" WEAPONIZING MOBILE INFRASTRUCTURE"
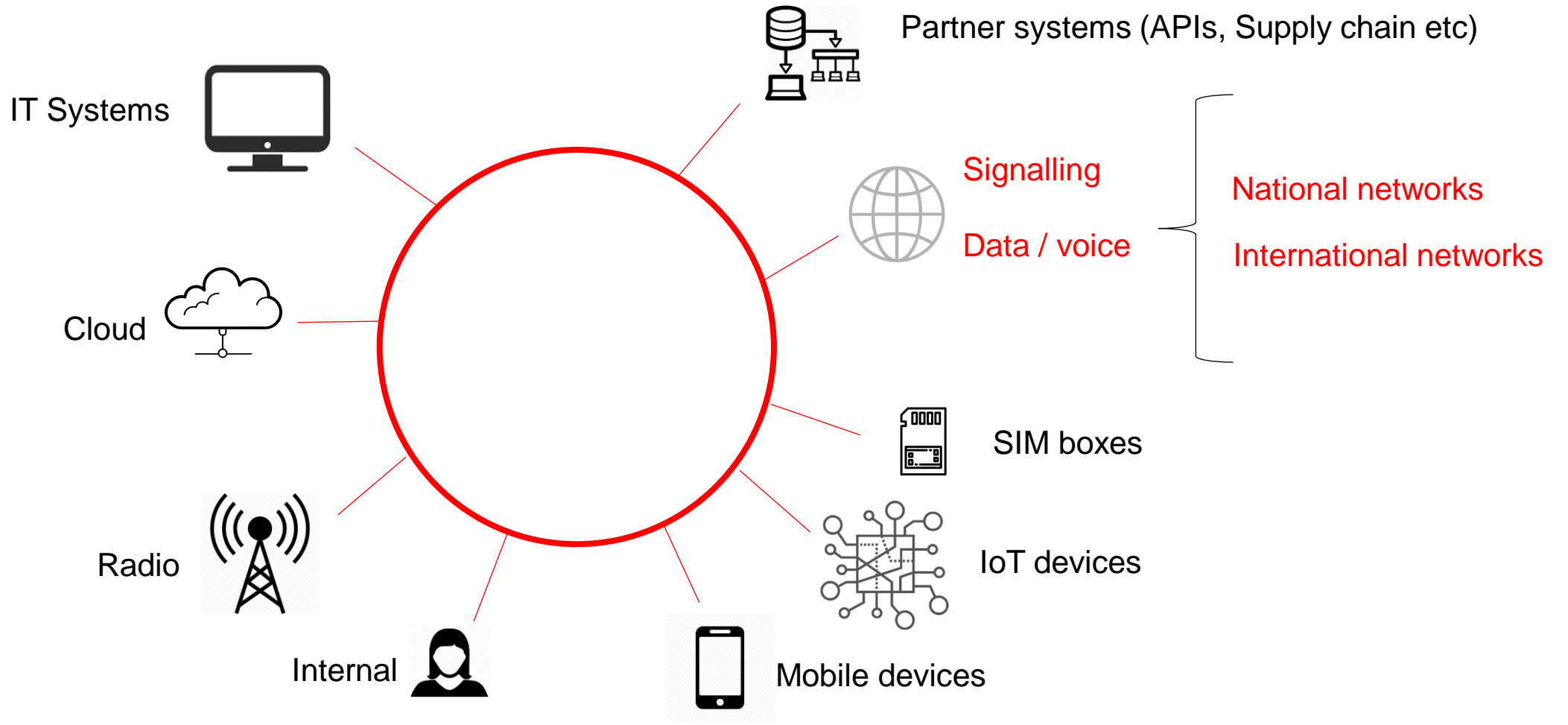
Are Politically Motivated Cyberattacks a Threat to Democracy?

security intelligence

Mobileum platform

mobileum

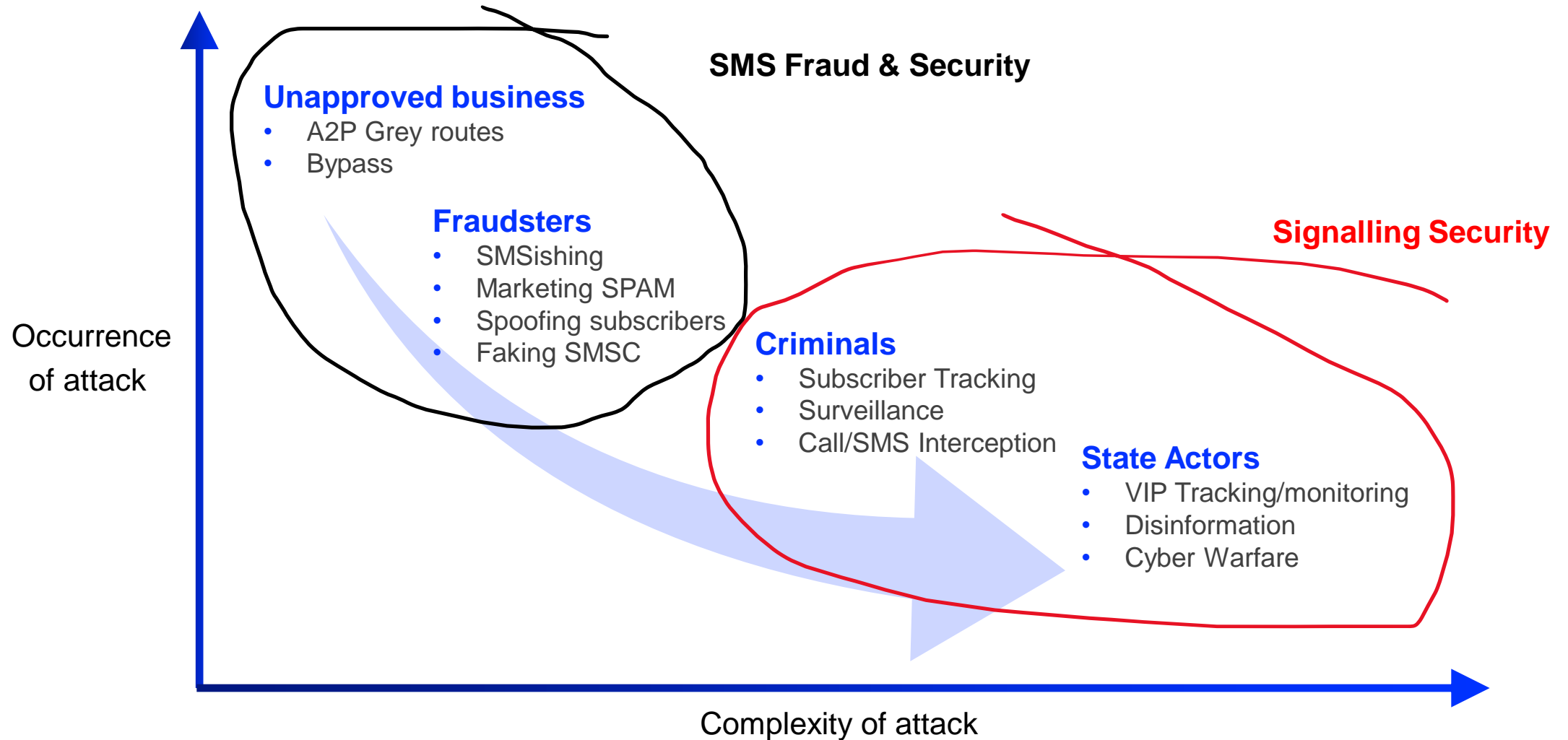Action driven by intelligence

Imran Saleem

AGENDA

1 Network Interconnect Threats?

2 Attackers Analogy and Groups

3 Role of Cyber attacks in armed conflicts

4 The Missed Intel

5 Political shift can drive cyber-attacks

6 The Financial Impact

7 Work Ethics & Disclosure

8 Recommendations

NETWORK INTERCONNECT THREATS

Partner systems (APIs, Supply chain etc)

IT Systems

Signalling

National networks

Data / voice

International networks

Cloud

SIM boxes

Radio

IoT devices

Internal

Mobile devices

ROAMING INTERCONNECT FRAUD & SECURITY….WHAT IS CSP EXPOSURE ?

