FIGI Security Clinic

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SS7 vulnerabilities and their impact on DFS

Infrastructure Security Workstream

Assaf Klinger, Vaulto

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Our mission

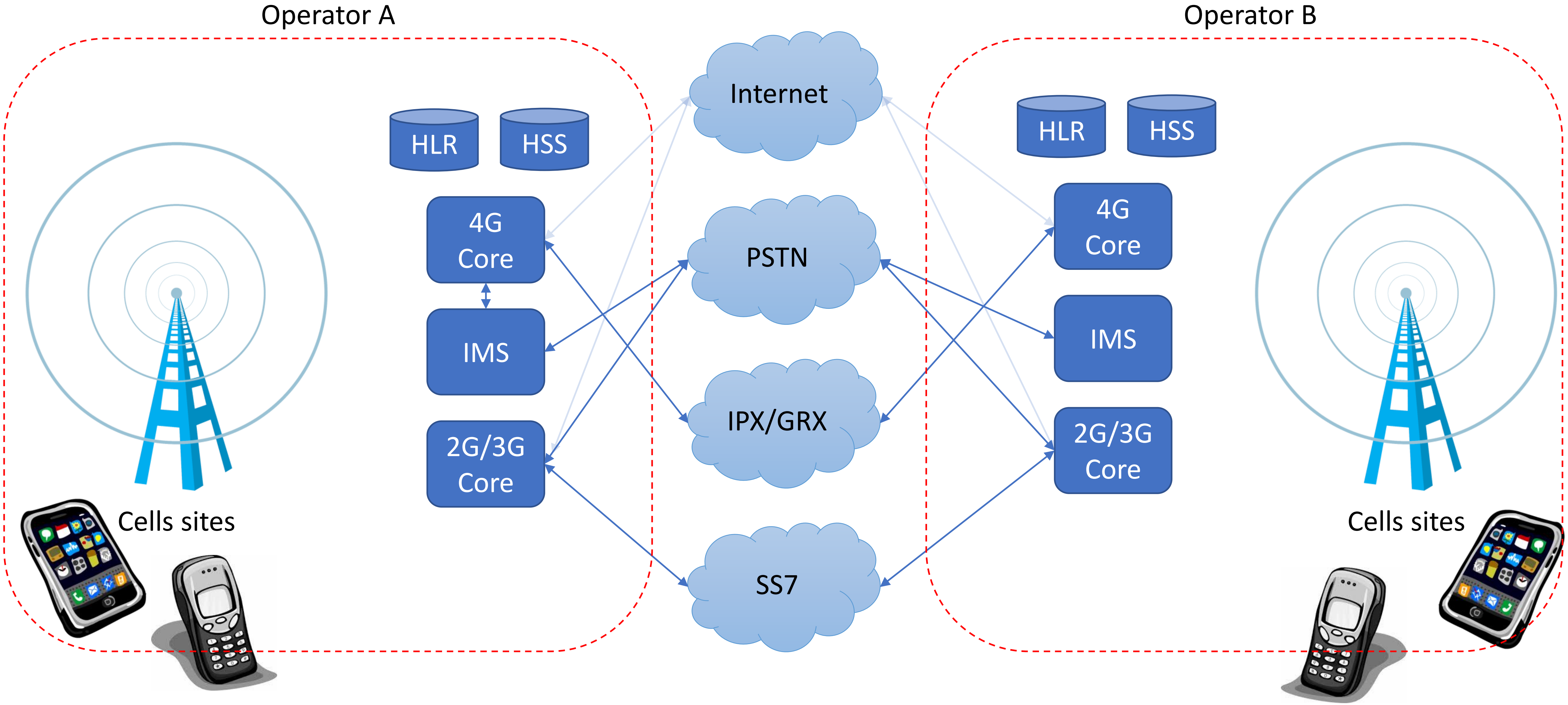
- Analyze the telecom infrastructure for vulnerabilities which enable DFS fraud

- Identify how are these vulnerabilities are exploited in the wild and to what degree

- Recommend mitigation measures for mobile network operators, DFS providers and regulators

