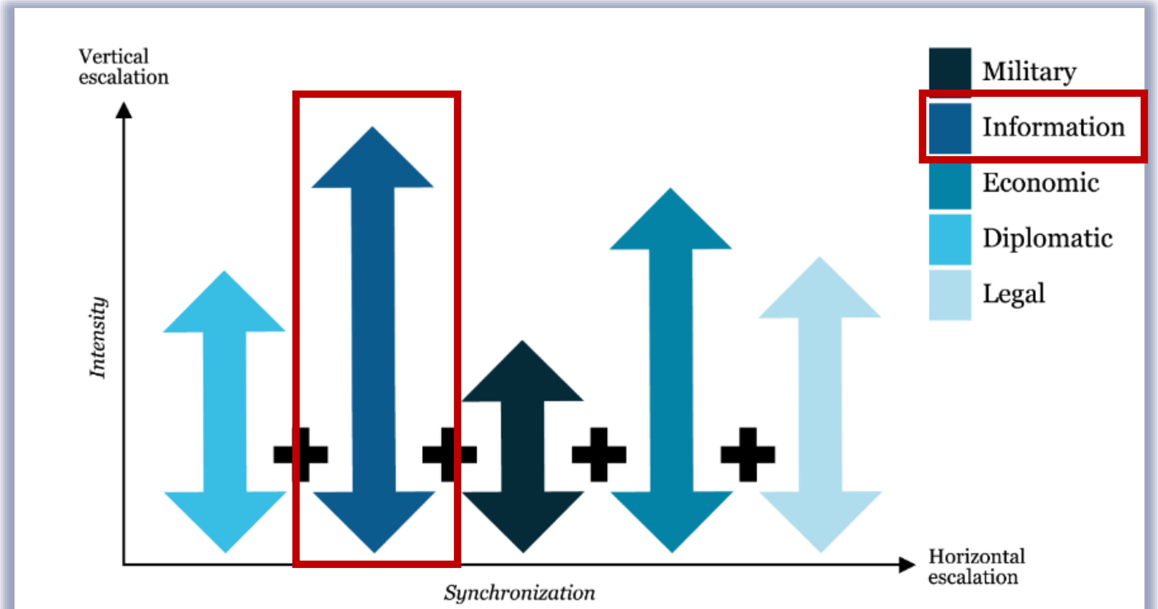
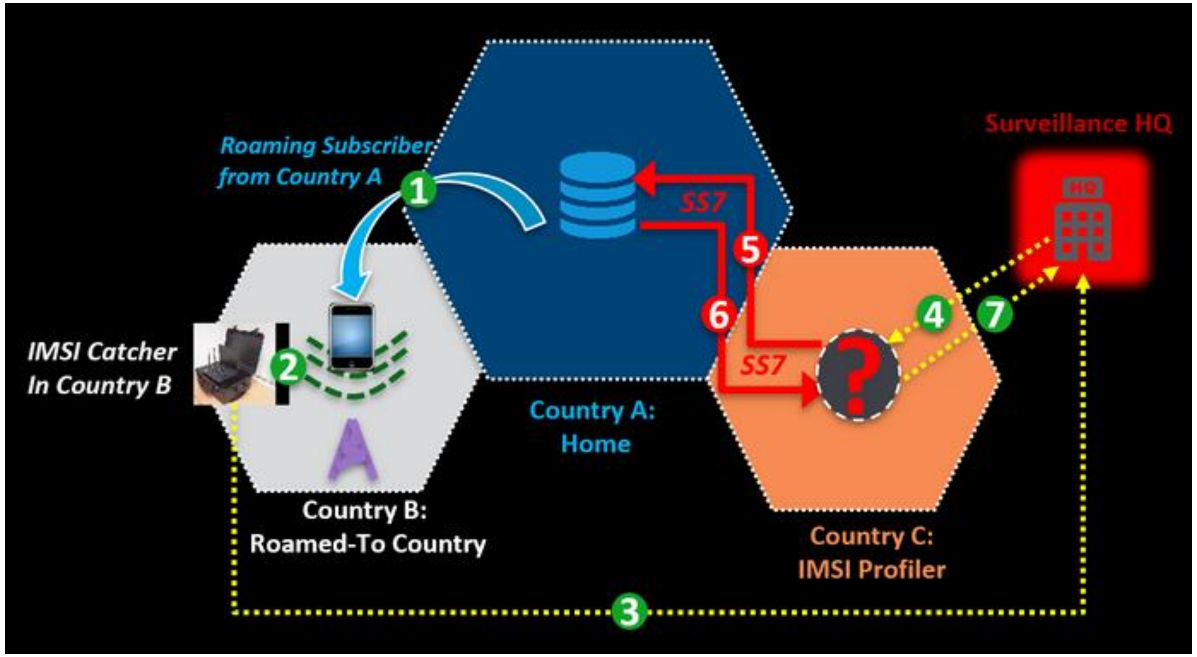


