Third Meeting for WSIS Action Line C5:
Building Confidence and Security in the Use of ICTs

Session 3: Cyber-attacks:
Are we ready for the battlefield of the 21st Century?
22 May 2008
Palais des Nations, Geneva

Universal Trusted Service Provider Identity to Reduce Vulnerabilities

Tony Rutkowski

Vice President for Regulatory Affairs and Standards, VeriSign

Co-editor, ITU-T Recommendation: Requirements for global identity management trust and interoperability

Member, ITU High Level Experts Group on Cybersecurity

Distinguished Fellow, Georgia Tech Nunn Center for International Strategy Technology and Policy

mailto:trutkowski@verisign.com

Introduction

- In the Cybersecurity Ecosystem, it is infrastructure-based capabilities that are most important
- Cybercrime arrangements are worth little except as they drive infrastructure forensic capabilities
- Among infrastructure-capabilities, it is trusted Identity Management that is most important
- Infrastructure includes all telecommunications/ICT of which internets are just a small part
- Among Identity Management, it is trusted service provider identity capabilities that are the most important
- These capabilities have also the largest benefit-cost ratio: easily and quickly achievable at negligible cost and adverse impact
- The challenge is how to bring about infrastructure-based cybersecurity capabilities, especially global interoperable trust

Universal Trusted Service Provider Identity is essential

- Significantly diminishes existing and potential threats for
  - Governments
  - Providers
  - Consumers
- Enhances infrastructure stability
- Provides developers and service providers with new “trust service” opportunities
- A universal service provider trust infrastructure can be implemented quickly, easily, and at minimal cost

Trusted-SPID is like doing a “fingerprint” check on the identity of a Service Provider

Service Provider = everyone except end users (enhances privacy)

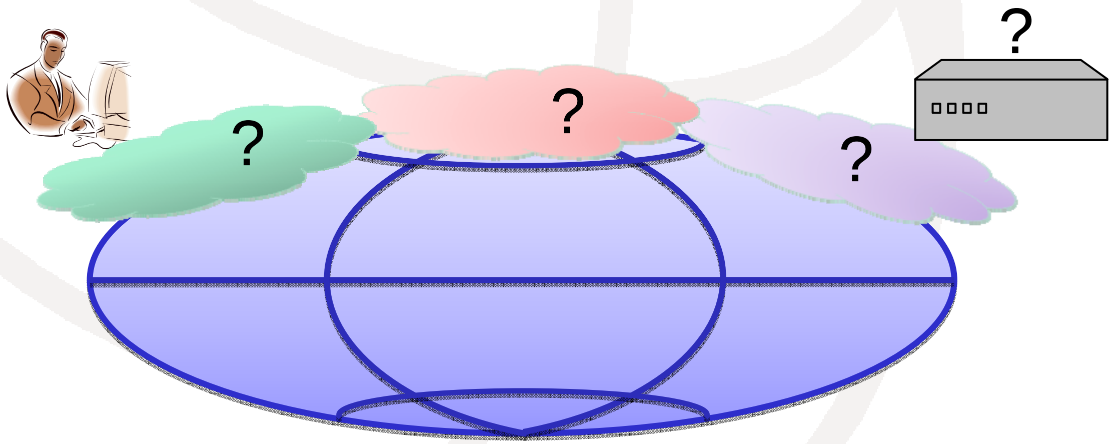
1995-2008: the cybersecurity "Perfect Storm"

- Service Provider trust that is essential for network security was provided by
  - ❑ closed, fixed networks
  - ❑ operating under substantial domestic and international regulatory regimes
- During the past decade
  - ❑ open public networks (e.g., Internet), wireless, nomadicity, globalization, smart terminal devices, application providers, and a shift away from legacy regulatory regimes
  - ❑ without the development of any kind of underlying global service provider trust infrastructure

The problem: provider identity and trust have disappeared

- In the legacy telecom world, service providers were identified and trust levels established through common carrier regulation

- In the IP-enabled, deregulated network world, it is difficult to identify who the service providers are, much less assess trust levels