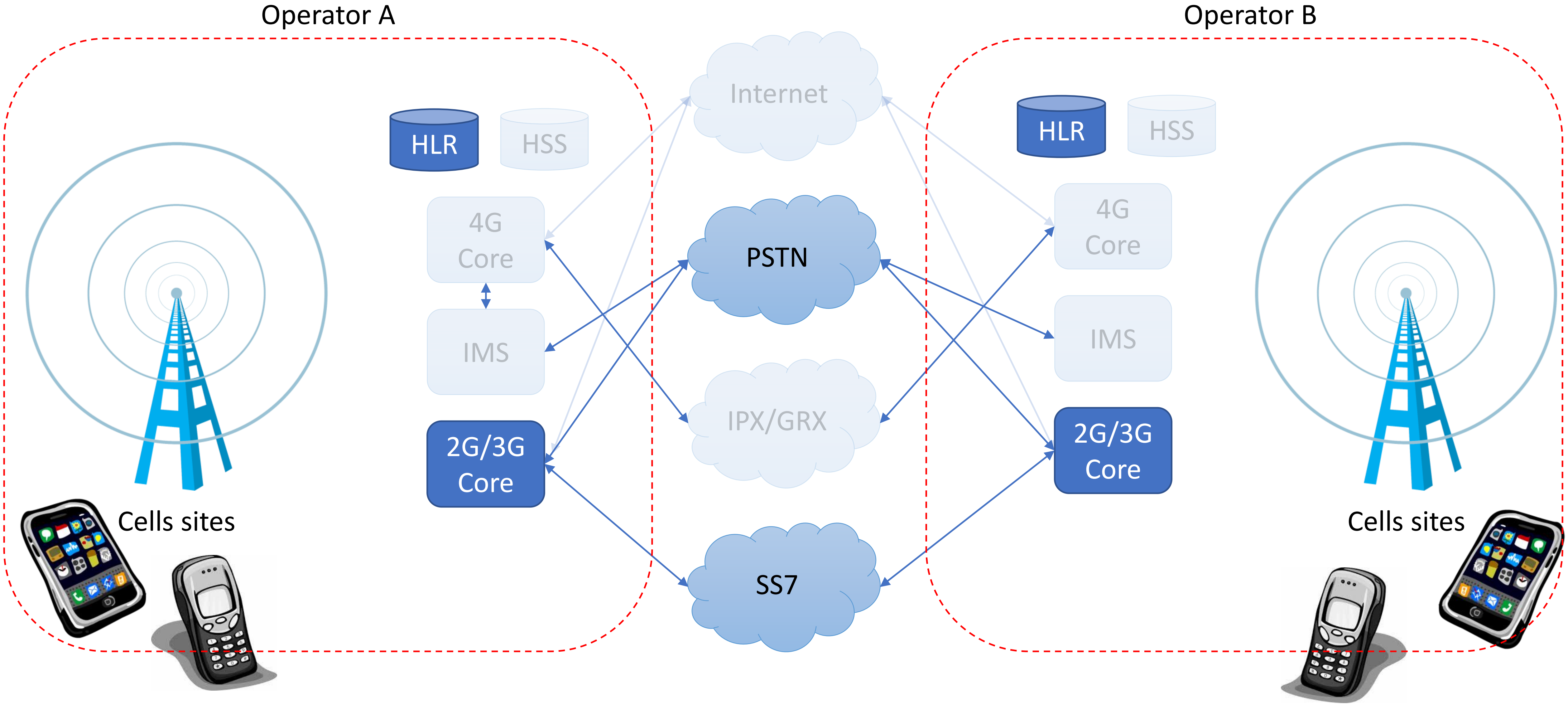
- **Main Output →** [Technical report on SS7 Vulnerabilities and mitigation measures for DFS]()

