One Consortium

The Restore Trust initiative

One Consortium – one year in

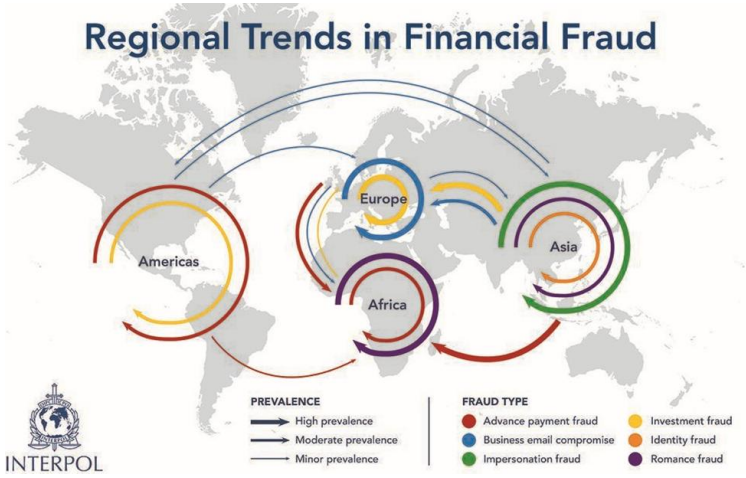
telecom industry and regulators join forces globally
to fight unwanted & fraudulent communications

the $1 trillion war against scams : a global issue, voice and SMS are key

- $1 Trillion lost worldwide in scams (1)
- phone calls and texts remain primary methods reported (approx. 64% of cases). (1)
- only 13% of victims got all or most of the money back. (1)
- only 0,05% of all cybercriminals are prosecuted (2)

scammers act from anywhere to anywhere, and go free : they operate globally, when we (telecom service providers, banks, law enforcement…) operate mostly locally, in multiple jurisdictions and frameworks

beyond remarkable national initiatives and regional cooperation, the telecoms ecosystem can contribute to global alignment and cooperation, prevention, traceability, and information sharing - working with all other stakeholders



suspected unwanted calls, Q3 2024 (3)

9.7 Billion
Global calls flagged as suspected spam in Q3 2024

105 Million
Calls flagged as suspected spam per day

(1) GASA "2024 Global State of Scams" report
(2) World Economic Forum
(3) Hyia "Threat Report Q3 2024" - as measured by Hyia in 40+ countries. Spam defined as unwanted calls, includes both fraud calls and nuisance calls

One Consortium

One Consortium

UNODC

scams, fraud and organized crime:

the role of telecoms

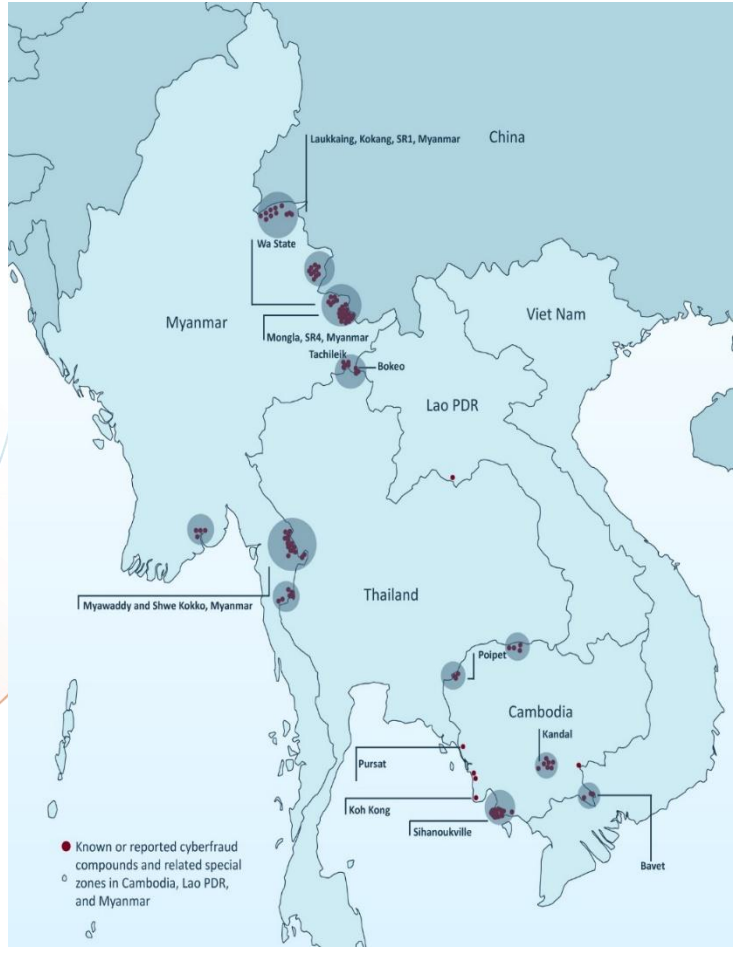
United Nations - Office on Drugs and Crime