Occurrence of attack

SMS Fraud & Security

Unapproved business
- A2P Grey routes
- Bypass

Fraudsters
- SMSishing
- Marketing SPAM
- Spoofing subscribers
- Faking SMSC

Signalling Security

Criminals
- Subscriber Tracking
- Surveillance
- Call/SMS Interception

State Actors
- VIP Tracking/monitoring
- Disinformation
- Cyber Warfare

Complexity of attack

SIGNALING SECURITY ACROSS INTERCONNECT

FS.11
SS7 Security

FS.19
Diameter Security

FS.36
5G Interconnect Security

FS.20
GTP-C Security

ROAMING INTERCONNECT ARCHITECTURE

MSC/VLR

GMLC

SGSN

SGW

MME

SS7

Diameter

GTP

HTTP2

STP/**DEA**/**BGW**/**SEPP**

VPLMN

SS7/IPX/GRX carrier

STP/**DEA**/**BGW**/**SEPP**

HPLMN/MVNO

HLR/HSS

gsmSCF

SMSC

IN

GGSN/PGW

IMS/PCC

SS7

Diameter

GTP

HTTP2
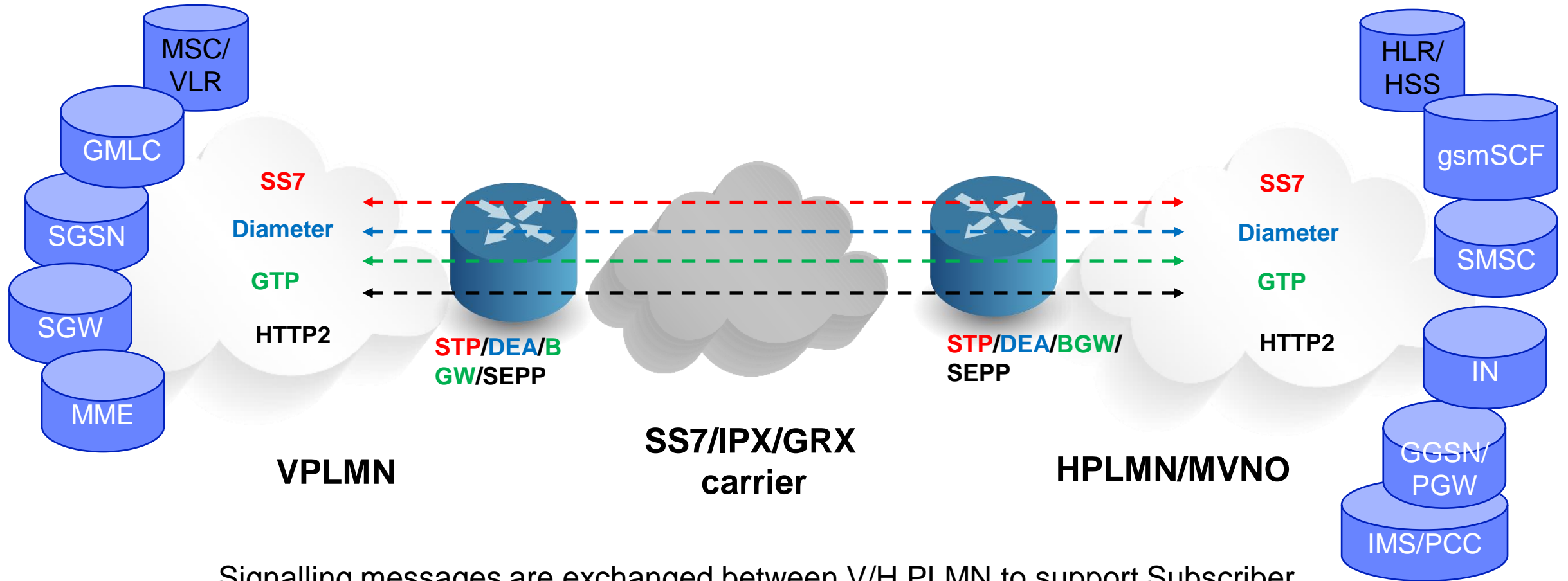
Signalling messages are exchanged between V/H PLMN to support Subscriber Roaming/Voice/SMS/Data…..**Hackers inject messages to exploit weaknesses**

WHO SENDS ILLEGAL MESSAGES?

1. We focus on signalling in telecoms.

2. Signalling security helps identify what attackers are trying to do.

3. We go "upstream" from the attacker's perspective.

ATTACKER'S ANALOGY

Adversaries are:

- Sophisticated and armed with new techniques

- Well informed and intelligent

- Well paid and funded

- Well connected and grouped

How much do we know about them?

- Keep trying approach

- Access to community documents and groups

- Expert in protocols standards

- Aware that most operators use a more tick box security approach and are not enabled with intelligence

- Mobile Operator's don't investigate into unknowns

Groups of Attackers

1. Script Kiddies

- Small number of badly-formed messages
- **Confused with broken equipment**
- Send multiple messages to the same test SIMs
- Often send after work hours

2. Grey Operators

- A2P grey route / SRI-SM location and IMSI checking
- **Mass messages** / bulk business
- Static ranges – some movement of specific GTs
- Focus on **Home Routing bypass** techniques

3. Surveillance Companies

- **Well-funded**
- Centrally co-ordinated across 10-20 GTs
- Use the same software
- Lease A2P GTs
- Creative encoding methods
- **Move their service provider groups around the world**

Groups of Attackers

4. State Actors
- Static, **country-based** GTs
- More standard messages

5. Criminal Service Organizations
- Specific fraud attacks for **online banking**
- Account takeover (2FA) hijack attacks
- Public / dark web websites

6. Security Audit Companies
- **Good guys!**
- Static GTs
- Use their own software stacks
- **Highly innovative attacks** – often copied by others

7. DoS Agents
- Aim to **bring down** networks
- Being tested recently
- Successful in bringing down Network element.

ROLE OF CYBER ATTACKS IN ARMED CONFLICTS

TRUST IS NOT A CYBERSECURITY STRATEGY

WHY CYBER WARFARE PLAYS A KEY ROLE IN ARMED CONFLICTS?

Espionage : Monitoring other countries to steal state secrets.

Sabotage : Hostile governments or terrorists may steal information, destroy it.

D/DoS : Prevent users from accessing legitimate service.