Our scope

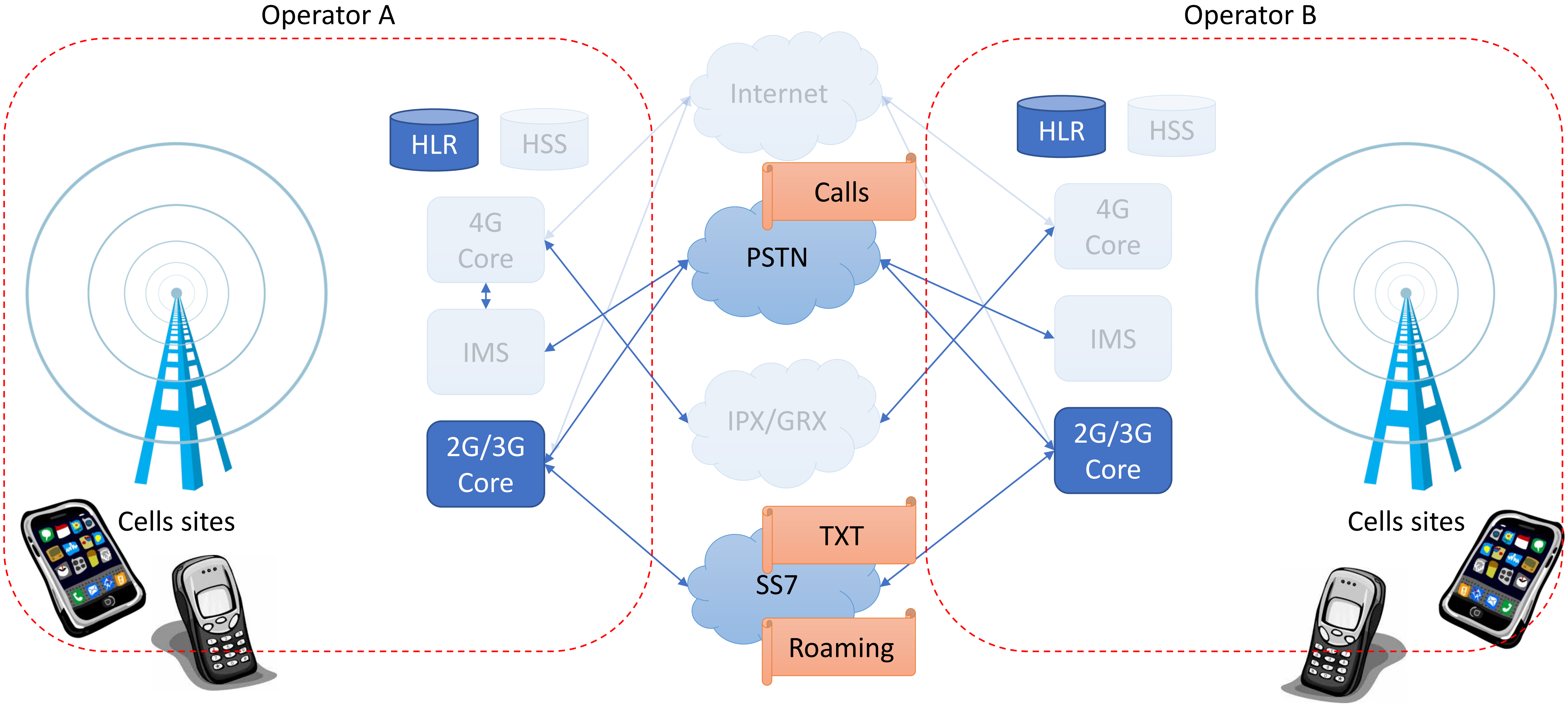


Operator A
Operator B
HLR
HSS
4G Core
IMS
2G/3G Core
Cells sites
Internet
PSTN
IPX/GRX
SS7
HLR
HSS
4G Core
IMS
2G/3G Core
Cells sites

Our scope

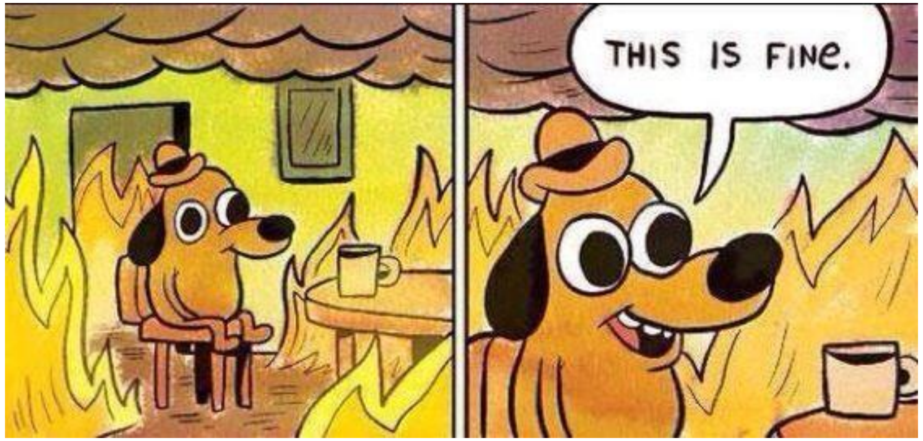

Operator A
Operator B
HLR
HSS
4G Core
IMS
2G/3G Core
Cells sites
Internet
PSTN
IPX/GRX
SS7
HLR
HSS
4G Core
IMS
2G/3G Core
Cells sites