Figure 3: Combining instruments of power in hybrid conflict[5]



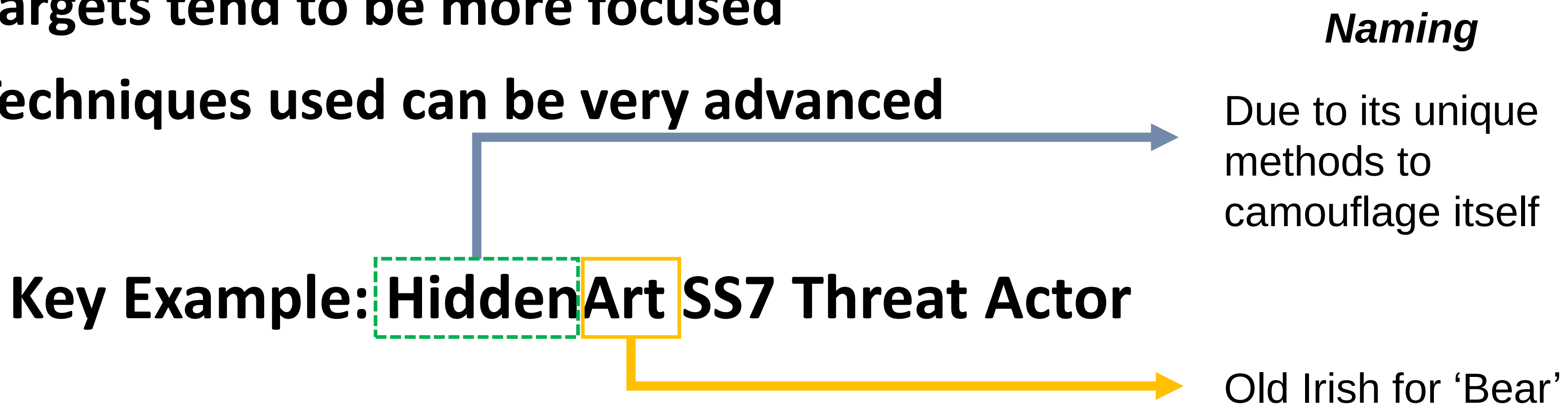
Roaming Subscriber from Country A
1
2
3
4
5
6
7
SS7
SS7
Surveillance HQ
HQ
IMSI Catcher In Country B
Country A: Home
Country B: Roamed-To Country
Country C: IMSI Profiler

Detected combined deployment of IMSI Catcher & Signalling Attack for Target Acquisition

State-Level Threat Actors

Behaviour can appear similar to Surveillance Companies, but some differences:

- **Volumes tend to be considerably lower**
- **Extended periods of inactivity, normal activity is often reconnaissance/probing based, occasional periods of large activity**
- **Targets tend to be more focused**
- **Techniques used can be very advanced**



Naming

Key Example: HiddenArt SS7 Threat Actor

Due to its unique methods to camouflage itself

Old Irish for ‘Bear’

More info: https://blog.adaptivemobile.com/the-hunt-for-hiddenart

HiddenArt – A Sophisticated Core Network Signalling Threat Actor

Behaviour:

- Primarily Location Tracking, Voice and SMS Interception
- Activity in Bursts, long period in between attacks. Periodic reconnaissance against target networks