Electrical Grid : Attacking the power grid allows attackers to disable critical systems.
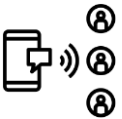
Propaganda : Attempts to control the minds and thoughts of people living in or fighting for a target country

Economic Disruptions : Attacking financial institutions.

Historical Outlook to politically motivated Cyberattacks?

Nation state a phenomenon existed in past.

Target	Attack	Attribution
Estonia 2007	DDoS attacks on online services of banks, media outlets, and government bodies	Russia (state-sponsored groups)
Georgia 2008	Combined cyber and kinetic attack DDoS attacks on Georgian government websites, i.e. the president's website	Russia (state-sponsored groups)
Iran 2010	The Stuxnet worm attacked numerous centrifuges in Iran's Natanz uranium enrichment facility and caused physical destruction on the equipment controlled by the infected computers	The US and Israel (state actors)
WannaCry 2017	Ransomware attacks brought down numerous computer systems worldwide	North Korea (state-sponsored groups)
NotPetya 2017	Ransomware attacks brought down numerous computer systems worldwide	Russia (state-sponsored groups)

"THE MISSED INTEL"

"U.S" withdrawal from "AF"

TIMELINE OF U.S. WITHDRAWAL FROM AFGHANISTAN – REFLECTION

A geopolitical conflict leads to patterns captured on the global threat landscape which can provides useful insights on these developing situations.

Trump Strikes a Deal

Feb. 29, 2020 — U.S. and Taliban sign an <u>agreement</u> that sets the terms for a U.S. withdrawal from Afghanistan by May 1, 2021,

The US Exit: Views From Afghanistan's Civil Society

With Biden's announced timeline for full U.S. withdrawal, there's a looming question of failed promises in Afghanistan.

By **Ritu Mahendru** and **Inshah Malik**
April 17, 2021

https://thediplomat.com/2021/04/the-us-exit-the-view-from-afghanistan/

Biden Follows Through

April 14 ,2021— Saying it is "time to end the forever war," Biden announces that all troops will be removed from Afghanistan by Sept. 11.

https://www.factcheck.org/2021/08/timeline-of-u-s-withdrawal-from-afghanistan/

U.S. WITHDRAWAL FROM AFGHANISTAN – A GLIMPSE OF INTELLIGENCE

Key Artifacts:

- Afghanistan was never prime target based on historical investigations.
- Malicious activities started to appear in Feb 2021 due to the political shifts and administrative changes.
- The threat actor behind these operation are nefariously known and potentially have links to Nation state.
- Supported by a few other unresolved sources with the same origin.
- These sources were clustered.
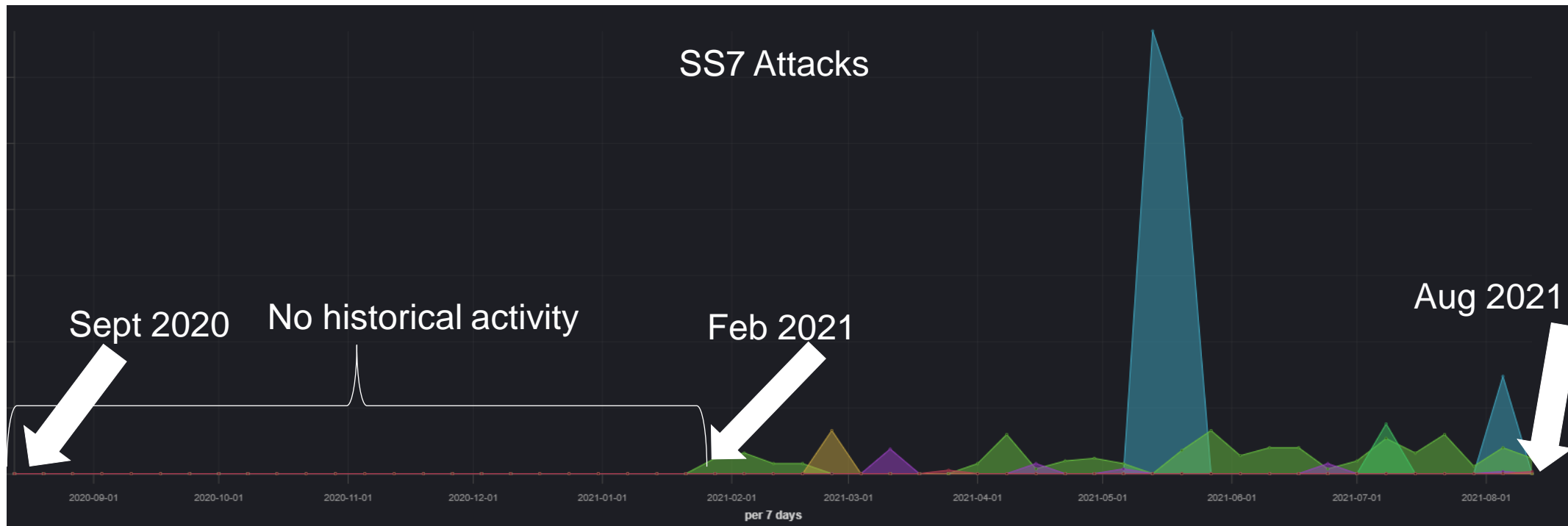
U.S. WITHDRAWAL FROM AFGHANISTAN – MOTIVE & TARGETS

Targets

- Prime targets : AF
- Secondary targets : Roamers in AF (Few from NATO Countries)

Potential victim Organization could be:
- News and Media
- NGO's
- Government Institutions

SS7 Attacks
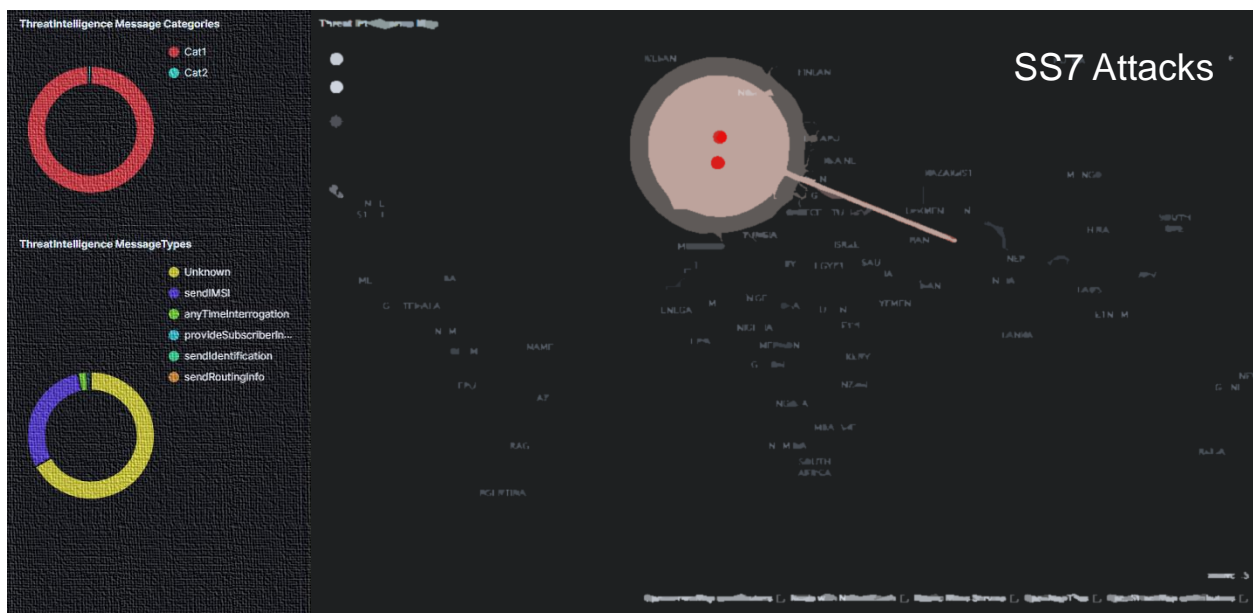
Motive

- IMSI Gathering and Network discovery
- Users Surveillance and tracking
- Potential communication interception at radio level.