Telecom services over SS7



SS7: vulnerability by design

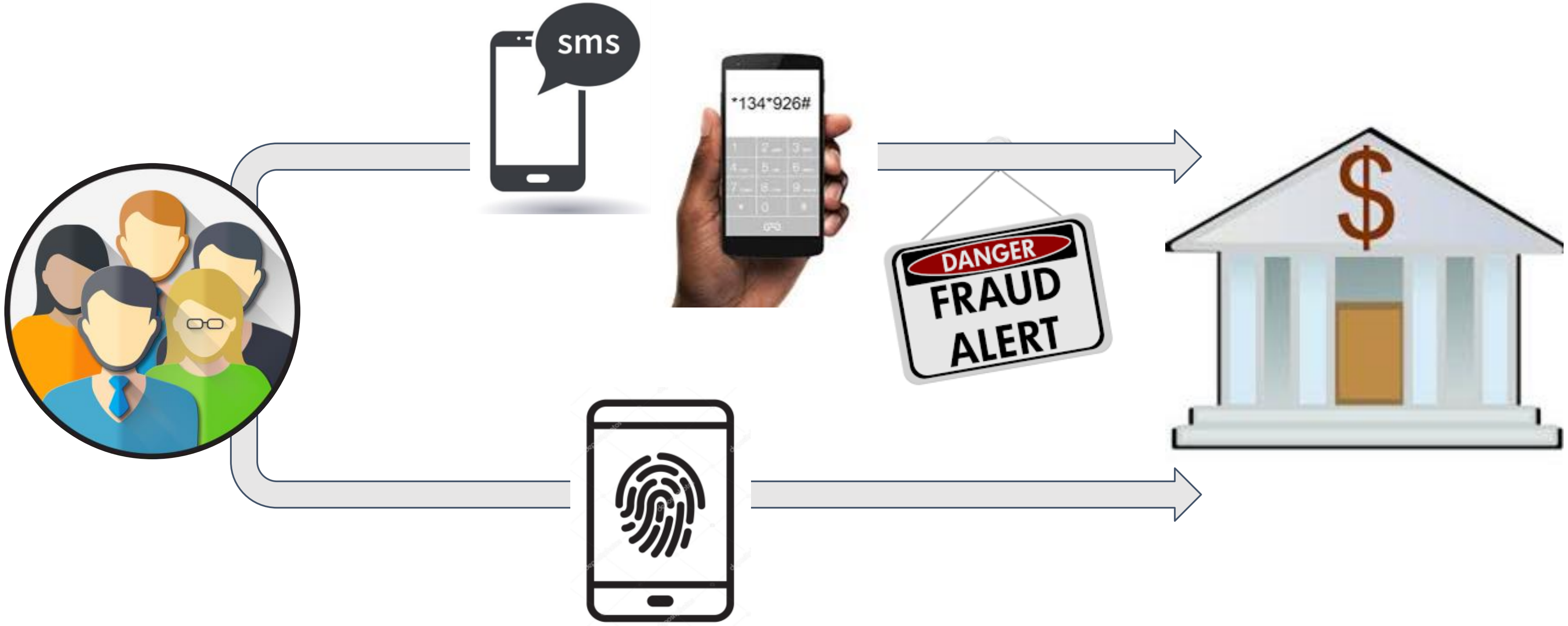
- Flat network (switched, not routed, no NATs)
- Static address allocation (ITU managed)
- All network elements are trusted without question
- No encryption
- No authentication required to join the network



DFS - Digital financial services

- Digital financial services (DFS) relies heavily on the underlying teleco infrastructure to enable users send and receive money
- DFS is very popular in developing countries where traditional banking infrastructure is not present
- The channels in which the end-user communicates with the DFS provider are mostly USSD and SMS, due to the lack of 3G/LTE deployment in these countries.
- According to surveys, less than 30% of the telcos in the European Union (EU) and less than 0.5% of telcos in developing countries have implemented any mitigation measures, despite the existence of such measures.

DFS + Telecom = Fraud?

