ITU Workshop on "SS7 Security"
Geneva, Switzerland
29 June 2016

Observations on SS7 Network Security

Pascal Dejardin
Roaming Architect & Solutions Manager,
Orange group, Belgium
pascal.dejardin@orange.com

1956 2016
CCITT / ITU-T

Agenda

- Context
- GSMA categories
- Audits results
- Conclusions

Context

- **Trusted** SS7 network is **broken**
- Abuses:
  - **Tracking** the location
  - **Intercepting** the calls by
  - **Manipulating** the subscribers profile
  - Camping subscribers in **Deny of Services**
  - Popular **Spamming** for fraud revenues
- Standards are not the issue
  but well the **confidence** in the access
- Worst in the coming all-IP world

Orange position

- Active in **GSMA** – IR82 (NG & FASG)
- Leading **audits** (SS7)
- Active vulnerabilities **testing**
- **Protection** with existing nodes
- Market study on **Signalling Firewall**

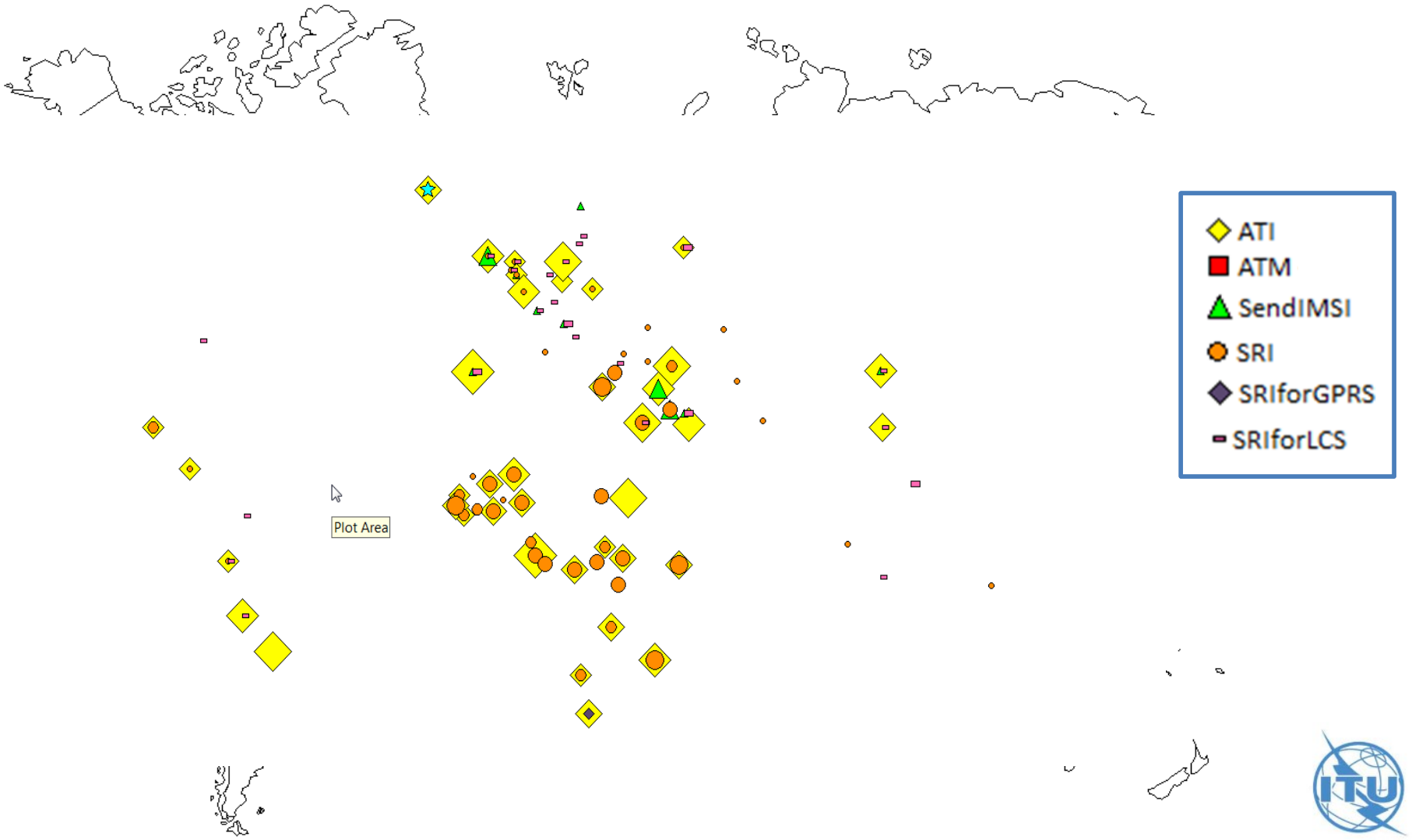
GSMA – IR82

Categories	Classification	Operation Codes	Filters
Cat. 1	Home exclusive	SRI, Send IMSI, ATI,ATM, SP..	Block OpCodes
Cat. 2	Roaming Home>Visited	PSI/L, PRN,CL, ISD, DSD	Check HLR
Cat. 3	Roaming Visited>Home	UL, FwdSM, SAI, RegSS, PrUSS	Check Location
Cat. 4	SMS interconnection	SRI4SM, MT-FwdSM	Home Routing
Cat. 5	Call control >Home	CAMEL IDP	Check SCP