Threat Indicators

- Bypass security controls (If any)

POLITICAL SHIFT IN A REGION CAN DRIVE CYBER-ATTACKS!

IS "UA" – "RU" CONFLICT ANY DIFFERENT THAN "AF".

Russia hacked Ukrainian satellite communications, officials believe

🕐 25 March 2022

Russia-Ukraine war

REUTERS

Russia hacked Ukrainian satellite communications, officials believe - BBC News

Ukraine war: Major internet provider suffers cyber-attack

🕐 28 March 2022

Russia-Ukraine war

GETTY IMAGES
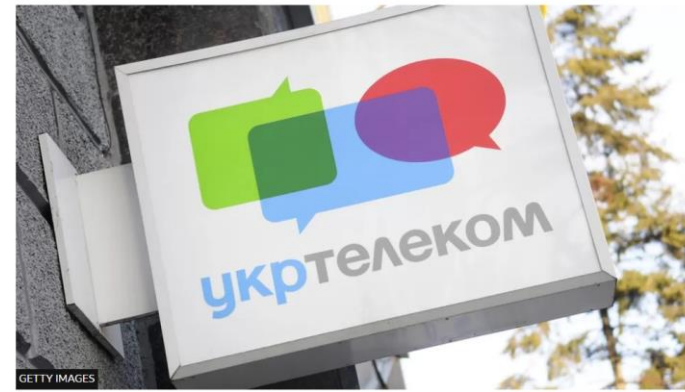
Ukrtelecom is geographically the biggest fixed internet provider in Ukraine

Ukraine war: Major internet provider suffers cyber-attack - BBC News

**Russia-linked cyberattacks on Ukraine
A timeline**

- **Organized and coordinated.**
- **Consistent and motivated.**
- **Intel sharing is the key.**
- **Centrally monitored (NATO)**

Does Telecom industry have a concrete intel sharing framework?

Russia's war on Ukraine: Timeline of cyber-attacks (europa.eu)
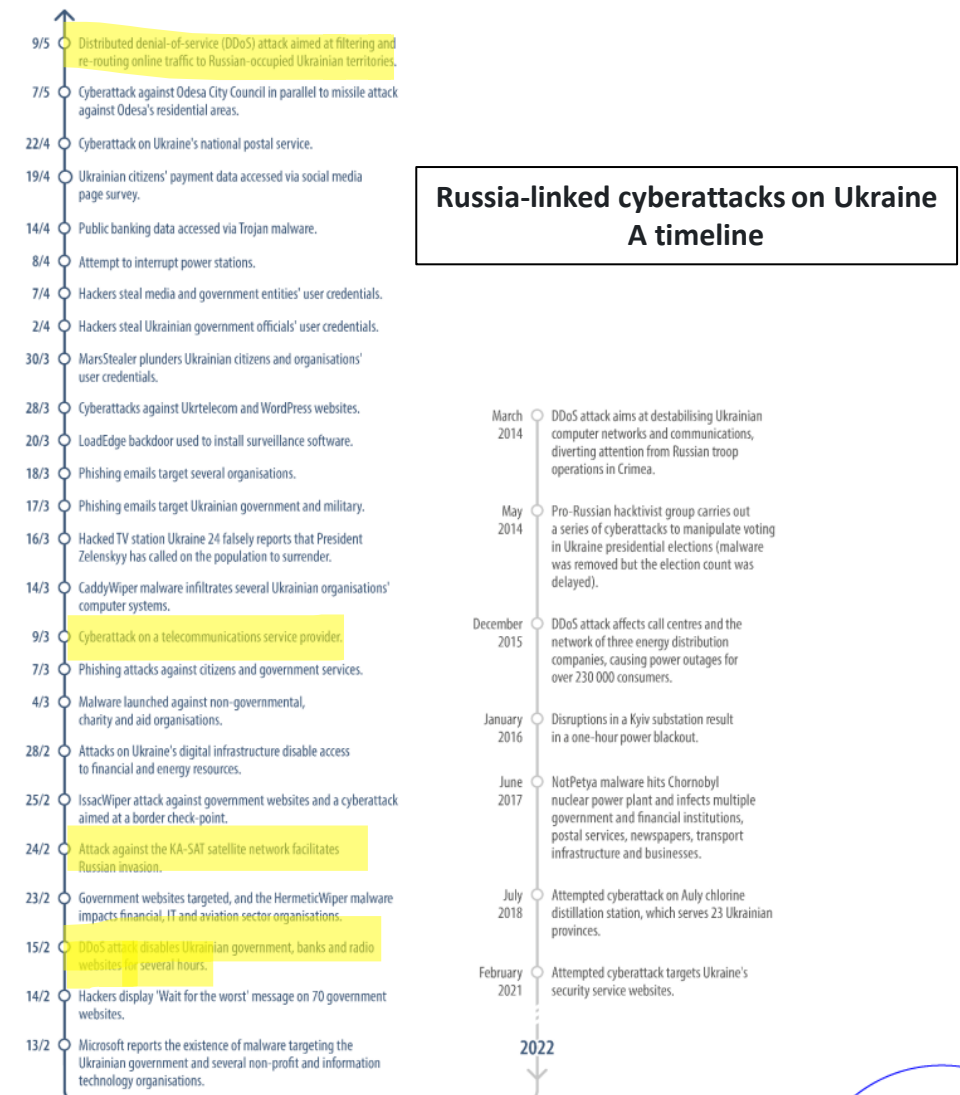
UNDERSTANDING RUSSIAN SIGNALLING ACTIVITIES

In 2022, Russia sources intensified the activities by up to **150 times** comparing to 2020/21 historical records.