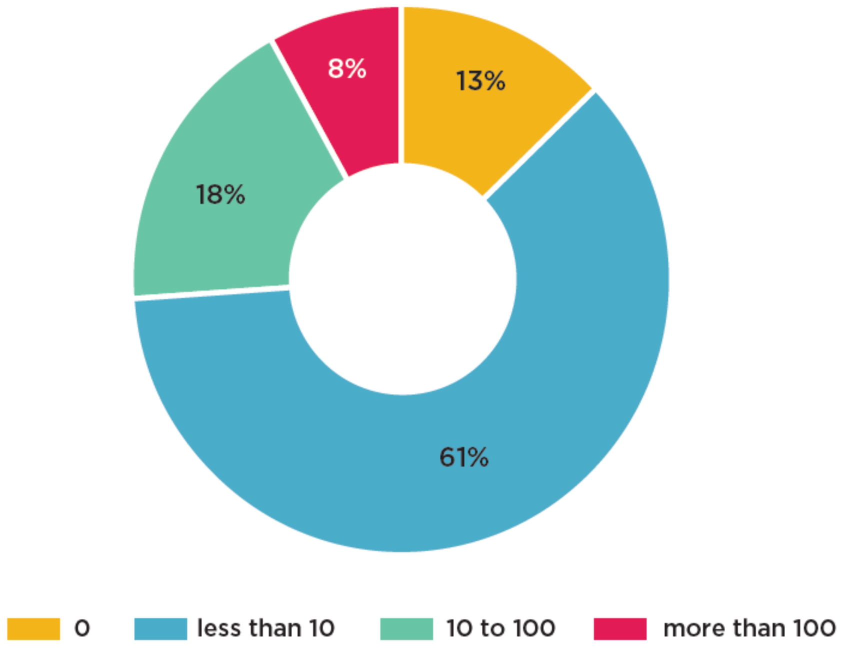


DFS, Telecom & the regulation gap

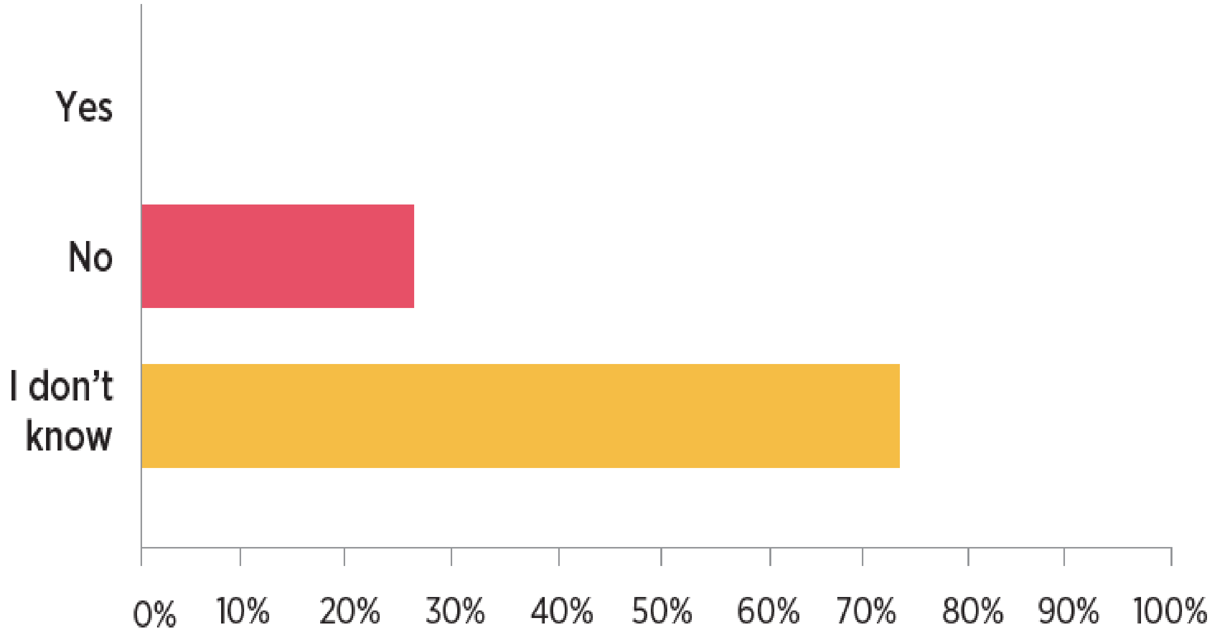
- Legacy technology (over 20yo) still active today – e.g SS7
- Published vulnerabilities still in affect, exploited in the wild for theft
- Telcos are not required to mitigate these vulnerabilities
- Misalignment of regulatory interests