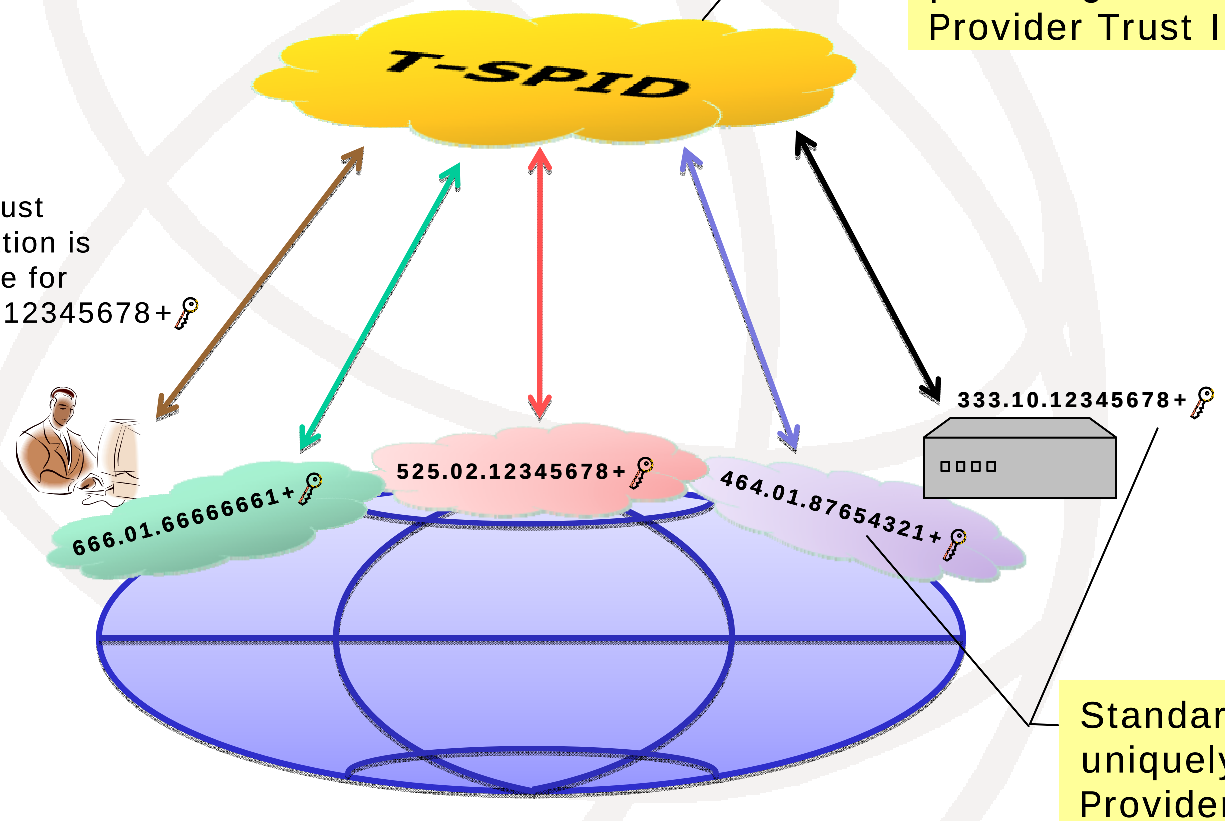
The lack of a trust infrastructure produced inevitable results

- “Battlefield conditions”
  - Provider fraud, identity theft, phishing, SPAM, “phantom traffic,” Denial of Service attacks, CallerID spoofing, Critical Infrastructure vulnerabilities, etc
- The increasing transition of public IP-enabled network infrastructures will exacerbate vulnerabilities
- The problems and abuses will likely continue to increase significantly without effective Service Provider identity trust remedies

What is required?

- A network platform for
  - a universally recognized, globally unique identifier (a kind of call-sign) for each provider
  - the ability to allow instant interoperable discovery and lookup of identity “trust information” associated with the provider
- Enable other providers and users to make trust decisions when relying on a provider’s identity and assertions in any context or situation
- Governmental and Intergovernmental action to implement the platform
  - Historically a basic role of the ITU and governments
  - Unlikely to occur without governmental support

Enabling Service Provider Trust



Standard universal "overlay" means for discovering and providing structured Service Provider Trust Information

What trust information is available for 333.10.12345678+

Standard universal means of uniquely identifying Service Providers and capturing available structured Trust Information