SS7 Attacks

Low activity in 2020/21

High activity in 2022
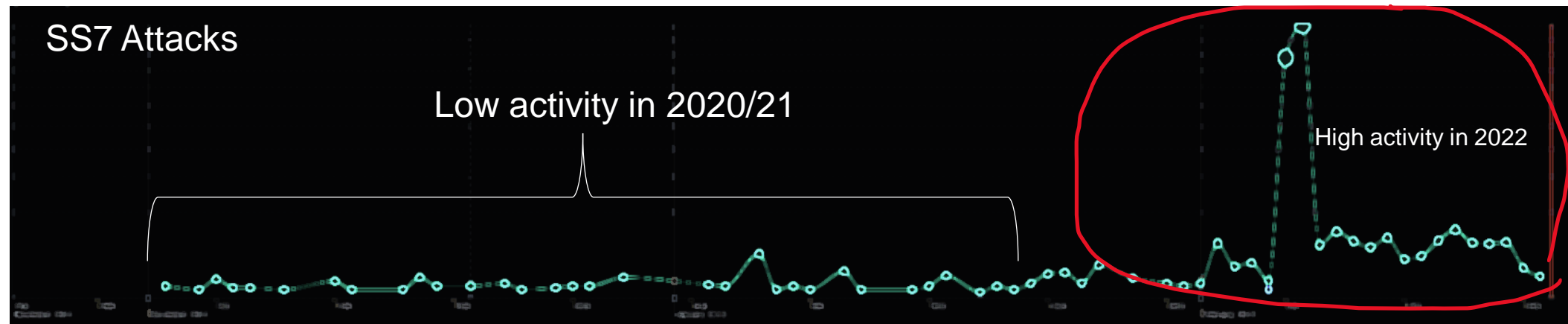
- These activities were supported by malicious threat indicators known to potentially bypass security controls.
- Known techniques listed in the FS.11 few others not available in the guidelines.
- Key fact "fuzzing executed targeting various networks."

UNDERSTANDING THE "RU" BACKED STATE ACTORS

Key behavioural characteristics and threat landscape

- Is Ukraine and NATO countries on the only target = NO
- Attack Intensity = High
- Coverage = Extreme
- Current state = Active
- Targeting inbound roamers in NATO countries
- Clustered group
- Zero-day exploit = Observed (CVD Submission)
- Identity Impersonation
- Identity spoofing
- Fuzzing
- 60+ countries were targeted.

SS7 Attacks
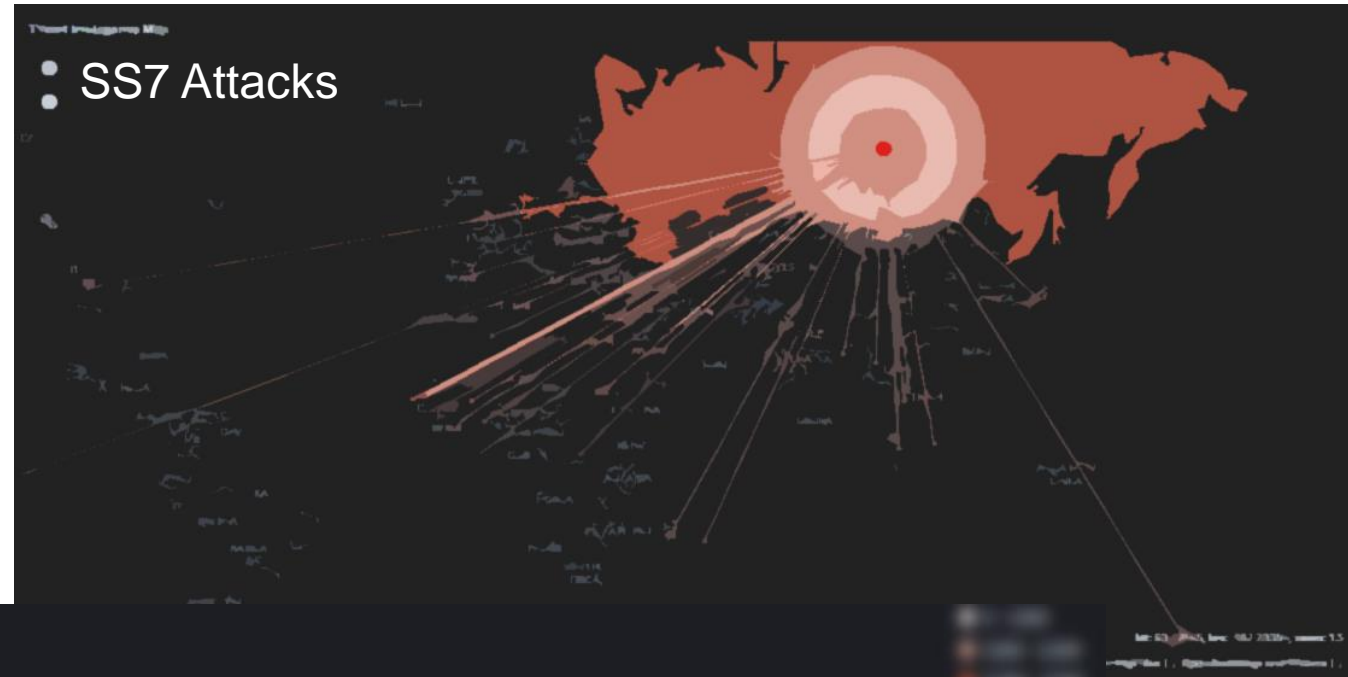
ARE THESE "APT'S", GOVERNMENT-BACKED ATTACKERS?

Russian attackers aggressively pursue wartime advantage in cyberspace using global signalling.

Threat Intelligence team has uncovered set of attacks targeted towards Ukrainian and NATO countries with following objectives

Attacks Involved	Unresolved Russian Origins	Targeted Nations
Network Discovery	Mapping the network topologies through scanning	• Ukraine • NATO Countries • Middle east • Africa
Information gathering	IMSI extractions and profile extractions.	
Location tracking	Performing surveillance on targeted victims.	
Hostile registrations	Hostile location updates made to potentially intercept the comms.	
Account takeover	Social media accounts taken over.	
Fraud	Financial fraud observed several other cases.	

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – RECON AND TARGETED SCANNING

Massive scale scan to discover and map networks.

Multiple networks and countries were scanned. Sequential network identifiers.

Sequential and incremental session ID

No.	Time	Protocol	Length	Calling Party Digits	Transaction Id	SubSy	Called Party Digits	SubSy	info	opCode	application-context-name
271	202...	TCAP	166		30	MSC...	37	HLR...	Begin otid(	30)	shortMsgGatewayContext-v3
272	202...	TCAP	166		30	MSC...	37	HLR...	Begin otid(	30)	shortMsgGatewayContext-v3
273	202...	TCAP	166		31	MSC...	46	HLR...	Begin otid(	31)	shortMsgGatewayContext-v3
274	202...	TCAP	166		31	MSC...	46	HLR...	Begin otid(	31)	shortMsgGatewayContext-v3
275	202...	TCAP	166		32	MSC...	52	HLR...	Begin otid(	32)	shortMsgGatewayContext-v3
276	202...	TCAP	166		32	MSC...	52	HLR...	Begin otid(	32)	shortMsgGatewayContext-v3
277	202...	TCAP	166		33	MSC...	54	HLR...	Begin otid(	33)	shortMsgGatewayContext-v3
278	202...	TCAP	166		33	MSC...	54	HLR...	Begin otid(	33)	shortMsgGatewayContext-v3
279	202...	TCAP	166		34	MSC...	95	HLR...	Begin otid(	34)	shortMsgGatewayContext-v3
280	202...	TCAP	166		34	MSC...	95	HLR...	Begin otid(	34)	shortMsgGatewayContext-v3
281	202...	TCAP	166		35	MSC...	10	HLR...	Begin otid(	35)	shortMsgGatewayContext-v3
282	202...	TCAP	166		35	MSC...	10	HLR...	Begin otid(	35)	shortMsgGatewayContext-v3
307	202...	TCAP	166		40	MSC...	39	HLR...	Begin otid(	40)	shortMsgGatewayContext-v3
308	202...	TCAP	166		41	MSC...	53	HLR...	Begin otid(	41)	shortMsgGatewayContext-v3
311	202...	TCAP	166		42	MSC...	61	HLR...	Begin otid(	42)	shortMsgGatewayContext-v3
310	202...	TCAP	166		43	MSC...	26	HLR...	Begin otid(	43)	shortMsgGatewayContext-v3
309	202...	TCAP	166		44	MSC...	53	HLR...	Begin otid(	44)	shortMsgGatewayContext-v3
312	202...	TCAP	166		45	MSC...	04	HLR...	Begin otid(	45)	shortMsgGatewayContext-v3
313	202...	TCAP	166		46	MSC...	83	HLR...	Begin otid(	46)	shortMsgGatewayContext-v3
314	202...	TCAP	166		47	MSC...	76	HLR...	Begin otid(	47)	shortMsgGatewayContext-v3
283	202...	TCAP	166		48	MSC...	07	HLR...	Begin otid(	48)	shortMsgGatewayContext-v3
284	202...	TCAP	166		48	MSC...	07	HLR...	Begin otid(	48)	shortMsgGatewayContext-v3
285	202...	TCAP	166		49	MSC...	04	HLR...	Begin otid(	49)	shortMsgGatewayContext-v3
286	202...	TCAP	166		49	MSC...	04	HLR...	Begin otid(	49)	shortMsgGatewayContext-v3