The commonality of Telecom attacks

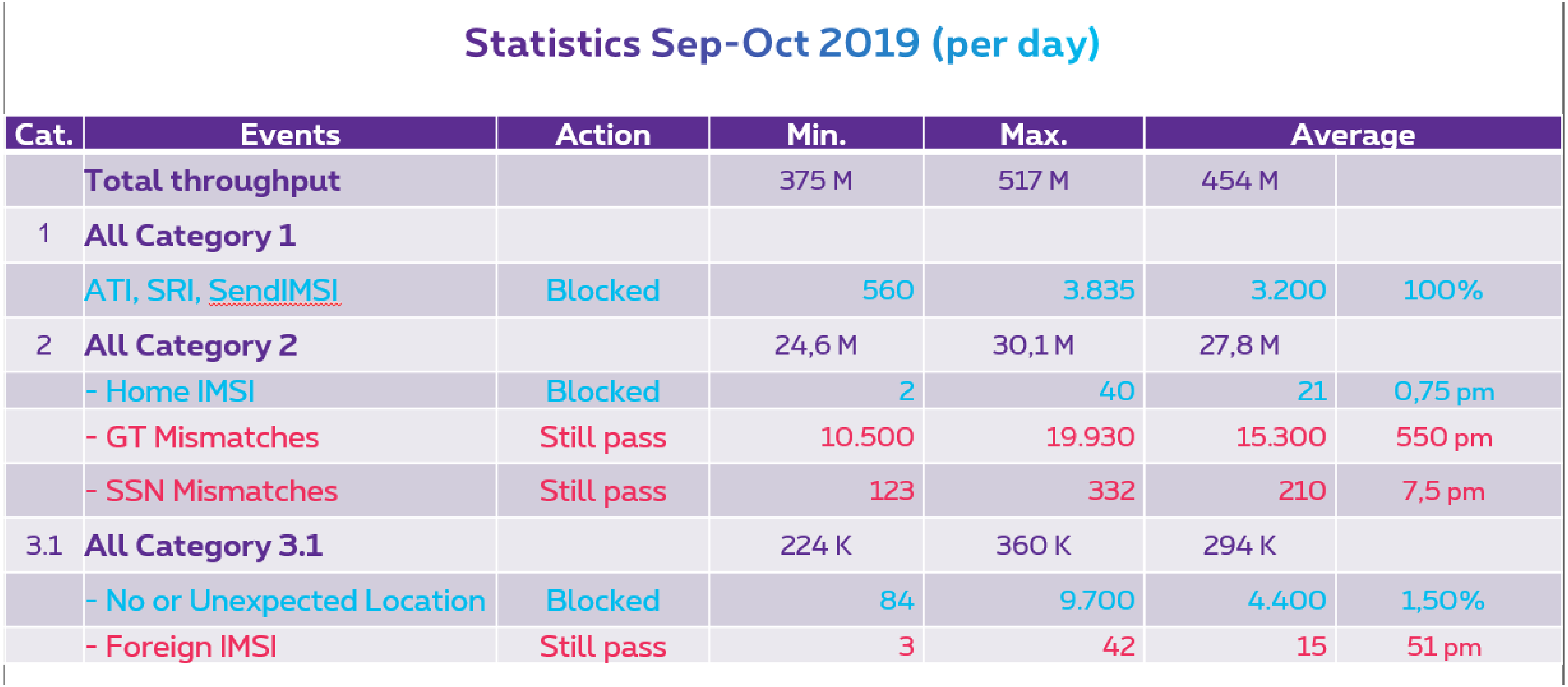
(reported) Frequency of attacks



Awareness to telecom attacks



Example from a major EU operator



Statistics Sep-Oct 2019 (per day)

Cat.	Events	Action	Min.	Max.	Average	
	Total throughput		375 M	517 M	454 M	
1	**All Category 1**					
	ATI, SRI, SendIMSI	Blocked	560	3.835	3.200	100%
2	**All Category 2**		24,6 M	30,1 M	27,8 M	
	- Home IMSI	Blocked	2	40	21	0,75 pm
	- GT Mismatches	Still pass	10.500	19.930	15.300	550 pm
	- SSN Mismatches	Still pass	123	332	210	7,5 pm
3.1	**All Category 3.1**		224 K	360 K	294 K	
	- No or Unexpected Location	Blocked	84	9.700	4.400	1,50%
	- Foreign IMSI	Still pass	3	42	15	51 pm