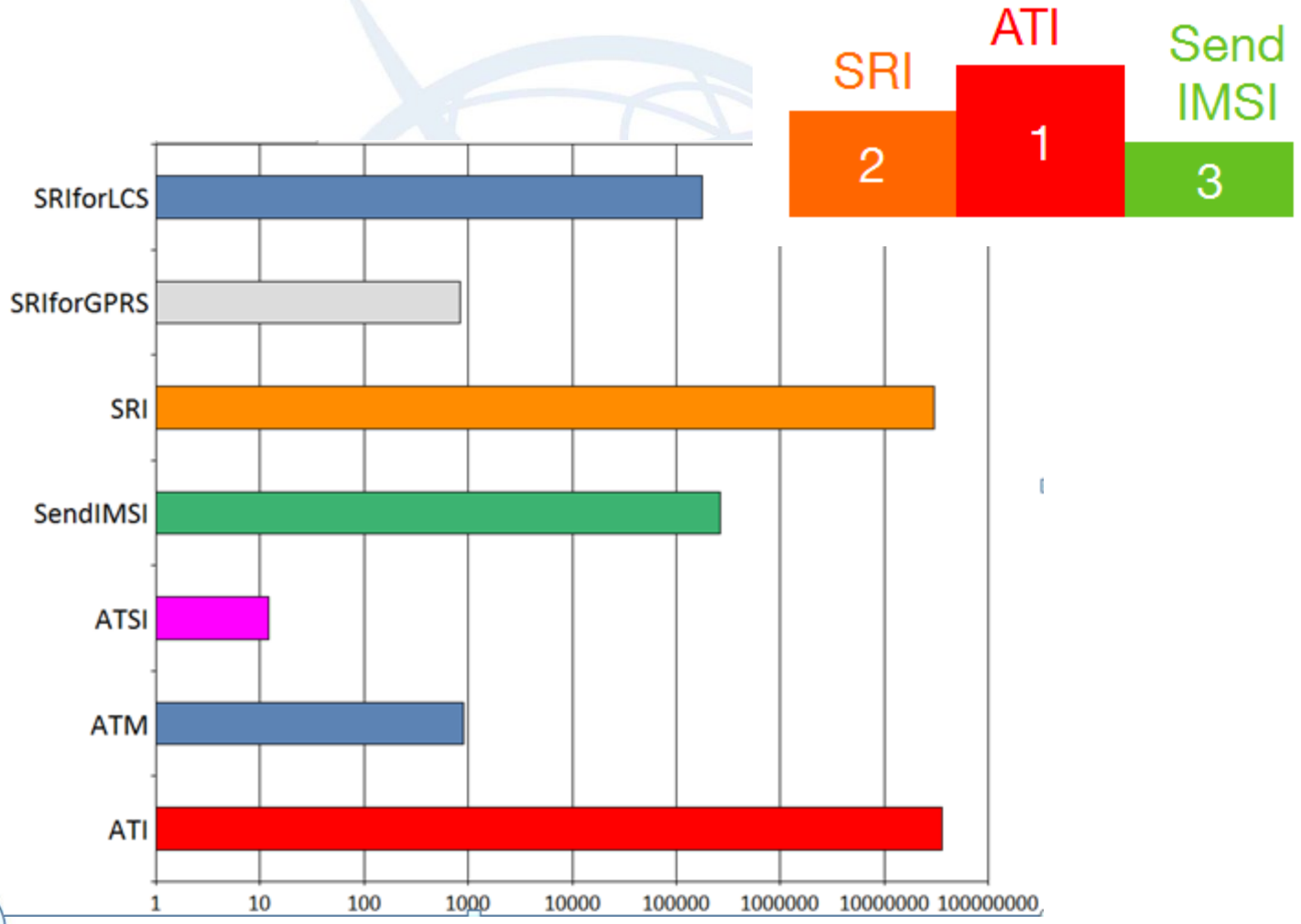
Audits framework

- Orange Carrier
  - Orange International Signalling traffic (in/out)
  - Daily Analysis for 1 year (Mar 2015 > Feb 2016)
  - Enriched with IR21 DB
  - Focus on Orange subscribers only