Joshua James
Regional Counter-Cybercrime Coordinator
UNODC (Bangkok)

scams, fraud and organized crime – the role of telecoms

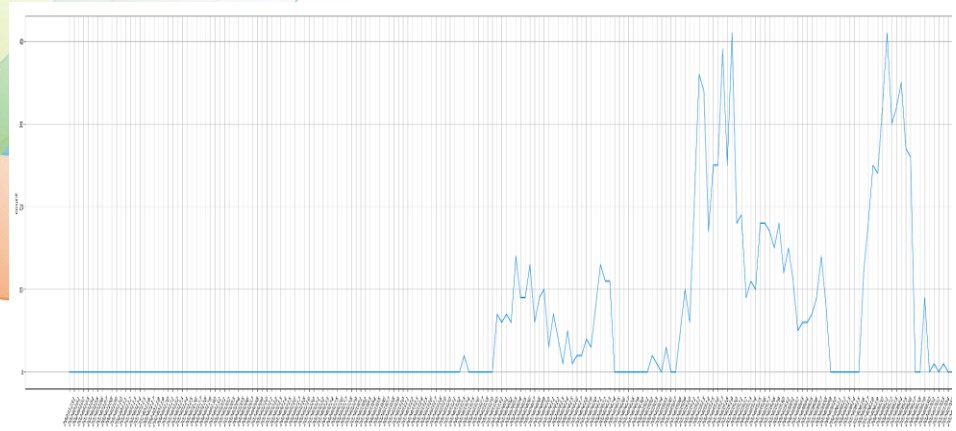
UNODC

scams, fraud and organized crime



scams, fraud and organized crime – the role of telecoms

UNODC



New development: misuse of Starlink

- Starlink identified following first cyber-enabled fraud seizure of Starlink equipment by RTP CIB
- Trend consistent with qualitative monitoring and reports by regional LE
- Similar surge in new underground vendors explicitly catering to cyber-enabled fraud operators in remote criminal enclaves in Mekong countries
- Demonstrates misuse of important dual use technologies – no different than crypto

scams, fraud and organized crime – the role of telecoms

UNODC

- Police have IP address, Phone Numbers
- Rely on telecoms to further the cases
  - International cooperation
- Telecoms is the key to it all
  - Phone registration, location, SIM, IMEI
- SIM card registration limits
  - 1% of registrants had 1000+ sims registered
  - Insider threats – sims “fall off the truck” a lot
- Simbox spoofing – still works!
- Fake Cell Tower (Dirtbox)
- **if global telecoms was interested in a coordinated effort, scam centers could be *decimated* immediately**

what can the telecoms ecosystem contribute ?
the Restore Trust initiative

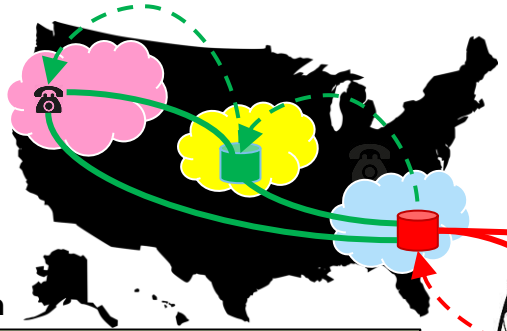
a major ecosystem-wide initiative to fight spams and scams

Philippe Millet
Founder and Chair, i3Forum
Leadership Council, One Consortium

the global telecoms ecosystem is complex, highly fragmented, opaque

how can we improve things together ? (some international voice examples : Alice calling Bob)

Alice

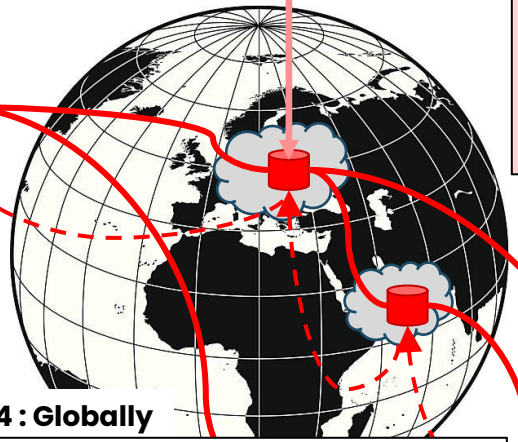


1 : at the Origin

Who owns the number, is the call "authorized" ?
- Know Your Customer: KYC
- number ownership & Right to Use: RTU
- spoofing : ok to alter/modify calling number?
- domestic traceback ← - - -

Fun facts (source Telegeography)
- annual international voice traffic : approx.
  - 350 Billion minutes (Telcos), = 666 years
  - and 1.2 Trillion minutes (OTTs) : x 3.5 !
- over 20,000 country-to-country int'l routes !
- 50+ routes carry 50% of the traffic (~ 1% each)
- each int'l call path takes multiple hops: ~ 5-10

One Consortium



2 : in international transit

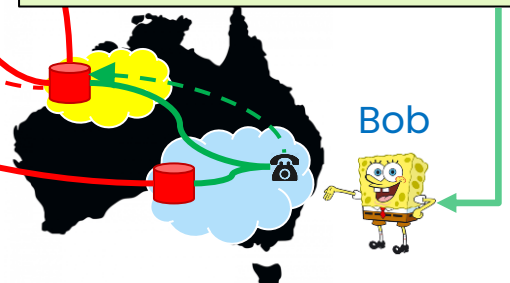
Is the traffic I'm transiting good traffic ? Are my carrier partners good partners ?
- Know Your Customer KYC
- Know your Traffic KYT
- calling number verification
- number blocking / call blocking (if allowed)
- international traceback ← - - -