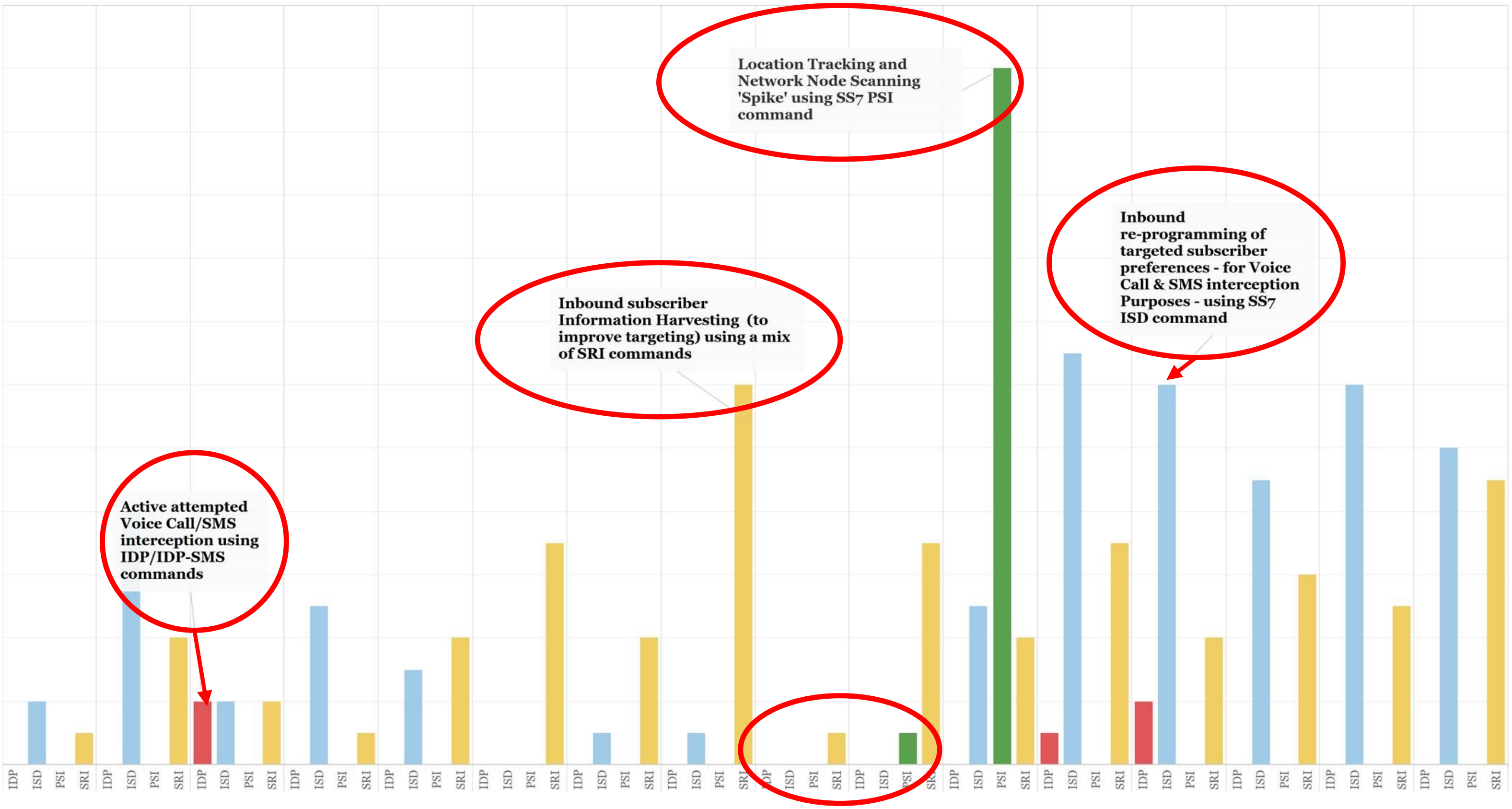
Targets:

- VIP Individuals, many Russian linked

Originating Source (indicative):

- African Mobile Operator Group

HiddenArt platform : Malicious network attacks over multi-day period



Location Tracking and Network Node Scanning 'Spike' using SS7 PSI command

Inbound re-programming of targeted subscriber preferences - for Voice Call & SMS interception Purposes - using SS7 ISD command

Inbound subscriber Information Harvesting (to improve targeting) using a mix of SRI commands

Active attempted Voice Call/SMS interception using IDP/IDP-SMS commands

Full details: https://blog.adaptivemobile.com/the-hunt-for-hiddenart

ENEA
AdaptiveMobile Security

Tracking the bear: Investigation and Attribution

- **Investigation into Mobile Operator origin source not consistent with indicative source of traffic**
- **Subsequent direct conversation with Mobile Operator Group**
  - Indicated that no GT leasing was involved.
  - Equipment compromise appeared unlikely, although possible at start
  - Mobile Operator Group Could find no evidence of outbound attacks

They were receiving responses however…

Two main questions:

1. **How was attack injected into network?**
2. **How were attackers getting back answer?**