Major types of telecom attacks on DFS

Caller ID spoofing

2FA account takeover

SIM swap

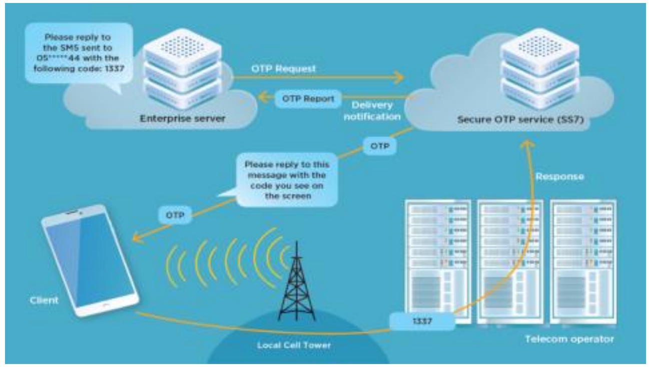
Live demo

2FA account takeover

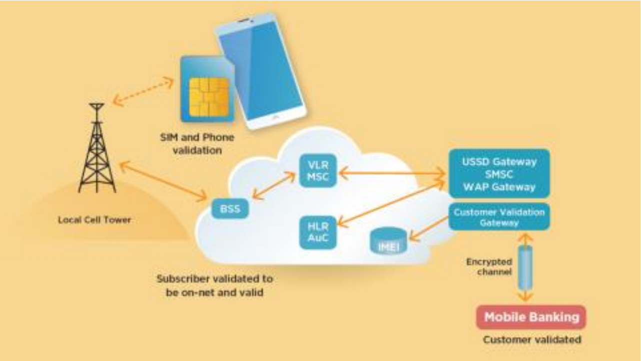
Mitigation Measures

For DFS providers

- Change the direction of 2FA



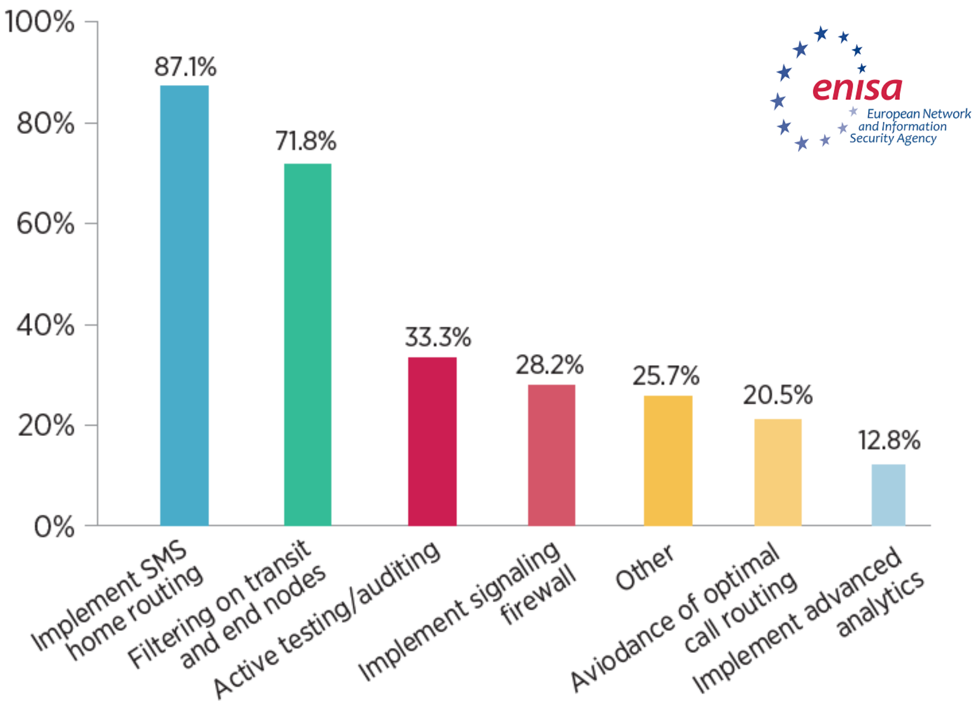
- Use a SIM Validation gateway

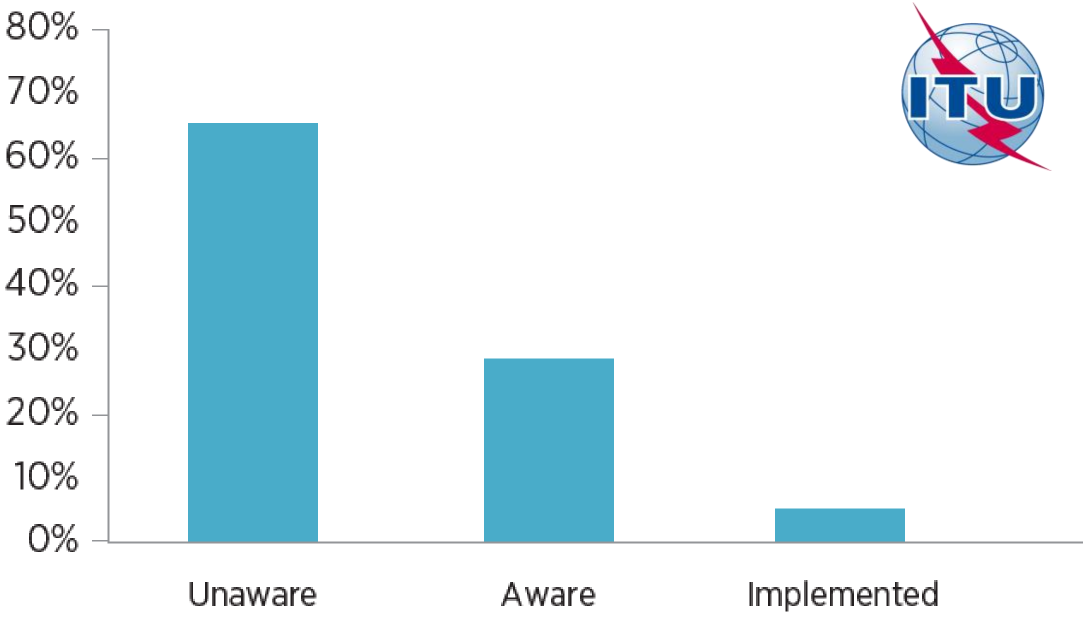


For Operators

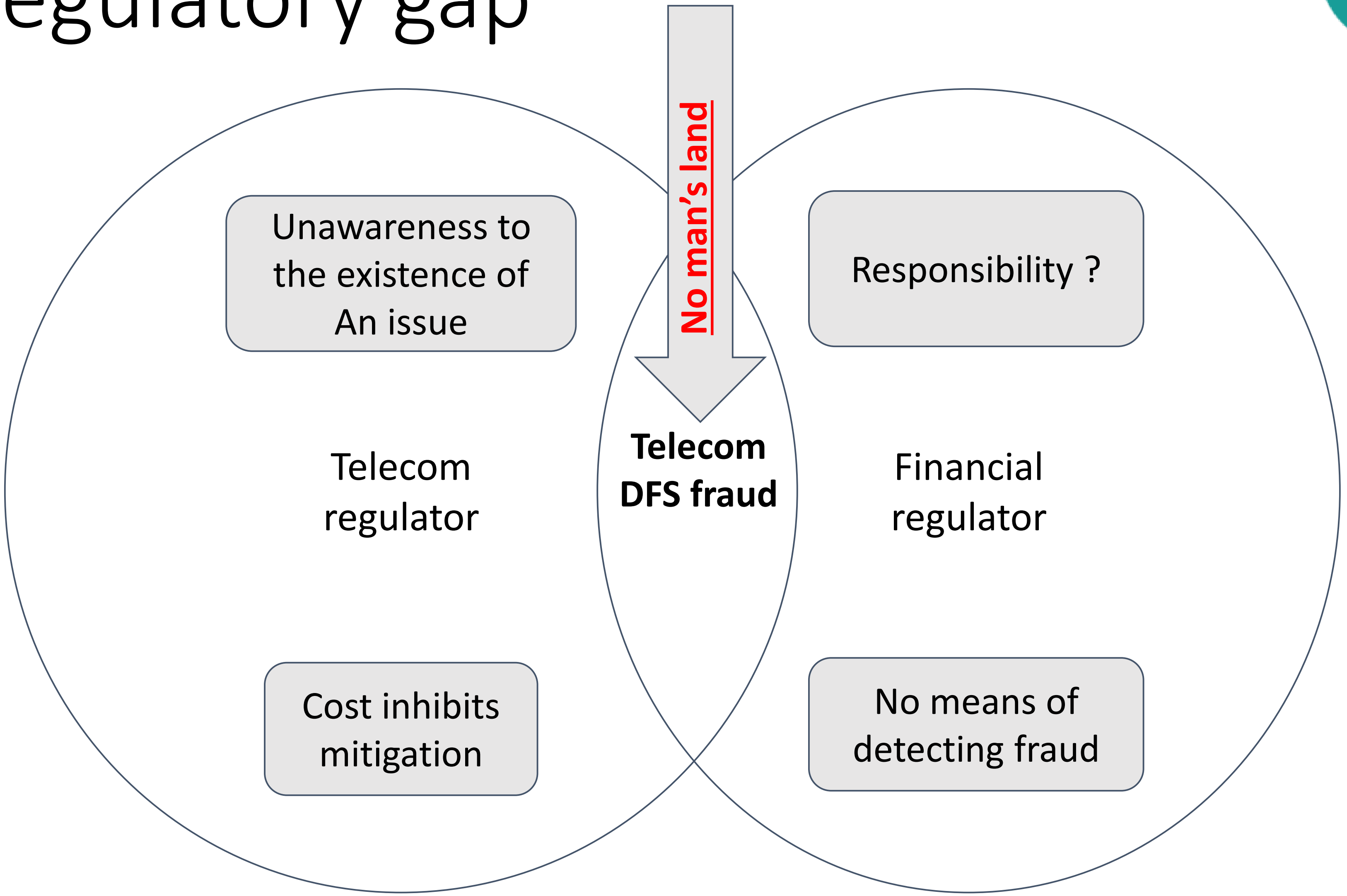
Attack	FS.11 (2/3G)	FS.07 (2/3G)	IR.82 (2/3G)	IR.88 (4G)
Spoofing	✓	✓	✓	×
SMS Hijack	×	✓	×	×
SIM swap	×	✓	✓	✓

Implementation of countermeasures





The regulatory gap



Unawareness to the existence of An issue

Cost inhibits mitigation

Telecom regulator

No man's land

Telecom DFS fraud

Responsibility ?

No means of detecting fraud

Financial regulator

Recommendations

1. Educate
    - Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS
2. Regulate
    - Regulation and legal framework to include measures for signaling security and reporting of such incidents
3. Create a security posture baseline
    - Telecom regulators to establish baseline security measures for each category (3G/4G/5G)
4. Close the regulatory gap by regulatory coordination (financial <-> telecom)
    - bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the central bank.
5. Incentivize the industry
    - create regulation that passes the financial damage from DFS fraud to the DFS providers and to the telcos, creating a financial incentive for action on their part
6. Industry cooperation and incentivization
    - Forums should be created where all commercial actors in the DFS ecosystem meet and interact regularly
    - Establish or promote a platform for security incident data sharing

Implementation

1. Educate → ITU has picked up the glove
   a) This report was adopted by ITU-T Study Group 11 as a technical report
   b) ITU Brainstorming session took place in October 2019 on how to address SS7 vulnerabilities
   c) Tomorrow's security clinics
2. Regulate → this is up to each country to do
   a) Local regulators need to put in place regulation to **mandate** the implementation of countermeasures in the telecos (communication regulators) or in the DFS providers (financial regulators) **and audit** the security posture of each operator / provider
   b) Setup a round table discussion with all local stake holders: DFS, Telcos, Financial and communication regulators

Implementation

3. Incentivize

   a) DFS can implement countermeasures regardless of telco / regulatory action to mitigate fraud and lower the financial damage from fraud

   b) Encourage global grant programs for technological innovation in the field of DFS fraud protection (with regards to SS7 vulnerabilities)

   c) Encourage the deployment of packet data networks (3G / LTE) in rural areas to enable more sophisticated forms of authentication to DFS

Thank you