3 : at the Destination

Is the inbound call "authorized" ?
- identify and allow legitimate use of national numbers used as origin number of inbound int'l calls (roaming, calls centers…)
- identify and block illegitimate use
- domestic traceback ← - - -

4 : Globally

- harmonized/consistent national legal & regulatory frameworks
- harmonized/consistent industry practices and tools
- for domestic and international (transit) traffic
- enablers, incentives, obligations
- collaboration + enforcement, nationally and globally



Bob

Restore Trust initiative : Telcos and Regulators together against scams, globally

three pillars for global collaboration, from vision to action to impact (voice & sms +…)

Initiative kick-off Sept. 7, 2023

One Consortium March 2024

GIRAF June 2024

Joint roadmap Feb 2025

You are here

Recommendations & Guidelines 2025 onwards

Adoption & Compliance 2026 onwards

Industry discussions

PreConsortium: planning for One Consortium

One Consortium for the industry : 50+ members incl GSMA, ITG, ATIS, CCA
five working groups : traceback, spoofing, messaging…

Joint Roadmap for multi-stakeholder engagement

Regulatory discussions

NRA Reach Out: building GIRAF

GIRAF the global regulatory forum : 35+ NRAs from 5 continents
informal and independent, led by NRAs (Nkom & others)

Broader ecosystem

Engaging with the broader ecosystem : Government Authorities, Law Enforcement, Global organisations (UNODC, ITU…), Banking and Payment industry…

Restore Trust Communication

April 10 webinar

One Consortium

One Consortium for the international communications industry

the industry's contribution to restoring trust in calls and messages.

- One Consortium, the industry pillar of the Restore Trust initiative, launched on March 15th, 2024
- inclusive, not-for-profit, members driven, members funded
- 50+ members : traffic carrying companies (carriers, service providers, CPaaS, global platforms…), vendors, industry organizations : GSMA, i3Forum, ATIS, ITG, CCA, CCUK…
- initial objectives, working with telecom National Regulatory Authorities (NRAs) :
  1) co-develop global guidance and a vendor neutral "toolbox"
  2) drive adoption in the industry
  3) build an industry-wide self-governance to drive compliance
- unique in several ways :
  1) purpose built to address a global societal issue from the perspective of the international telecoms industry
  2) purpose built to co-develop solutions with regulators, globally (GIRAF)
  3) participation from major industry associations : leverage existing work, prevent duplication, boost awareness and adoption

One Consortium

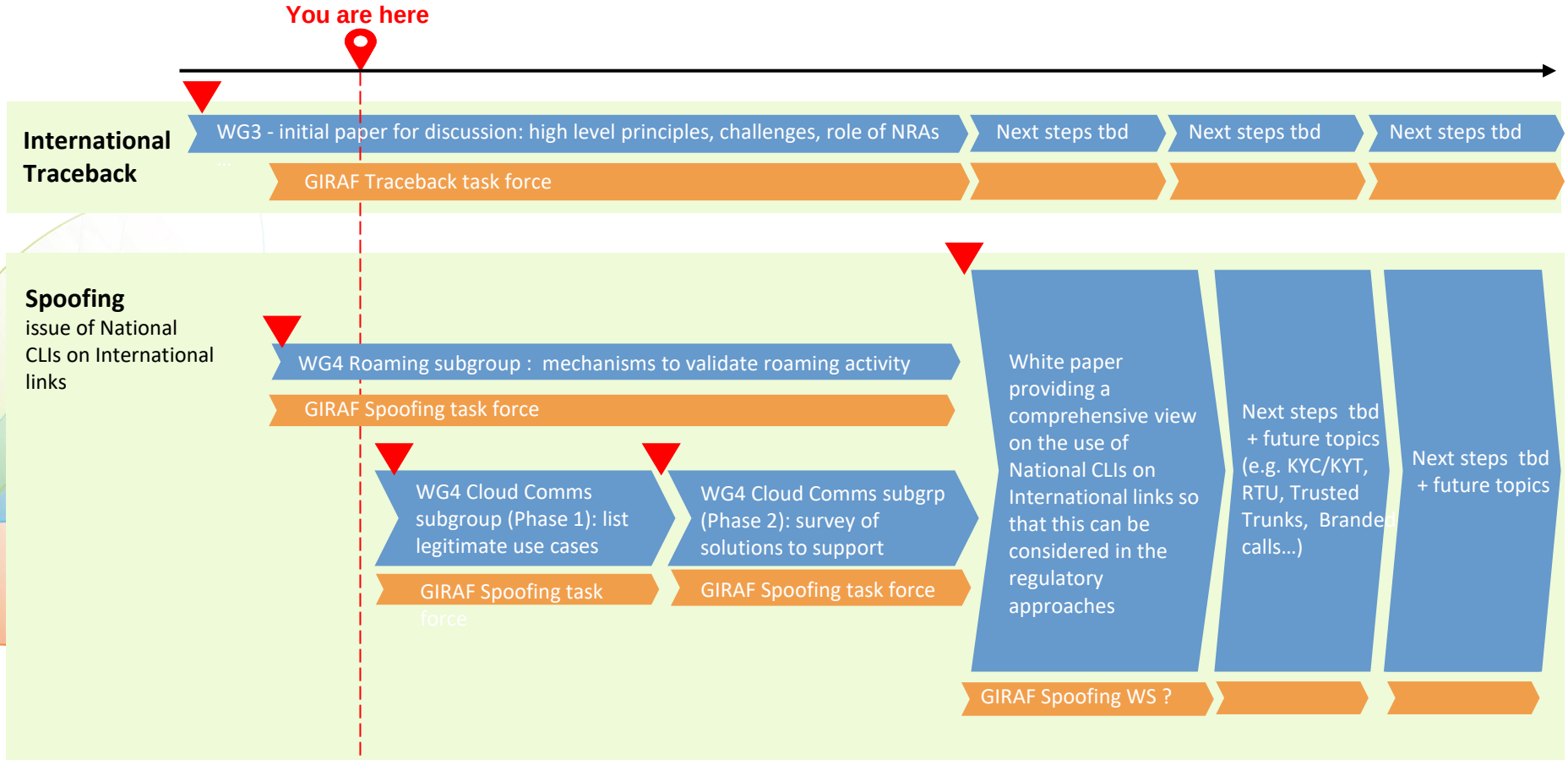
GIRAF : a global informal forum for telecom regulators