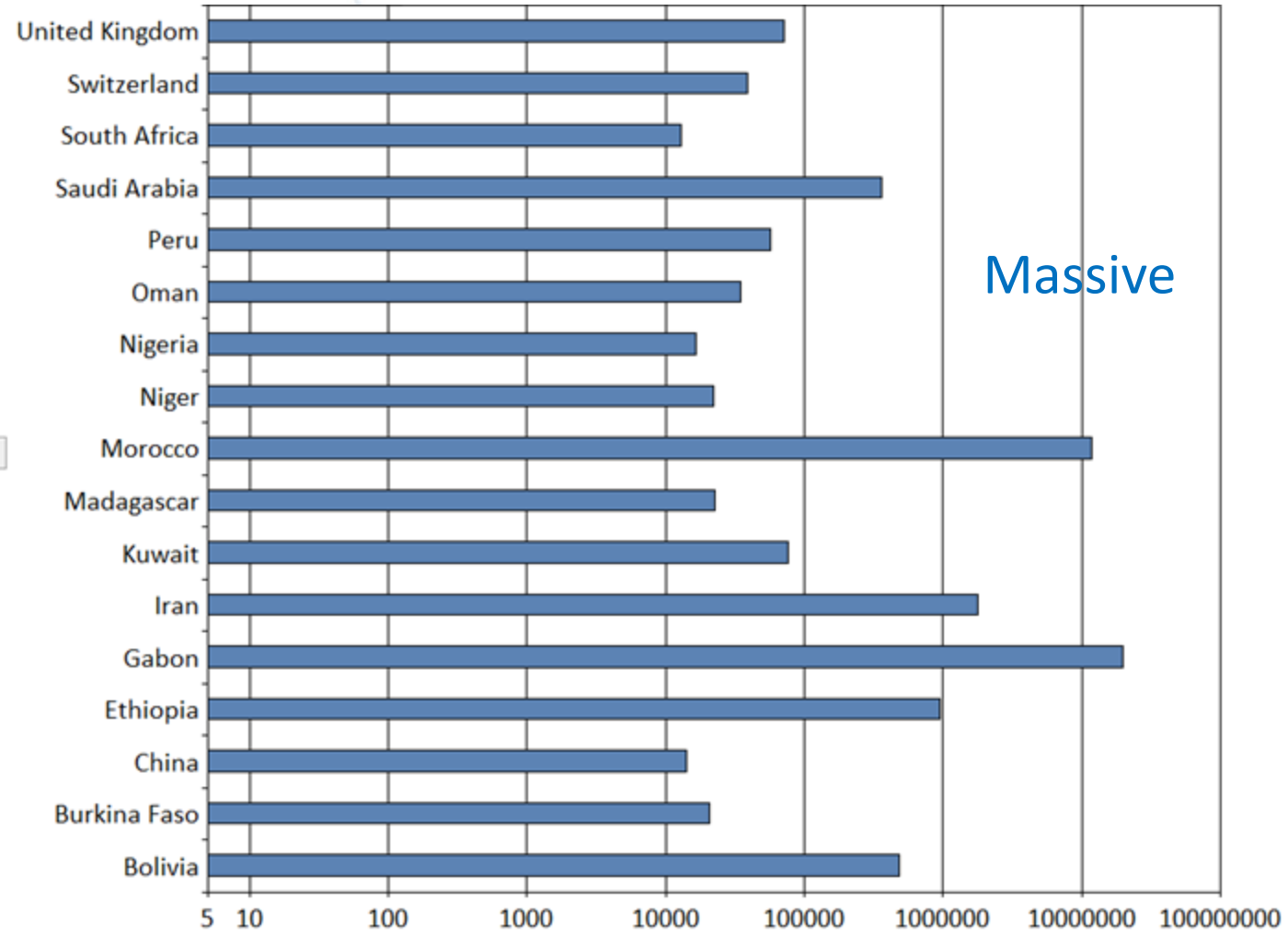
Category 1 – HLR target



Cat 1. Top 3 of HLR attacks