ENEA
AdaptiveMobile Security

Evidence: Sometimes an Attacker Wants to Have a Conversation

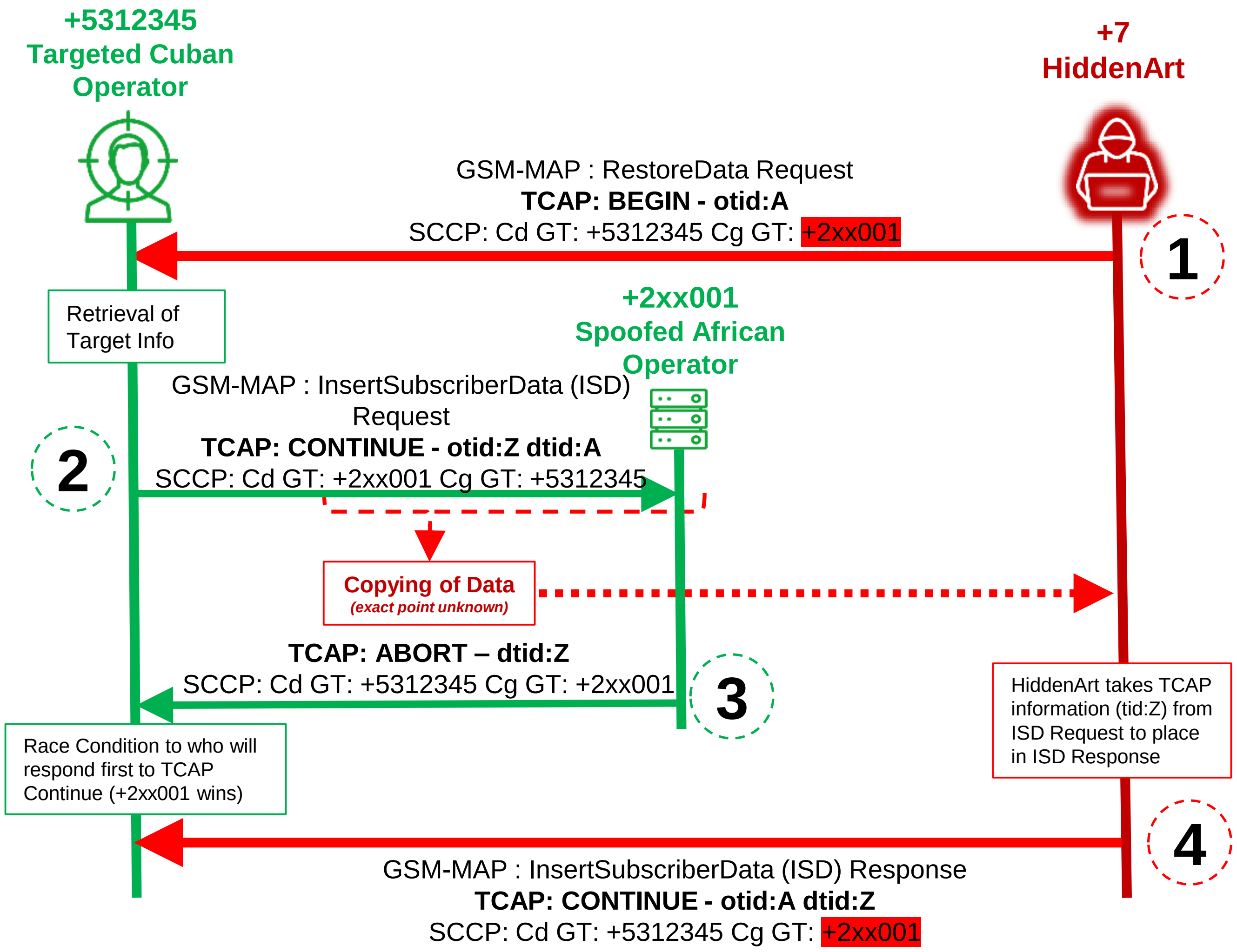
1) **Attacker sends RestoreData**
2) **Victim responds with ISD request**
3) **Spoofed Networks responds with Abort**
4) **Attacker responds with ISD response**

Step 4 : 2nd response - shows copying occurred

- Step 4 could not happen unless copying occurred
- Why? Because no SS7 node would respond twice

Partially unstable system

- Normally Russian GTs represent less than ~1%
- But 75% Russian GTs are used when TCAP sequence is needed (to avoid TCAP Timeout or race condition, as here)