harmonize & enhance the telecom regulatory framework against spams and scams

- informal group of experts launched in June 2024 ; 35+ regulatory authorities from 5 continents (fast growing), monthly plenary meetings, working groups, joint sessions with One Consortium (all virtual meetings)
- scope : unwanted/fraudulent voice & messaging initially.
- goal : foster multilateral NRA collaboration, global cooperation with the international communications industry (One Consortium) and other stakeholders
- initial objective : framework of non-binding, harmonized recommendations, best practices and guidelines
- inclusive and free: opt-in, open to all NRAs or public competent Authorities with similar regulatory responsibilities, contributing as resources and availability allow
- neutral, non-binding and independent, led by regulators : Nkom (Norway) and others
- sovereignty : individual NRAs retain full sovereignty and are free to implement GIRAF guidelines and recommendations

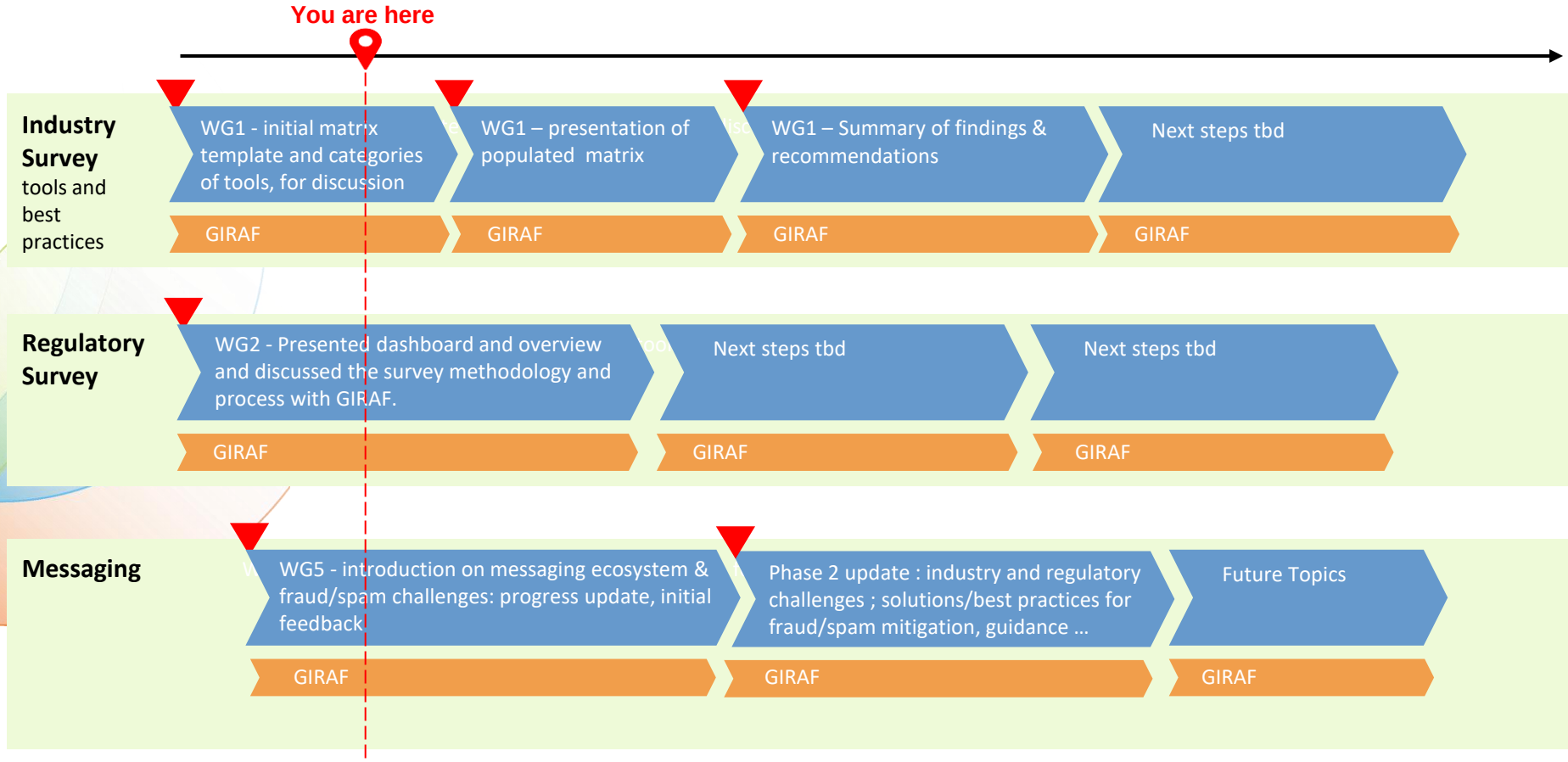
Joint Initial Roadmap

for global industry & NRA engagement 1/2



Joint Initial Roadmap