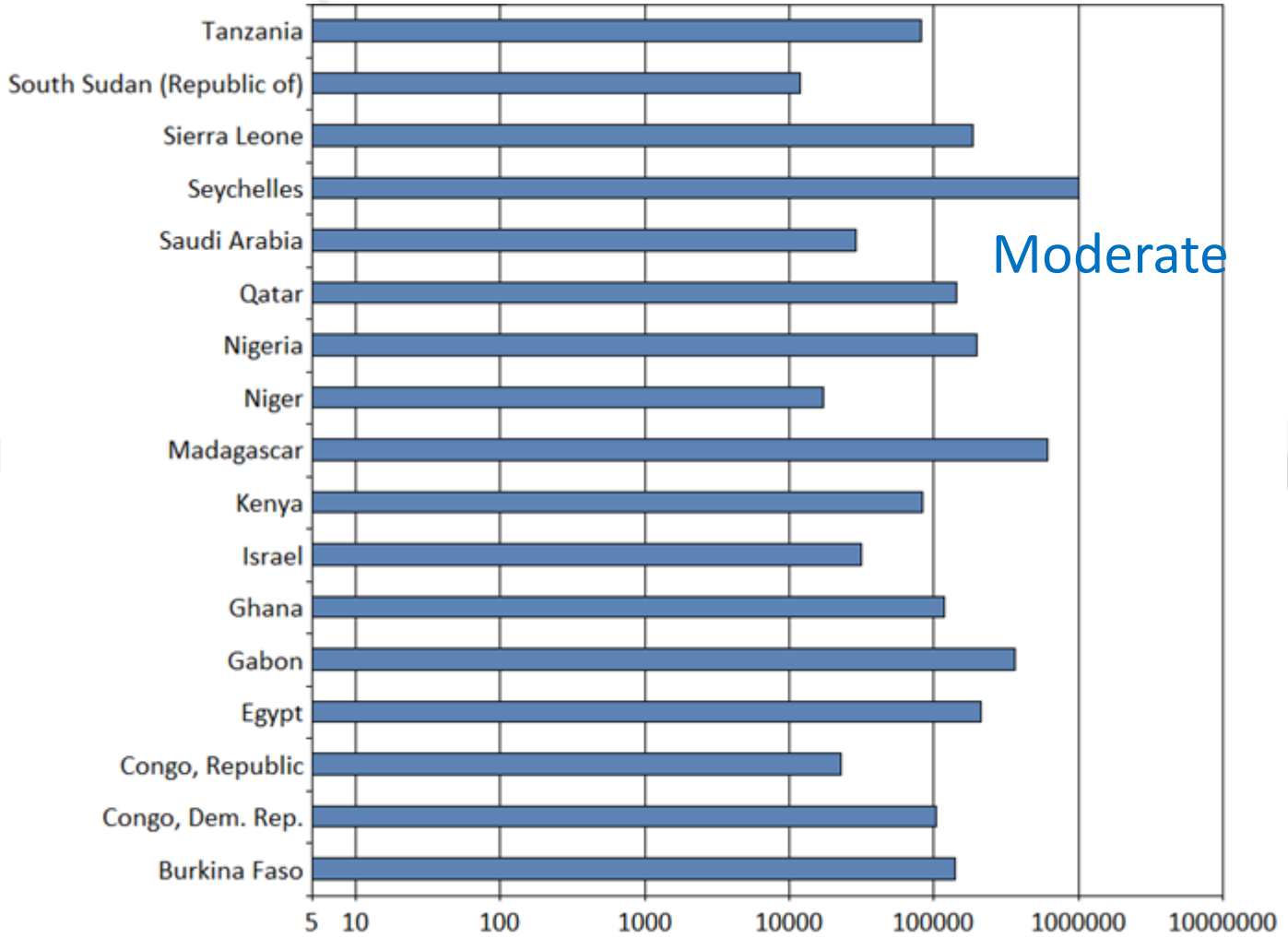


ATI



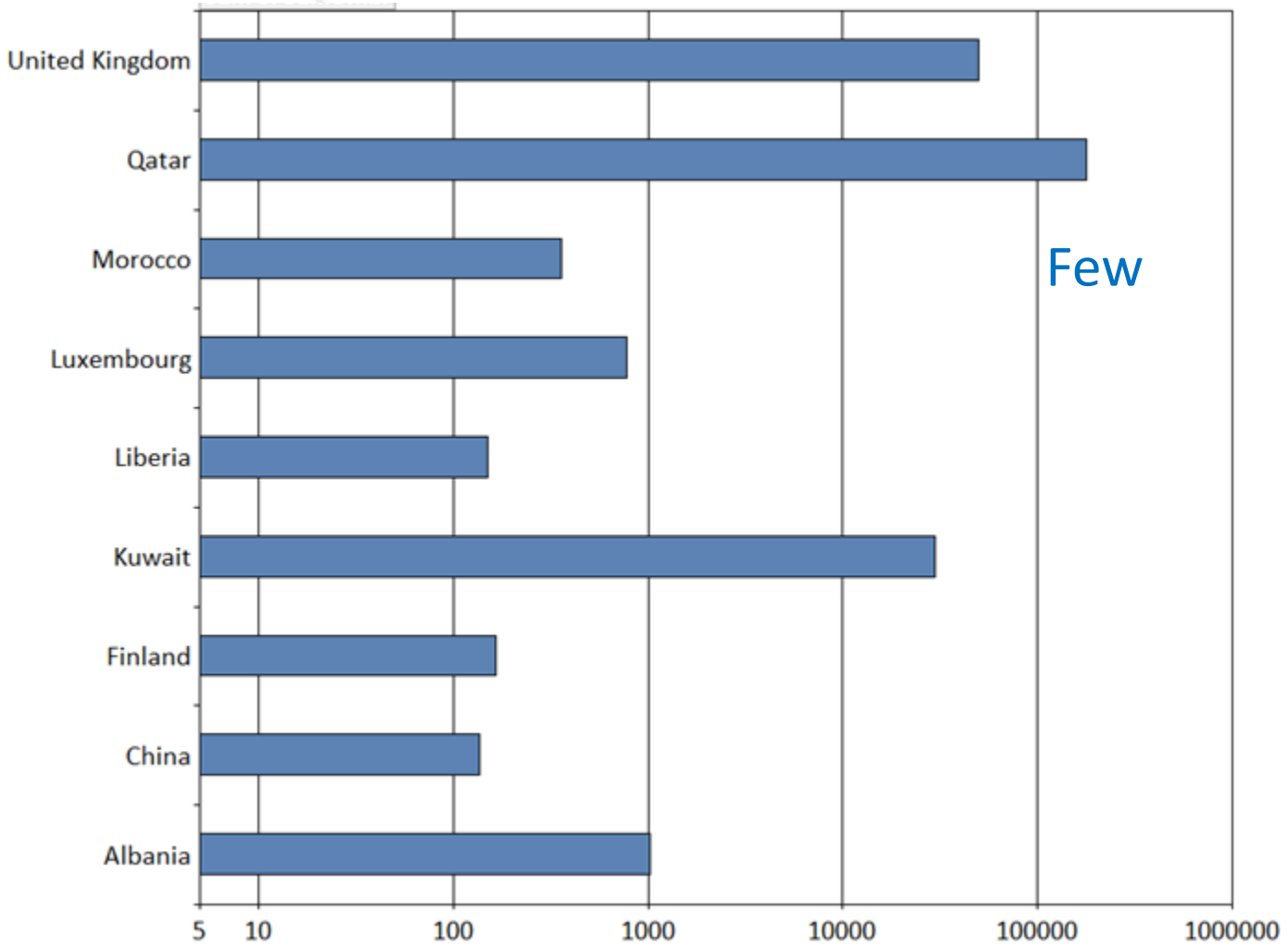
1956 2016
CCITT / ITU-T

SRI



1956 2016