+5312345 Targeted Cuban Operator

+7 HiddenArt

+2xx001 Spoofed African Operator

1

GSM-MAP : RestoreData Request
TCAP: BEGIN - otid:A
SCCP: Cd GT: +5312345 Cg GT: +2xx001

Retrieval of Target Info

2

GSM-MAP : InsertSubscriberData (ISD) Request
TCAP: CONTINUE - otid:Z dtid:A
SCCP: Cd GT: +2xx001 Cg GT: +5312345

Copying of Data
(exact point unknown)

3

TCAP: ABORT – dtid:Z
SCCP: Cd GT: +5312345 Cg GT: +2xx001

Race Condition to who will respond first to TCAP Continue (+2xx001 wins)

HiddenArt takes TCAP information (tid:Z) from ISD Request to place in ISD Response

4

GSM-MAP : InsertSubscriberData (ISD) Response
TCAP: CONTINUE - otid:A dtid:Z
SCCP: Cd GT: +5312345 Cg GT: +2xx001

***Note**: +53 (Cuba) is used here as a targeted country example only*

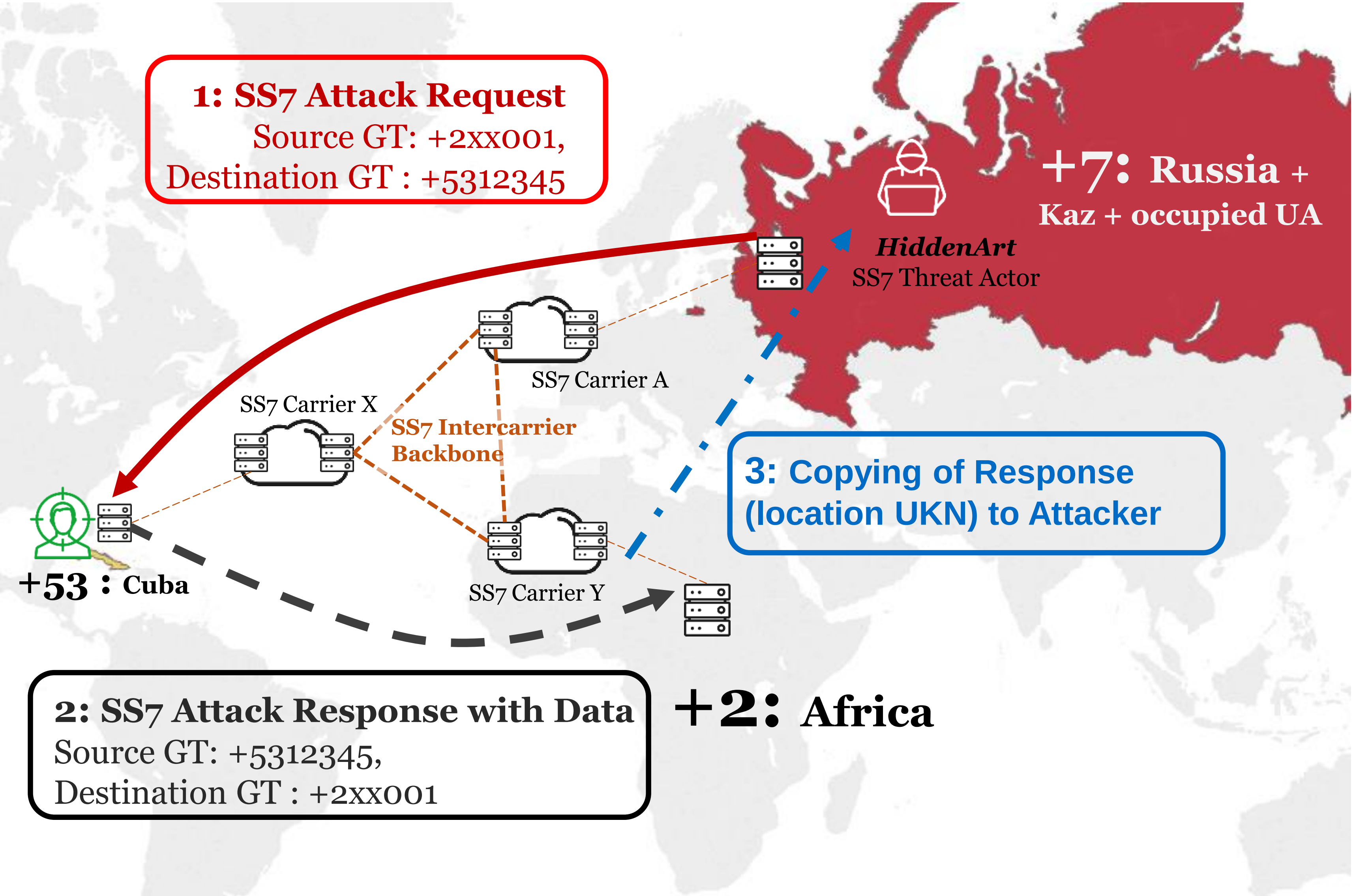
A Unique Method of Extracting Responses

Extraction:

- Attack Requests being injected using spoofed GTs
- If victim networks respond to this, the response **should** be lost

Working Theory: Attack Responses were being copied (at some stage) to Attacker

- Captured network traffic trace indicated this



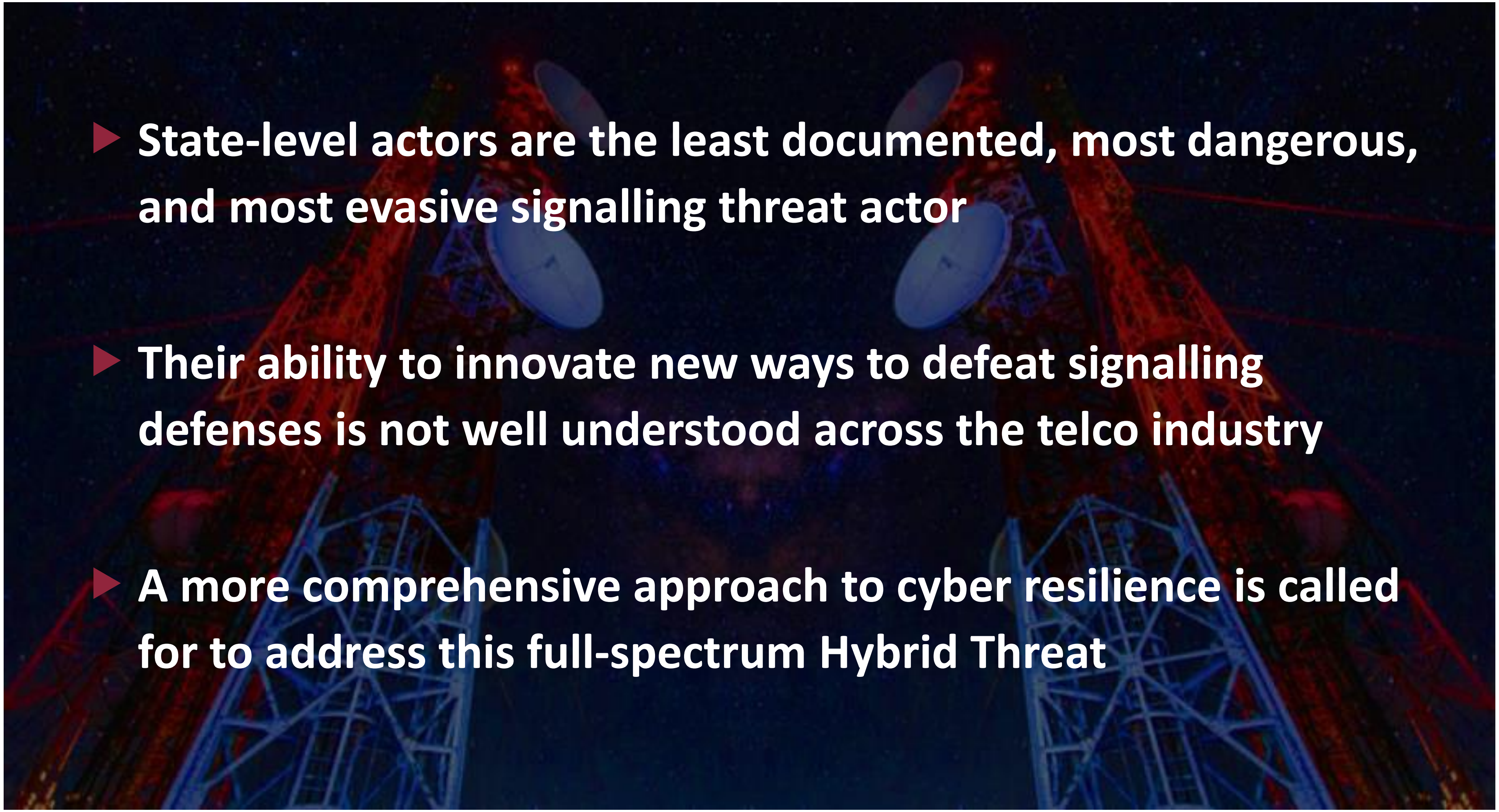
1: SS7 Attack Request
Source GT: +2xx001,
Destination GT : +5312345