for global industry & NRA engagement 2/2



One Consortium

traceback

locating the true origin of a call

Tim French
Technical Consultant
Working Group Co-Chair, One Consortium

Linda Vandeloop
AVP External Affairs/Regulatory, AT&T
Leadership Council, One Consortium

traceback – why do we need it to fight spams / scams?

why do we even need traceback ?

- locate the origin of targeted call, i.e. unwanted / fraudulent / illegal call – definitions are jurisdiction and other criteria dependent

- it is complicated to identify the true origin of a call
  - the origin number cannot be trusted : can be spoofed : manipulated/altered
  - not all spoofing is illegal : multiple legitimate business and technical use cases
  - spoofing is easy to use to support fraud

- retracing call path hop-by-hop is the only way – often manually
  - cooperation between operators and between countries is required
  - adequate legal & regulatory framework (information sharing, legitimacy of requests…)
  - industry cooperation, central, neutral mechanism

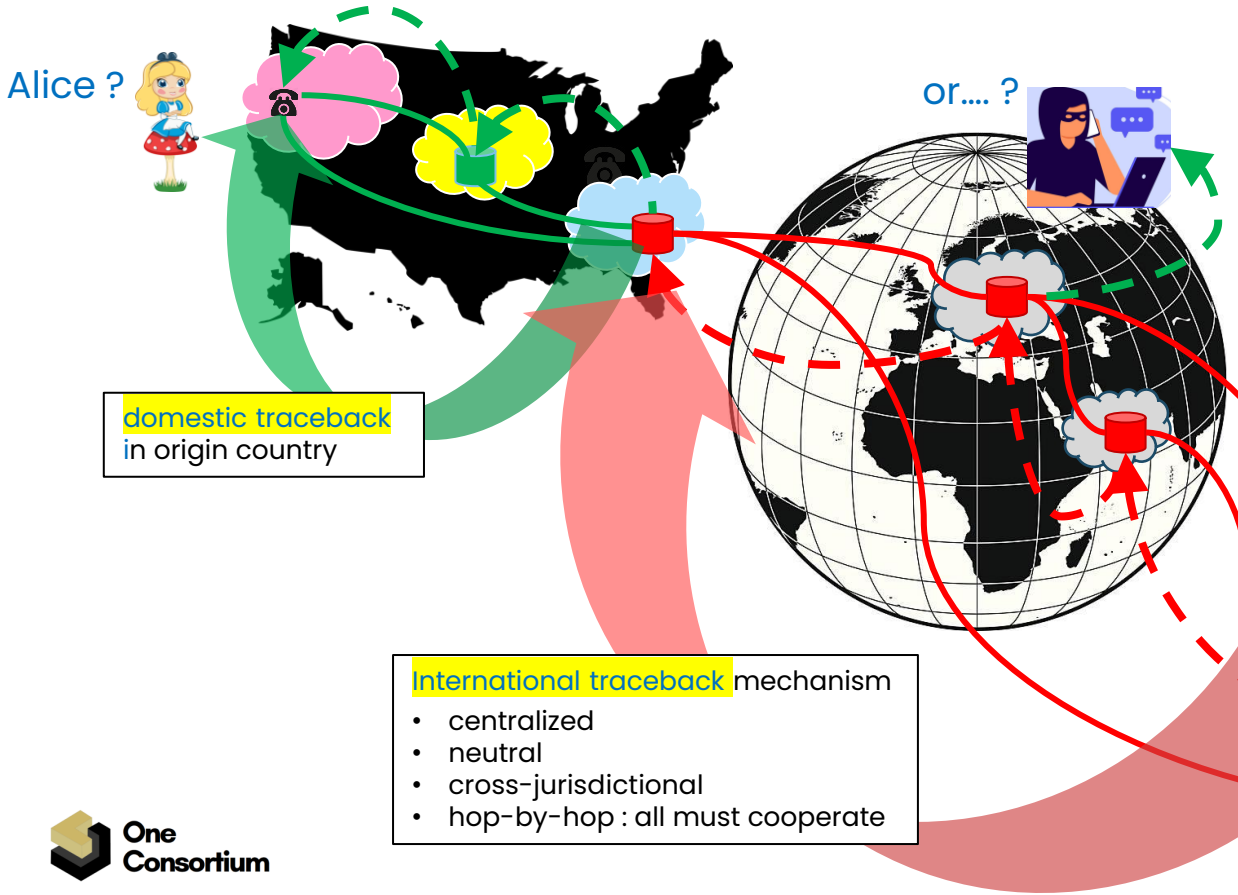
international traceback : locating the origin across multiple countries