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – IDENTITY IMPERSONATION

Identity impersonation for social application through account takeover.

No.	Time	Protocol	Length	Calling Party Digits	Trans	SubSy	Called Party Digits	SubSy	info	opCode	application-context-name	localValue
232	202…	GSM MAP	198	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue	infoRetrievalContext-v3	sendAuthenticationInfo
233	202…	GSM MAP	198	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue	infoRetrievalContext-v3	sendAuthenticationInfo
234	202…	GSM MAP	218	7	19…	VLR…	2	HLR…	invoke updateLocation	localValue	networkLocUpContext-v3	updateLocation
235	202…	GSM MAP	218	7	19…	VLR…	2	HLR…	invoke updateLocation	localValue	networkLocUpContext-v3	updateLocation
238	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue	networkLocUpContext-v3	insertSubscriberData
239	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue	networkLocUpContext-v3	insertSubscriberData
240	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
241	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
244	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
245	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
250	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue		insertSubscriberData
251	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue		insertSubscriberData
256	202…	GSM SMS	354	2	16…	MSC…	7	MSC…	invoke forwardSM	localValue	shortMsgMT-RelayContext-v2	mo-forwardSM
257	202…	GSM SMS	354	2	16…	MSC…	7	MSC…	invoke forwardSM	localValue	shortMsgMT-RelayContext-v2	mo-forwardSM

Hostile Registration

Home network shares user profile to malicious source

2FA token access

```
∨ TP-Originating-Address - (INFOSMS)
      Length: 13 address digits
      1... .... = Extension: No extension
      .101 .... = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)
      .... 0000 = Numbering plan: Unknown (0)
      TP-OA Digits: INFOSMS
  > TP-PID: 0
  > TP-DCS: 0
  > TP-Service-Centre-Time-Stamp
      TP-User-Data-Length: (152) depends on Data-Coding-Scheme
```

Rebtel

Get a new PIN

Make sure your phone number is correct

+44781234567890

Send me a new PIN

Back to Log in

Using a landline?
We can call you instead

Rebtel

Call the World

Experience premium-quality international calling

Where do you want to call?   Search

Popular destinations 🇨🇺 Cuba 🇮🇳 India 🇳🇬 Nigeria
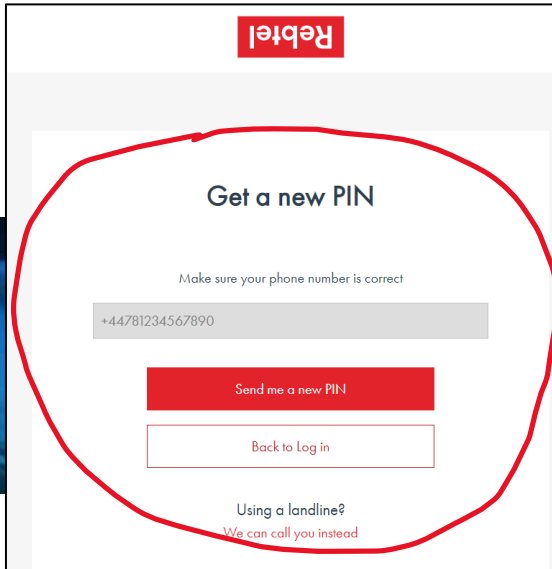
- Social Application account takeover
- Input Required : Phone number
- Not linked to email.

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – IDENTITY SPOOFING

How we back our statement that these are nation backed activities.

No.	Time	Protocol	Length	Calling Party Digits	Tran:	Message Type	SubSy:	Called Party Digits	SubSys:	info	opCode	application-context-name	localValue
1	202…	GSM SMS	283	3	00…	Unitdata	MSC …		MSC …	invoke forwardSM	localValue		mo-forwardSM

SCCP layer Spoofed Identity

Spoofed E.164 numbering plan doesn't belong to any of Operators that owns these low layer identities

```
∨ Message Transfer Part Level 3
  > Service information octet
  ∨ Routing label
    > .... .... .... .... ..01 0110 0101 0011 = DPC:
    ∨ .... 1000 0011 0011 11.. .... .... .... = OPC:
        Signalling Area Network Code (SANC): Afghanistan       Low layer Spoofed Identity
        Unique Signalling Point Name:
        Signalling Point Operator Name:
      0000 .... .... .... .... .... .... .... = Signalling Link Selector: 0
```

```
∨ Message Transfer Part Level 3
  > Service information octet
  ∨ Routing label
    > .... .... .... .... ..10 1111 0000 1011 = DPC:
    ∨ .... 1000 0111 1000 01.. .... .... .... = OPC:
        Signalling Area Network Code (SANC): United Arab Emirates    Low layer Spoofed Identity
        Unique Signalling Point Name:
        Signalling Point Operator Name:
      0000 .... .... .... .... .... .... .... = Signalling Link Selector: 0
```

Link Level analysis revealed traffic initiated via Russian operator

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – ZERO-DAY EXPLOITS

How we back our statement that these are nation backed activities.

No.	Time	Protocol	Length	Calling Party Digits	Transaction Id	SubSy	Called Party Digits	SubSy	info	opCode	application-context-name
404	202…	TCAP	166	▬▬▬▬▬		MSC…		HLR…	Begin otid( )		shortMsgGatewayContext-v2.0

No.	Time	Protocol	Length	Calling Party Digits	Transaction Id	SubSy	Called Party Digits	SubSy	info	opCode	application-context-name
468	202…	TCAP	166 7			MSC…		MSC…	Begin otid( )		shortMsgMT-RelayContext-v2.0

Application Context with additional sub-identifier

```
∨ Transaction Capabilities Application Part
  ∨ begin
      [Transaction Id:      ]
    ∨ Source Transaction ID
        otid:
        oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    ∨ dialogueRequest
        Padding: 7
      ∨ protocol-version: 80
          1... .... = version1: True
          application-context-name: 0.4.0.0.1.0.20.2.0 (shortMsgGatewayContext-v2.0)
        components: 1 item
∨ GSM Mobile Application
  ∨ Component: invoke (1)
    ∨ invoke
        invokeID: -1
      ∨ opCode: localValue (0)
          localValue: sendRoutingInfoForSM (45)
      ∨ msisdn:
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x1)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
        ∨ E.164 number (MSISDN):
            Country Code:
          sm-RP-PRI: False
      ∨ serviceCentreAddress:
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x1)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
        ∨ E.164 number (MSISDN):
            Country Code:
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090                    08 04 00 00
00a0  01 00 14 02 00    02 01 2d
00b0
00c0
```

In this vulnerability, the offending source includes an additional sub-identifier in the object identifier field. The last octet represents the additional sub identifier.