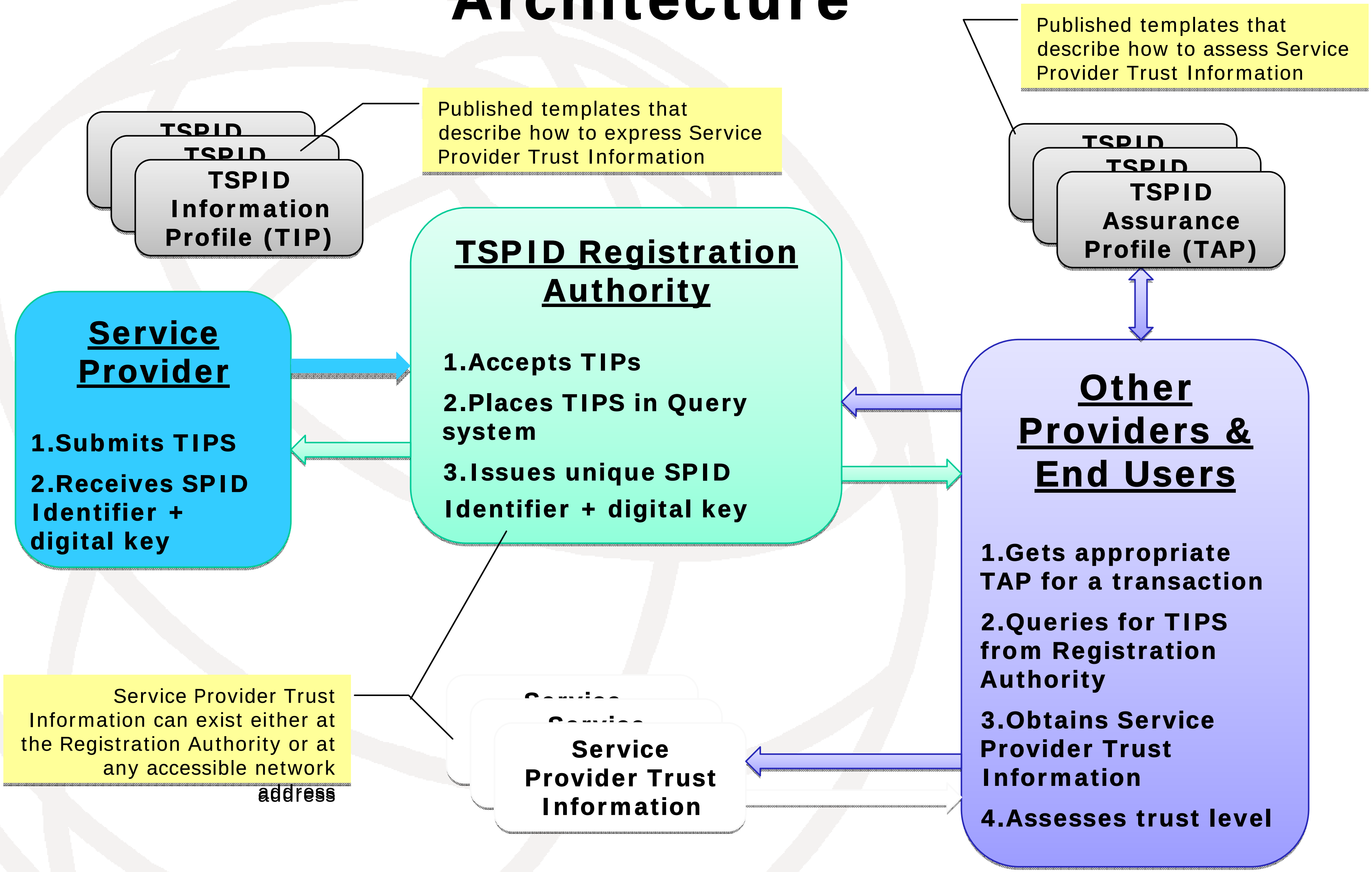
Needs for Trusted Service Provider Identity

Amongst Service Providers	End Users	Government
Infrastructure security and integrity	Access trust	Critical infrastructure protection
Traffic exchange and settlements	Transaction trust, i.e., minimize fraud	Emergency telecommunication services
Roaming settlements	Protection against identity theft	Law enforcement forensics
Content IPR protection, controls and fee settlements	Protection of Personally Identifiable Information	Public safety services
Access of content/application providers to traffic termination providers	Preventing unwanted intrusions, e.g., SPAM, cyberstalking	Universal Service contributions
Threat management; incident response trust capabilities	Trusted Caller/Sender ID	Number resource allocations
Federation interoperability; provider bridging capabilities		Government network security and integrity
“Network Neutrality”	Disability assistance	“Network Neutrality”

Service Provider Trust Information

Service Provider Credentials	X.509 PKI digital certificates Other credentials
Service Provider Assigned identifiers	Operational identifiers (e.g., OIDs, ITU Carrier Codes, E.212 MCC/MNCs, Autonomous System Number blocks, IP address handles) Signalling point codes (SANS) Public safety and emergency telecommunications identifiers Billing and settlement identifiers Regulatory identifiers Tax identifiers Law Enforcement identifiers (LI and retained retention)
Service Provider Allocated Public Numbering Resources	E.164 number blocks IPv4/v6 addresses blocks Autonomous System Number blocks
Service Provider Attributes	Legal name Business names Headquarters jurisdiction Billing and settlement attributes Federations Emergency services authorizations and capabilities Disability assistance capabilities Customer support contacts Privacy support capabilities Additional regulatory, infrastructure protection, and security attributes
Service Provider Patterns	Reputation datastores or metadata