a tool for the organizations responsible for fighting unwanted/ fraudulent calls

- each country is :
  - a destination : bad traffic can be received - and traceback requested
  - an origin : bad traffic can be originated
  - a transit point for international traffic – a hop in the traceback mechanism
- domestic traceback in a given country : same jurisdiction, regulator, rules, process…
- global traceback for international traffic : across multiple jurisdictions.
- "three segment" traceback model:
  - initial domestic segment in destination country : single jurisdiction, initiates request
  - middle segment covering international transit call path : multiple jurisdictions
  - final domestic segment in origin country : single jurisdiction, has origin's information
- One Consortium focuses on international segment, interfaces with domestic segments, and support to domestic jurisdictions – and discusses the regulatory framework with GIRAF
- status to date : high level outline available, initiated joint discussion with GIRAF

One Consortium

Who's really calling Bob ???



multiple challenges across multiple jurisdictions , including :

- what is a legitimate traceback request ?
- who can make a request, when ?
- what information can be shared?
- with whom?

NOTE : traceback is an enabler, not a substitute to law-enforcement

One Consortium

One Consortium

trusting national numbers on international calls

enabling legitimate spoofing use cases,

blocking fraudulent traffic

Eli Katz
CEO and Founder, XConnect
Board member, i3Forum
Leadership Council, One Consortium

Katia Gonzalez
Head of Public Policy, Proximus Global
Board member, i3Forum
Leadership Council, One Consortium

use of national numbers as origin on international inbound call

enabling legitimate spoofing use cases

- why would a call coming from abroad, with an origin number (CLI) from the destination country, be legitimate ???
- clearly, the origin number has been spoofed (i.e. modified/altered)
- to protect their country's people and businesses, regulators look to block such spoofed international inbound calls
- but multiple use cases of such spoofing are legitimate
  - roaming : when a roamer calls home from abroad, the origin number is his home mobile number - the call coming from abroad looks like it's coming from the destination (home) country
  - cloud numbers
- One Consortium focuses on mechanisms to distinguish legitimate use cases from traffic that should be blocked – and discusses the regulatory framework with GIRAF
- status to date : high level paper available, initiated joint discussion with GIRAF

One Consortium

trusting national CLIs on int'l calls : roaming

checking if an incoming national CLI is from an outbound roamer calling home from abroad

is-roaming WG4 subgroup status

- for mobile the home network of originator (A-party) knows if subscriber is roaming
- for SIP/VoLTE the call is routed via the home network.
  - The originators home network can check roaming and block if not
  - The destination network (or the national gateway) can check the call arrives nationally
  - Easy long-term solution
- for SS7 (2G/3G) the destination network or international gateway must check roaming
  - This may be a mobile or a landline network
  - A standard approach to check roaming is required
  - SS7 will be around for a long time
- is-roaming check options
  - Signalling – Technically easy and exists, but security risk exploited in the past
  - API – Standard APIs exist but not are widely deployed. Recommended
  - Query could be to individual operators or a shared gateway
- other controls required (by A party) for wifi, late call forwarding and fraudsters using roaming SIMs
- presented and discussed with GIRAF

One Consortium

trusting national CLIs on int'l calls : Cloud Communications

Cloud Communications

WG4 subgroup

(Work in Progress)

- what are "cloud numbers" ? they are virtual phone numbers, i.e. regular phone numbers that are not linked to any mobile phone or a landline, that are utilized in cloud-based technology to facilitate communications.
- unlike traditional phone numbers tied to physical phone lines, cloud phone numbers are part of a VoIP system, allowing users to make and receive calls over the internet

Use-case : Number Anonymity

- objective: anonymize called identification facilitating communications between end-users and service providers without exposing personal phone numbers
- examples: Identity masking is used by Uber, Airbnb, etc

Use-case : Conferencing Platform

- objective: allow users to join a meeting from any location using dial-in numbers or to invite user to join the meeting (dial-out)
- examples: Teams, zoom, etc

Other use-cases : Cloud Contact Center, Corporate telephony, Call Center, Call Forwarding, DIDs for remote device, Click to Call, etc

One Consortium

leveraging existing industry tools and practices to help restore trust

Tim French
Technical Consultant
Working Group Co-Chair, One Consortium

Angela Dais
Director | Federal Regulatory, AT&T
Working Group Co-Chair, One Consortium

leveraging existing industry tools and practices to help restore trust

industry survey in progress :

we're not starting from scratch!

- telcos and carriers deploying tools and processes to reduce illegitimately spoofed, illegal, malicious, scam, or unwanted calls
- multiple vendors developing and enhancing services and solutions
- One Consortium's initial focus : survey, describe and categorize existing tools.
- longer-term output :
  - high-level paper summarizing the tools identified
  - recommendations on vendor neutral "toolbox" and best practices
  - jurisdictions have unique needs : certain tools more appropriate in one jurisdiction than another
- progress to date : initial survey Matrix almost finalized (approx. 40 tools described), being shared with GIRAF for comments
- very active and highly structured working group : 28 experts ranging the entire call path eco-system from around the world. Meeting twice a month. Sub-groups on specific tools, peer reviewed.