2: SS7 Attack Response with Data
Source GT: +5312345,
Destination GT : +2xx001

3: Copying of Response (location UKN) to Attacker

Note*: +53 (Cuba) is used here as a targeted country example only*

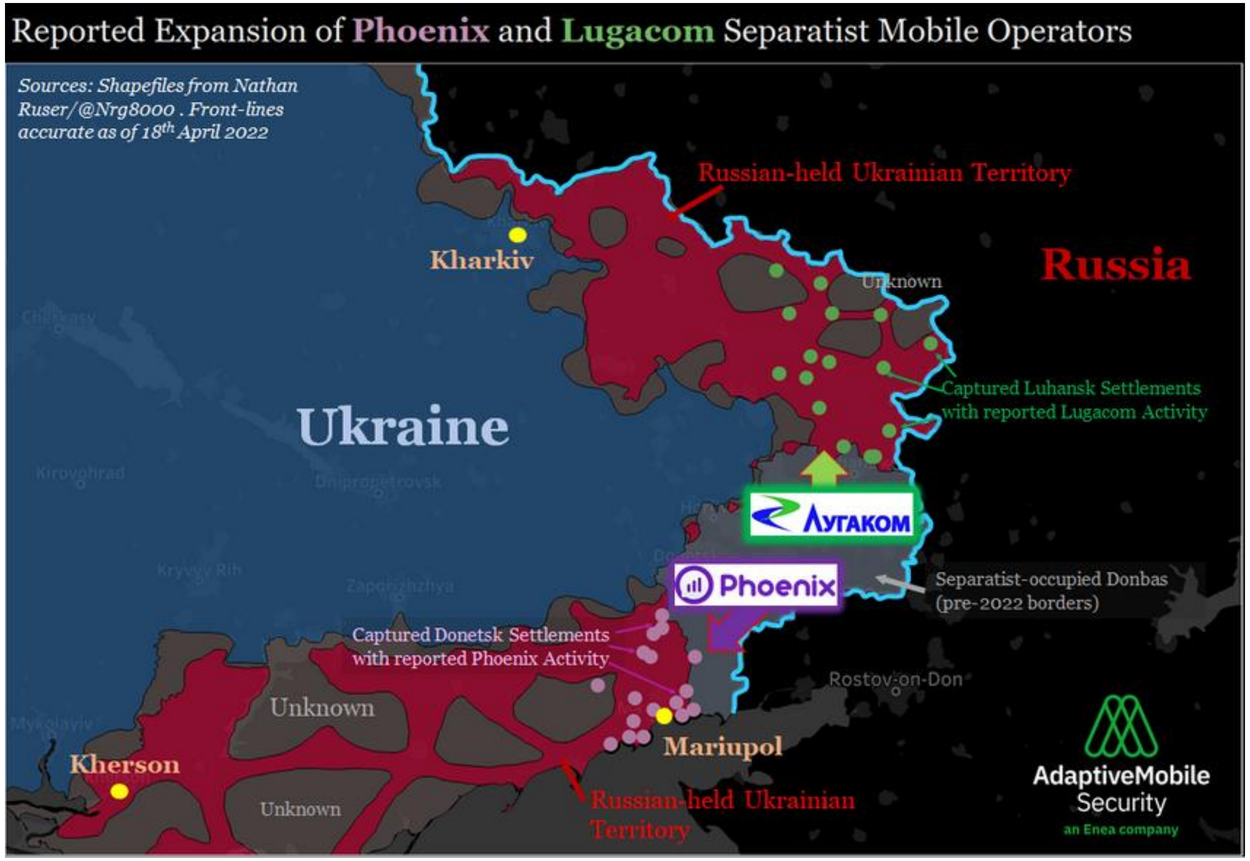
Conclusion



- State-level actors are the least documented, most dangerous, and most evasive signalling threat actor
- Their ability to innovate new ways to defeat signalling defenses is not well understood across the telco industry
- A more comprehensive approach to cyber resilience is called for to address this full-spectrum Hybrid Threat