CCITT / ITU-T

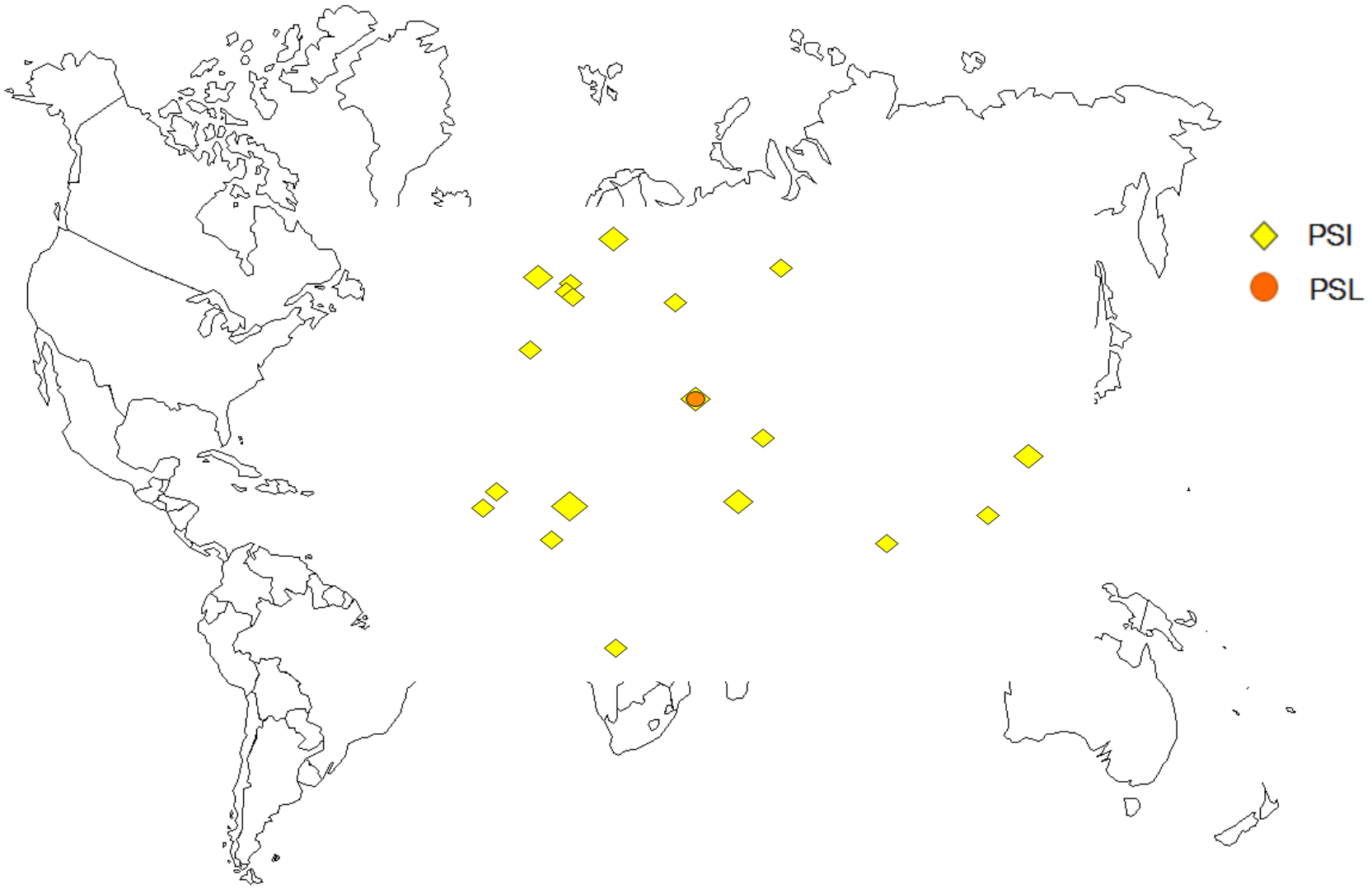
Send IMSI



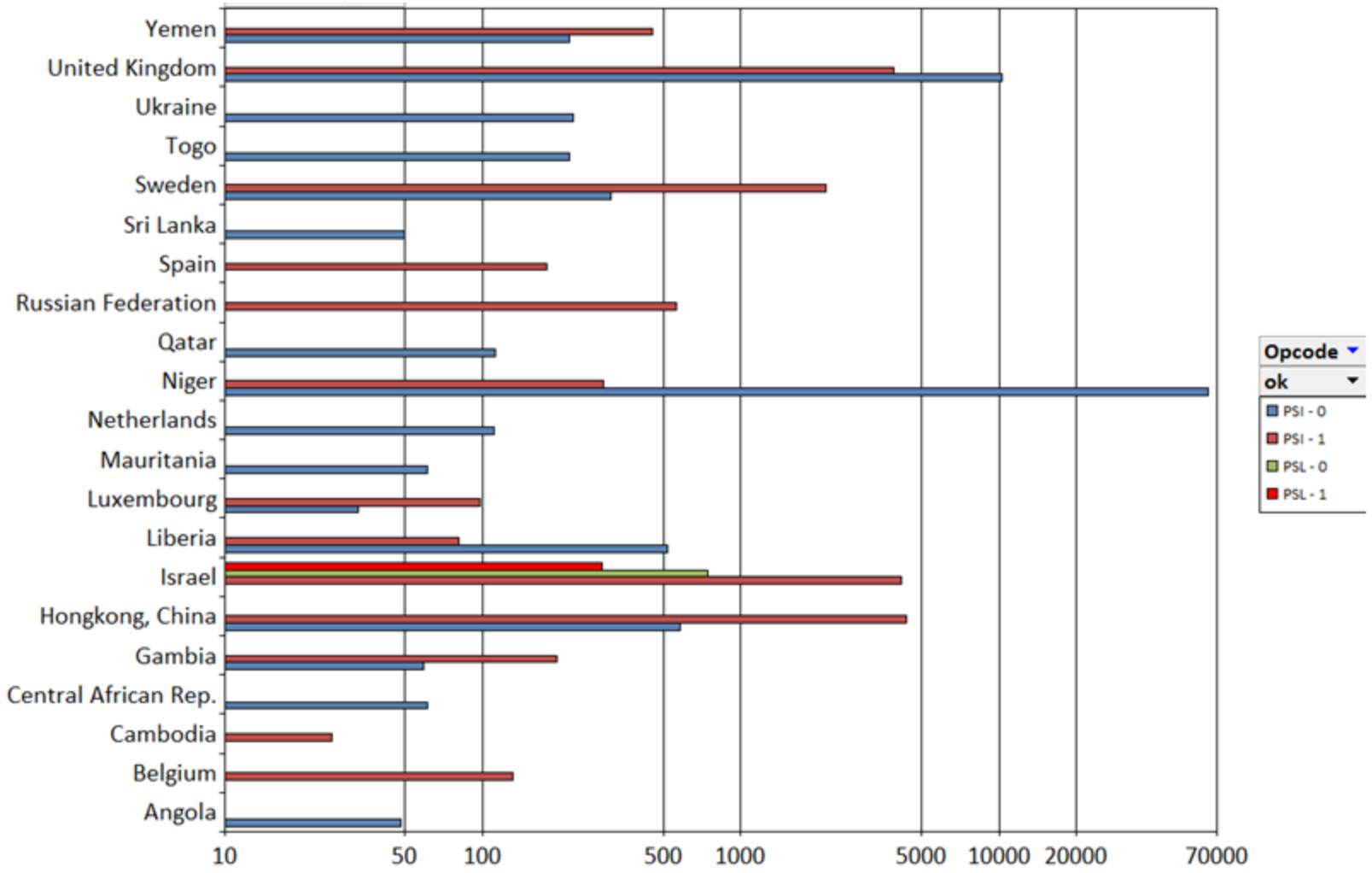