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – ZERO-DAY EXPLOITS

In this incident, the offending source attempted hostile registration using standalone SendAuthenticationInfo (SAI) targeted towards multiple operators with the use of TCAP transaction ID of length 8 octets. While investigation revealed portion of the vulnerable networks responded to these improperly composed MAP Invoke..

TCAP transaction ID length

In this vulnerability, the offending source use of TCAP transaction ID of length 8 octets to perform hostile registration.


```
∨ Transaction Capabilities Application Part
  ∨ begin
       [Transaction Id: 3937313830344230]
     ∨ Source Transaction ID
         otid: 3937313830344230
       oid: 0.0.17.773.1.1.1 (id-as-dialogue)
     ∨ dialogueRequest
         application-context-name: 0.4.0.0.1.0.14.3 (infoRetrievalContext-v3)
       components: 1 item
∨ GSM Mobile Application
  ∨ Component: invoke (1)
     ∨ invoke
         invokeID: 2
       ∨ opCode: localValue (0)
           localValue: sendAuthenticationInfo (56)
         IMSI:
       ∨ [Association IMSI:
           Mobile Country Code (MCC):
           Mobile Network Code (MNC):
         numberOfRequestedVectors: 1
         immediateResponsePreferred
         requestingNodeType: vlr (0)
```

```
0000
0010
0020
0030
0040
0050
0060
0070
0080    08 39 37 31 38 30 34  42 30
0090
00a0
00b0
00c0
```
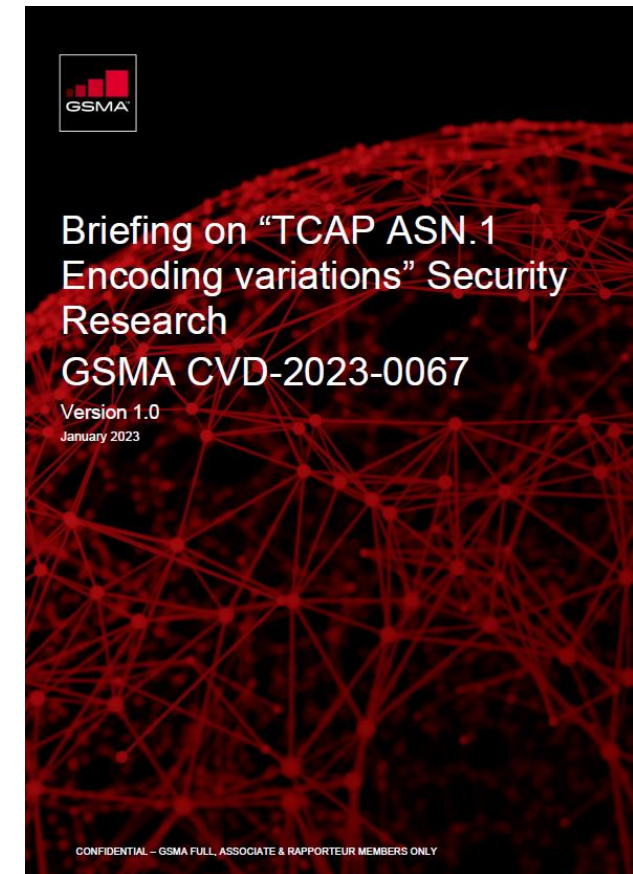
RESPONSIBLE VULNERABILITY DISCLOSURE

Coordinated Vulnerability Disclosure

- Briefing paper released.

Actions towards Mobile Operators

- Mobile Operators are requested to reproduce this vulnerability in their labs.

"THE FINANCIAL IMPACT"

Financial loss towards operators for zero-day exploit!

The Mobileum Threat Intelligence team discovered a new vulnerability back in early April 2021

General Details	
Operator(s)	Unknown
Date of Threat	2021/03/31- 2021/04/01
Date of Reporting	2021-04-09
Threat Originating Network	SCCP Calling GT prefixes: Unknown:
Threat Originating Node(s)	SCCP Calling GTs: Unknown:
Protocol	SS7, MAP, SMS
Messages	PDU_SS7_MAP_sendRoutingInfoForSM , PDU_SS7_MAP_mo-forwardSM, PDU_SS7_MAP_mt-forwardSM

A global operator group reported a fraud incident between April and Nov 2021 that exploited that vulnerability

FRAUD INCIDENT: DETAILS	
Dates of fraud incident/s:	April to November 2021
Estimated Loss in US$:	$48K in 12 days
How fraud committed. Method of fraud – what did they do? Attached diagrams on separate page if required.	An ___ affiliate was victim of SMS Firewall Bypass where the fraudsters manipulated the SMS signaling while hiding behind a leased GT. The SMS signaling manipulation allowed the SRI-for-SM message to be routed directly to the HLR instead of the SMS Firewall and involved manipulating the TCAP TAG parameter of this message, a technique previously reported: see CVD-2021-0052.
Details of fraudsters: Any information that may assist another operator to identify the fraudsters	The GT used to commit this fraud was leased from another ___ affiliate on the pretense that it was required by the national police. We don't know if our affiliate received the GT leasing request from fraudsters who impersonated the authorities or from the legitimate authorities.

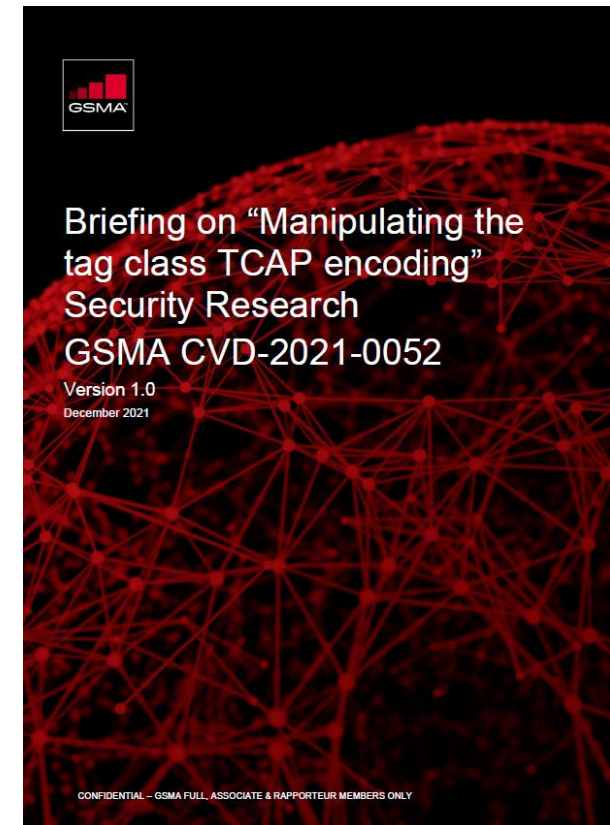**Overall financial impact of this zero-day is not fully known.**
- This can be due to factors like lack of visibility.
- Lack of interest in reporting such incident towards GSMA.