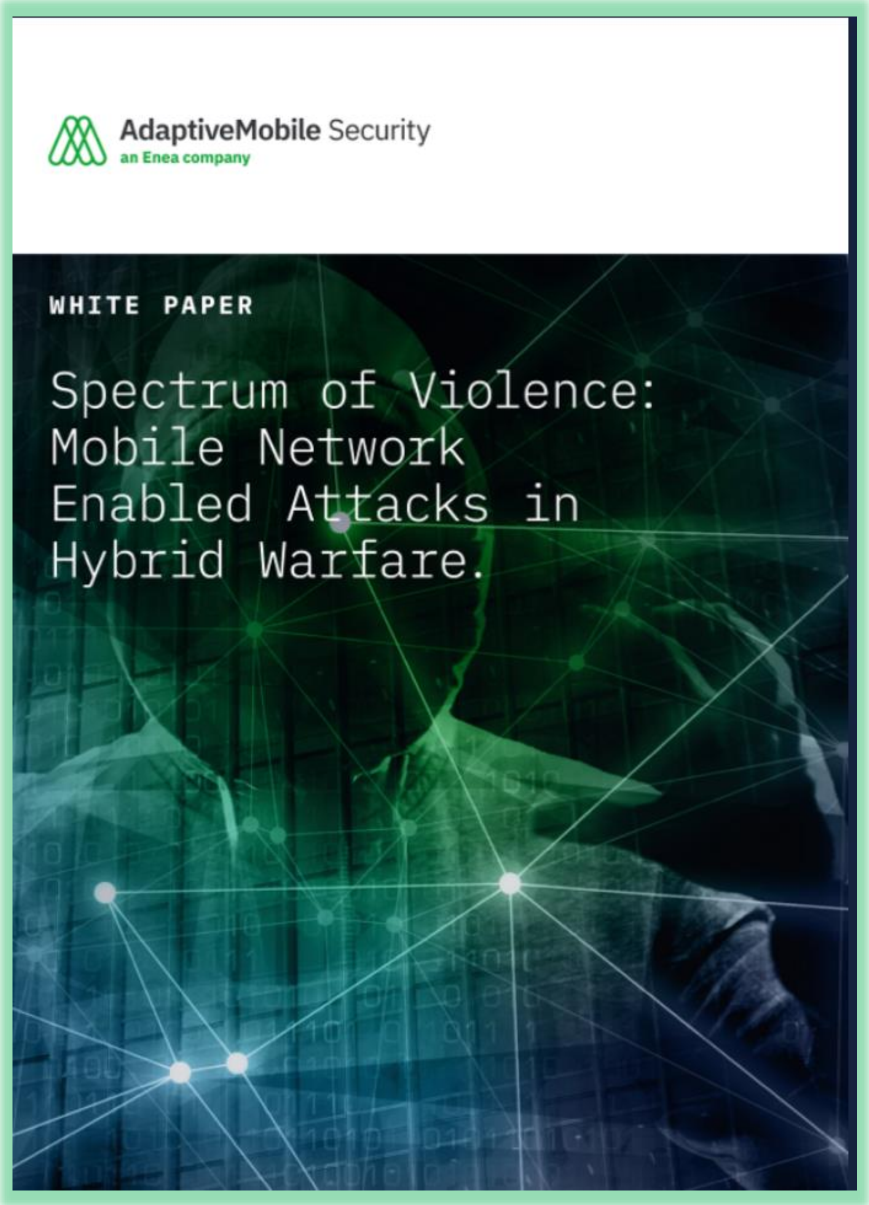
More information

- 3-part Blog series on Mobile Network Battlefield in Ukraine
- Pre-war Blog on HiddenArt
- Pre-war Whitepaper on Hybrid Warfare


Reported Expansion of Phoenix and Lugacom Separatist Mobile Operators

Sources: Shapefiles from Nathan Ruser/@Nrg8000 . Front-lines accurate as of 18th April 2022

Russian-held Ukrainian Territory
Kharkiv
Unknown
Russia
Captured Luhansk Settlements with reported Lugacom Activity
Ukraine
Луганком
Phoenix
Separatist-occupied Donbas (pre-2022 borders)
Captured Donetsk Settlements with reported Phoenix Activity
Rostov-on-Don
Unknown
Mariupol
Kherson
Unknown
Russian-held Ukrainian Territory
AdaptiveMobile Security
an Enea company


AdaptiveMobile Security
an Enea company

WHITE PAPER

Spectrum of Violence: Mobile Network Enabled Attacks in Hybrid Warfare.

www.adaptivemobile.com

ENEA

AdaptiveMobile Security

www.adaptivemobile.com