Cat.2 Audit

- Focus on Orange VLR
- Check if the origin is a real HLR
- Correlation between CgSCCP@ & Country IMSI
- Excluding Roaming Hubs

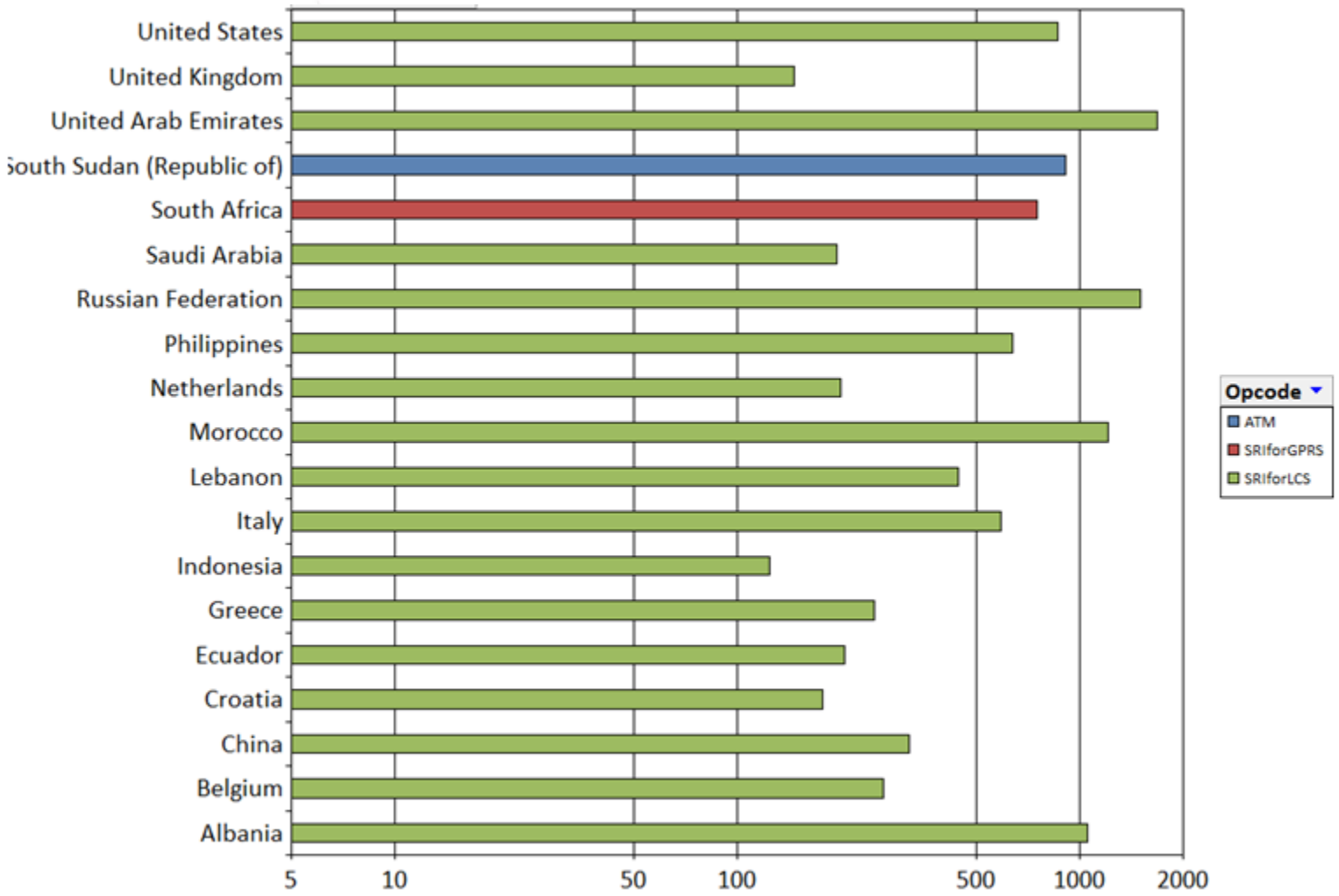
Cat.2 – Get any subscribers Location in Orange