RESPONSIBLE VULNERABILITY DISCLOSURE

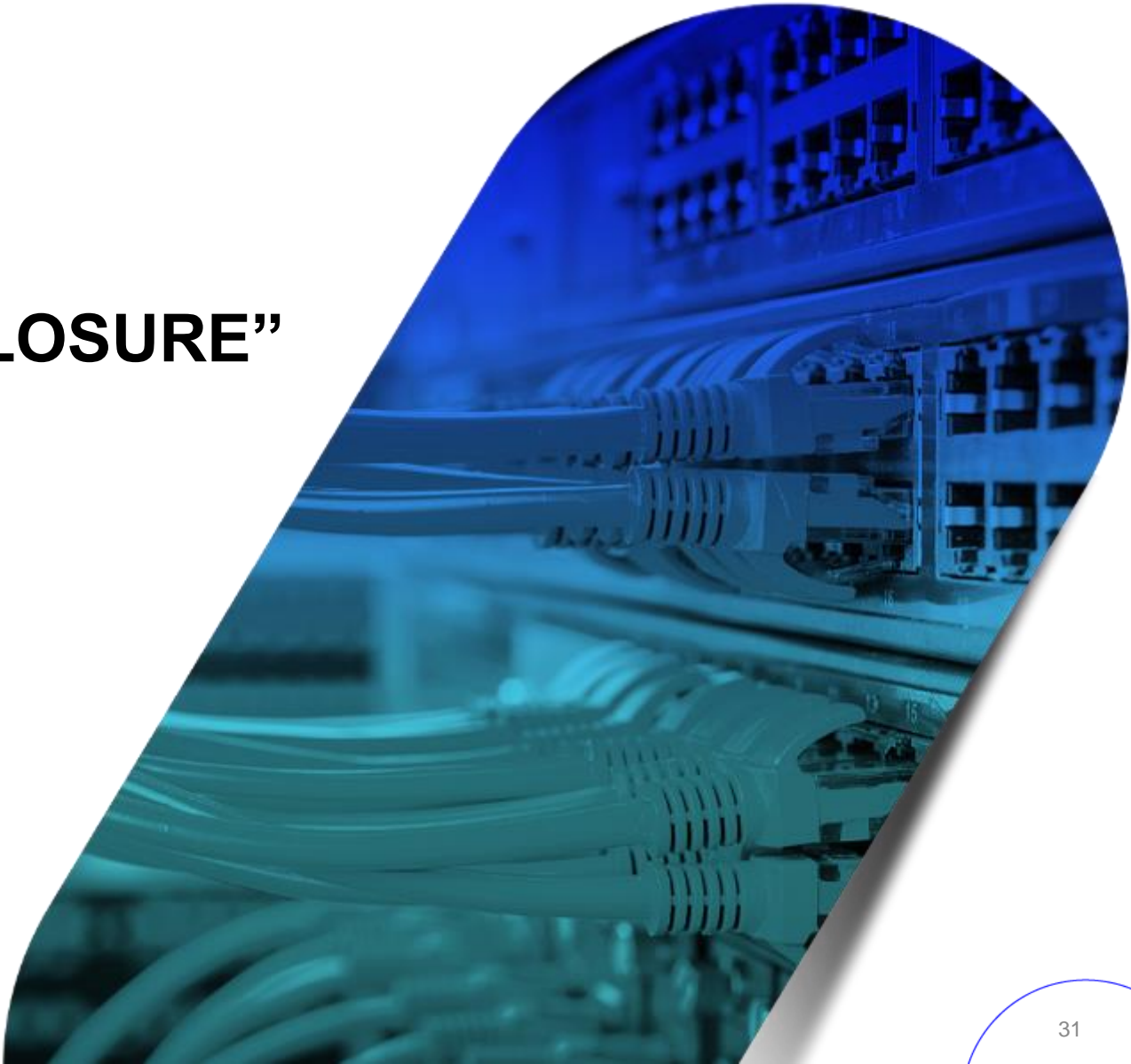**Coordinated Vulnerability Disclosure**

Actions towards Mobile Operators

- Mobile Operators were requested to reproduce this vulnerability in their labs.

- Operators should consider adapting to the global threat intelligence services.

Briefing on "Manipulating the tag class TCAP encoding" Security Research
GSMA CVD-2021-0052
Version 1.0
December 2021

CONFIDENTIAL – GSMA FULL, ASSOCIATE & RAPPORTEUR MEMBERS ONLY

https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements/
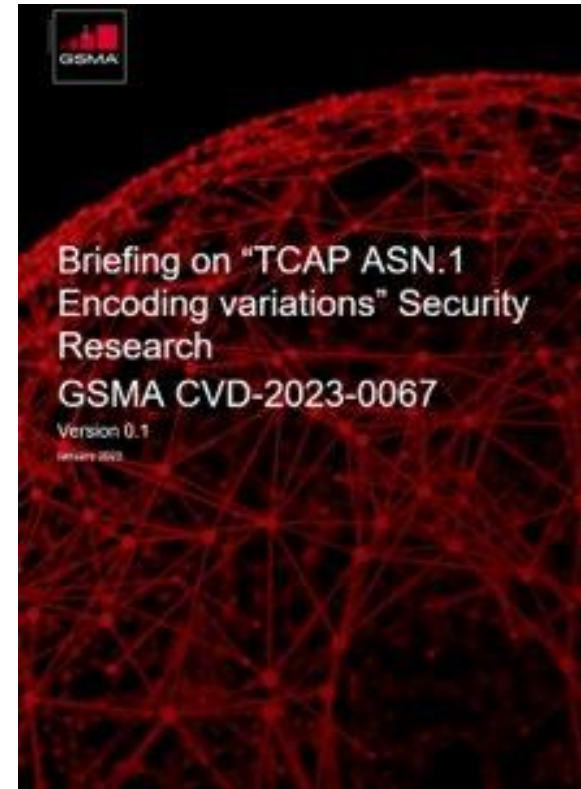
"WORK ETHICS & DISCLOSURE"

WORK ETHICS AND DISCLOSURE

Coordinated Vulnerability Disclosures

- Share key intelligence gathered through security research back to the Industry.

- Share details on zero day exploits that can avoid security breaches and financial losses.

- Objective driven to secure services offered by operators.

Briefing on "TCAP ASN.1 Encoding variations" Security Research
GSMA CVD-2023-0067
Version 0.1

Briefing on "Manipulating the tag class TCAP encoding" Security Research
GSMA CVD-2021-0052
Version 1.0
December 2021

CONFIDENTIAL – GSMA FULL, ASSOCIATE & RAPPORTEUR MEMBERS ONLY

"BLACK HAT SOUND BYTES"

- Industry should learn from enterprise and build a telecom focus intel sharing framework. Like (STIX, TAXI)

- Processes are key to the implementation of an effective cyber-safety strategy to handle cyber conflicts.

- Security guidelines are not a measure of absolute security.

- Operators to enable themselves with a mindset of Global Threat Intelligence

THANK YOU

Q & A