One Consortium

matrix captures tools being used, considered, or developed today globally

content for each tool : description of the tool; its availability; whether implementation is mandated, and if so, where; services covered by the tool; scope of the tool's use, at origination or termination, etc..; source of the tool, whether it's commercial or standards-based, etc.; current coverage of the tool; implementation considerations; and known limitations

					Services covered		Scope						Source							
Name	Short description	Information URLs	Availabl	Mandat	Voice	SMS	At origina	At termina	End-to-E	N/A	Other	not appl	Comme	Standar	Propriet	Open so	Coverage	Implementation considerations	Known limitations
Do Not Call	Register of users who do not wish to be called for specific purposes or timeframes.																		
Do Not Originate lists	Maintained lists of numbers which should not originate calls. This includes freephone scenarios where certain numbers are not built for inbound or outbound calls and therefore should not be able to originate calls.	https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/do-not-originate/ https://www.comreg.ie/publication/consultation-on-network-based-interventions-to-combat-scam-calls-and-texts https://www.fcc.gov	In use	UK,IE,US	Yes	No	Yes	Yes	No	No	No	Yes	No	No	Yes	No	Country-by-country	DNO: implementation only required by the originating network with no interoperability considerations	Many different siloed solutions
Unallocated telephone numbers	List of numbers from regulator that have not assigned to an operator therefore should not originate calls.		In use		Yes	No	Yes	Yes	No	No	No		No	No	Yes	No	Single country	Carrier can to make these available to analytics engines	Many different siloed solutions
Unassigned Number List	List of numbers from (some) Carriers that are not allocated to customers.																		
Allow List	Allow listing lets a TN bypass call analytics services or blocking due to the accepted level of trust associated with the originating TN.		In use		Yes		Yes	Yes	Yes						No		Global		
Block List	Blocklisting restricts the privilege of a TN such that calls originating with the blocklisted number are typically blocked.		In use		Yes		Yes	Yes	Yes						No		Global		
GSMA IRSF database lookups	GSMA database is referred to for any wangiri/fraud calls flagged	https://www.gsma.com/solutions-and-impa	In use	No	Yes	Yes	No	Yes	No	No	No	No	Yes	No	No	No	Global	Technically an IRSF tool, but as this cover Waingiri and bot traffic it could still be good to reduce spam calls	The solution is based on detection of unwanted usage of numbers and is as such it cannot completely prevent issues but it can rapidly alert of them and provide scope for closing down issues more quickly and can even do so during the testing phase before usage has picked up. it should not be considered as authoritative data as the intel is gathered by diverse sources and their views may be impacted by the sources/routes/parties they work with (eg. a nbr involved in IRSF for a party may be completely clean for another one). Also, the numbers in this db are not cleaned up over time.
Aging Number Database	Such a database would identify numbers that have been recently taken out of service and are "aging" before being reassigned. During this "aging" period, these numbers would not be available for use, and therefore any calls with these numbers as the caller ID could safely be assumed to be illegitimate. **Note:** I don't believe this information is publicly available anywhere, so this category may not be appropriate for here.	https://www.fcc.gov/reassigned-numbers-d	In use	US	Yes	No	Yes	No	No	No	No		Yes	No	Yes	No	Single country	Good for legitimate enterprise, however, not going to be used by bad actors	Many different siloed solutions
Malformed numbers	Numbers that are not correctly formatted, and therefore cannot possibly be a legitimate Caller ID. One example that was often seen in the past is 000-000-0000. Since E.164 formats are well known, it is possible for service providers to identify calls with a malformed number in the Caller ID and, if allowed, block them.																	Each party to define its own rules and controls to define 'malformed' numbers.	Many different siloed solutions
Non-routable toll-free numbers	Toll-free numbers that aren't assigned to a Carrier Identification Code table.		In use		Yes		Yes	Yes	No	No	No		No	No	Yes	No	Single country	TNS can determine, but could also be made widely available by SOMOS	Many different siloed solutions
Reassigned Number Database	The FCC's Reassigned Numbers Database (RND) is designed to prevent a consumer from getting unwanted calls intended for someone who previously held their phone number. Callers can use the database to determine whether a telephone number may have been reassigned so they can avoid calling consumers who do not want to receive the calls. Callers that use the database can also reduce their potential Telephone Consumer	https://www.fcc.gov/reassigned-numbers-d	In use	US	Yes	No	Yes	No	No	No	No		Yes	No	Yes	No	Single country	Good for legitimate enterprise, however, not going to be used by bad actors	Many different siloed solutions

understanding regulatory requirements and industry voluntary initiatives across different countries

Andrew Bale
CEO, Rich Connexions
Leadership Council, One Consortium

Ivana Kiznic
Head of Public Policy Canada, Latin America, Emerging Markets, Verizon
Leadership Council, One Consortium

understanding regulatory requirements and industry voluntary initiatives across different countries

regulatory survey in progress:

many different approaches to similar issues

objective: comprehensive yet user-friendly matrix that indicates for various aspects whether a requirement exists, is under consideration, or if there are any voluntary industry measures in place. Uses binary values: YES / NO, and N/A (information not publicly available).

acknowledgements: special thanks to WG2 members!. Contributions from approximately 15 representatives from traffic-carrying carriers and vendors operating in the US, Europe, Asia, and internationally. Bi-monthly group meetings over the past 9 months.

starting point: a common set of definitions and 4 main categories with several attributes for each category.

tiered approach: Phase 1 completed for 30+ countries. Future releases will cover an additional 40+ countries.

next steps: Increase collaboration with GIRAF. Finalize the remaining countries. Find a hosting platform. Agree on a process for recurring updates.