Cat. 2 – PSI/PSL



Cat.2 – ATM/ATSI/SRIforGPRS-LCS



Cat.2 – Few Standalone ISD

- Difficult to state on ISD
- Origin could be faked (with real HLR@), there might be more than observed
- No DSD observed
- Few PRN observed

Cat.3 - Spoofing

- Activity sent from a fake location
- Observed and well-known issue
- For each activity,
  we need to check the real location

- SMS-MO protected by SMS Firewall

Cat.4

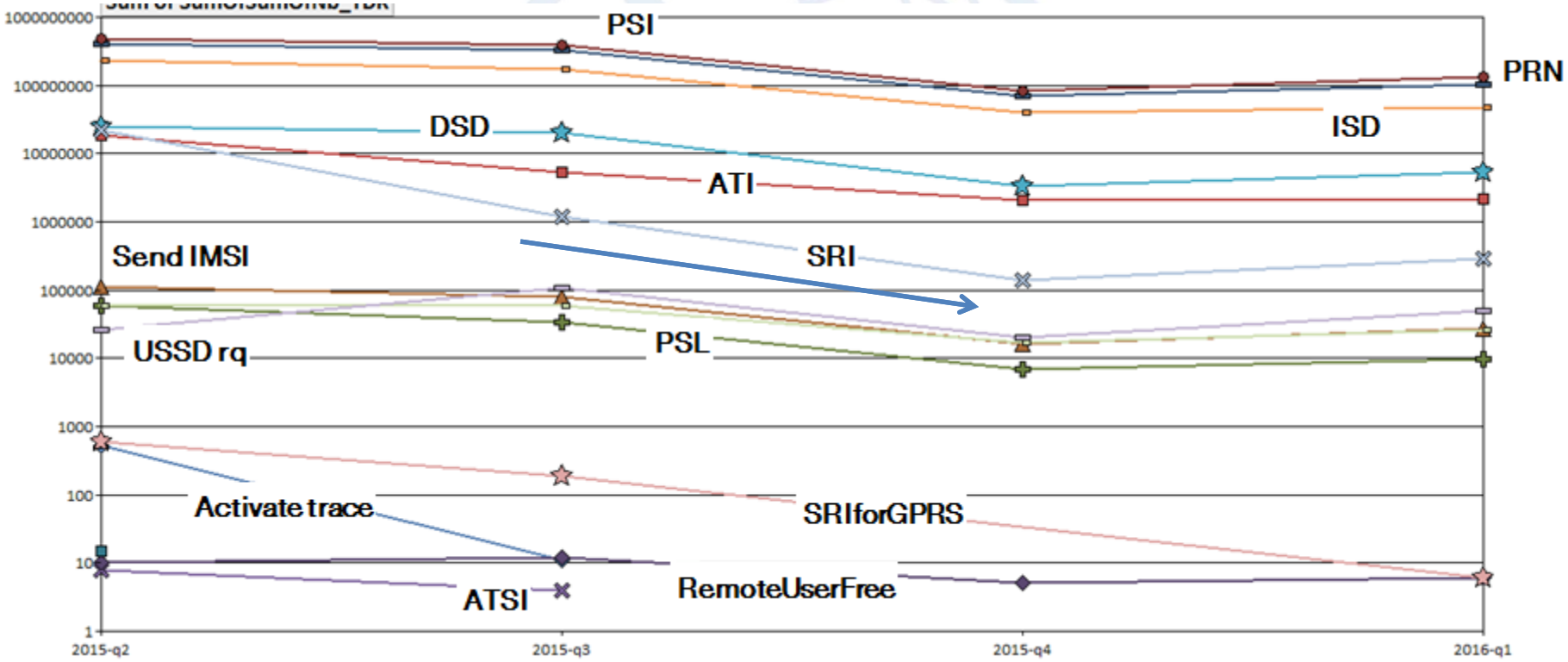
- SMS MT (SRI4SM and FWD-MT)
  - SRI4SM without Fwd-MT – Phishing
  - FWD-MT without SRI4SM – bypass
  - Grey routes
- Covered by SMS Firewall
  - Home Routing
  - anti-SPAM

Cat.5

- CAMEL profile manipulation
- (O-CSI) Marks to intercept the call
- Monitoring based on
  SCP@Network <> IMSI network
- Few observations
  Case by case analysis

Conclusions

- SS7 abuses are (observed) everywhere
- Current protection is good, but not complete



Next steps

- Industrialise the audits
- Improve existing network elements security
- Analyse security solutions in the market

Thank you

CCITT / ITU-T