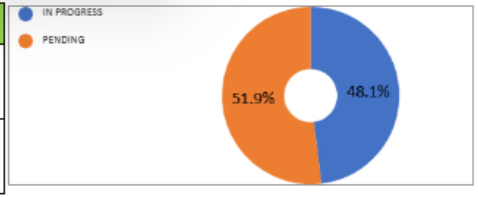
Regulatory Survey - Dashboard

COUNTRIES IN STUDY
77

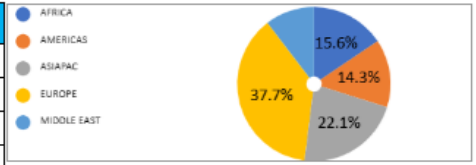
REGIONS IDENTIFIED IN STUDY
5

GIRAF PARTICIPANTS IN STUDY
29

SURVEY INPUTS STATUS		
IN PROGRESS	37	48%
PENDING	40	52%



COUNTRIES BY REGION		
AFRICA	12	16%
AMERICAS	11	14%
ASIAPAC	17	22%
EUROPE	29	38%
MIDDLE EAST	8	10%



One Consortium

Regulatory Survey - Dashboard

CURRENT ATTRIBUTE RESULTS (IN PROGRESS SURVEY ENTRIES)									
ATTRIBUTE	REQUIREMENT			UNDER CONSIDERATION			INDUSTRY VOLUNTARY		
	YES	NO	N/A	YES	NO	N/A	YES	NO	N/A
1a. AUTHENTICATION FRAMEWORK	6	24	0	3	25	0	5	24	0
1b. BLOCKING OR OTHER MITIGATION MEASURES	19	9	0	5	19	0	7	20	0
1c. BLOCK INCOMING INTERNATIONAL CALLS WITH NATIONAL CLI	12	15	0	3	21	0	2	21	0
1d. DO NOT CALL (DNC)	19	9	0	6	19	0	5	19	0
1e. DO NOT ORIGINATE (DNO)	8	19	0	3	22	0	4	20	0
1f. OTHER CALLING LINE IDENTIFICATION (CLI) MEASURES	13	13	0	5	18	0	4	20	0
2a. SHORT MESSAGE SERVICE (SMS)	18	8	0	2	21	0	4	20	0
2b. RICH COMMUNICATION SERVICES (RCS)	11	14	0	1	23	0	4	20	0
2c. ALPHANUMERIC SENDER ID	11	17	0	2	23	0	9	17	0
2d. SENDER ID REGISTRY	7	21	0	3	24	0	8	20	0
3a. NRA ENFORCEMENT TOOLS	26	3	0	3	23	0	3	24	0
3b. OTHER COLLABORATIVE INDUSTRY PROCESSES	3	21	0	1	22	0	18	6	0
4a. RULES USING ARTIFICIAL INTELLIGENCE (AI) MITIGATION TOOLS	16	11	0	5	21	0	6	21	0
4b. CONSUMER LABELING TOOLS	3	24	0	2	24	0	2	24	0
4c. KNOW YOUR CUSTOMER (KYC), KNOW YOUR UPSTREAM PROVIDER (KYUP), KNOW YOUR TRAFFIC (KYT)	19	9	0	5	24	0	7	22	0
4d. TRACEBACK	5	20	0	4	20	0	4	20	0

One Consortium

messaging:
another major vector
for spam & fraudulent schemes

Eli Katz
CEO and Founder, XConnect
Board member, i3Forum
Leadership Council, One Consortium

Kimberly Darrin
Public Policy, AT&T
Working Group Co-Chair, One Consortium

messaging – another major vector for spam & fraudulent schemes !

initial analysis and findings

what are the industry toolkit for reducing messaging fraud and scams ?

can voice solutions be leveraged to reduce messaging spam ?

challenges

- disparate regulatory treatment of business messaging around the world
- introduction of Rich Communications Service (RCS & RBM) bringing opportunities and some challenges
- shift from carrier-operated messaging services to OTT
- encryption - impacts to spam mitigation and lawful interception.

recommendations

- education and greater industry collaboration and alignment of tools and best practices are needed.
- increase harmonization in the messaging ecosystem and regulatory action around the globe

status: draft white paper, spam/scam mitigation tools, input from 1C industry and regulatory surveys; initial meeting with GIRAF

future focus:

- guidance/best practices on inbound international messaging
- National Brand or Campaign Registries for Business Messaging and international cooperation.
- trusted or verified messaging.

One Consortium

GIRAF
the global regulatory forum

Restoring Trust
in international communications

Call to Action – let's join forces!

- Telecom Industry , global tech
- Telecom Regulators
- Other industries and regulators : banking & payment…
- Law Enforcement
- Policy makers, law makers
- Other private or public initiatives

One Consortium

thank you !

www.oneconsortium.org