Trusted Service Provider Identity Architecture



Published templates that describe how to express Service Provider Trust Information

TSPID Information Profile (TIP)

Published templates that describe how to assess Service Provider Trust Information

TSPID Assurance Profile (TAP)

Service Provider

1. Submits TIPS
2. Receives SPID Identifier + digital key

TSPID Registration Authority

1. Accepts TIPs
2. Places TIPS in Query system
3. Issues unique SPID Identifier + digital key

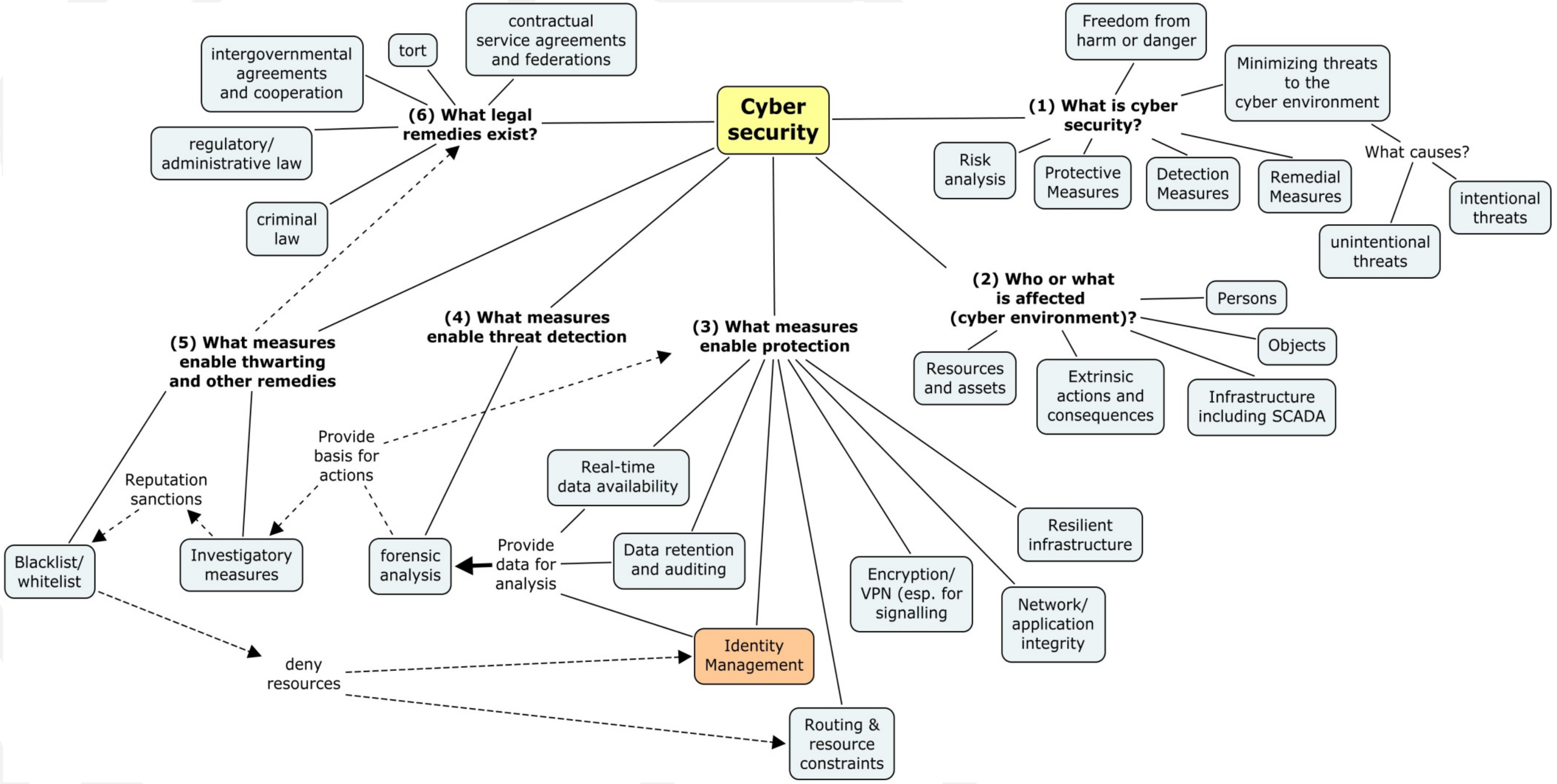
Other Providers & End Users

1. Gets appropriate TAP for a transaction
2. Queries for TIPS from Registration Authority
3. Obtains Service Provider Trust Information
4. Assesses trust level

Service Provider Trust Information

Service Provider Trust Information can exist either at the Registration Authority or at any accessible network address

Trusted Service Provider
Identity is core to cybersecurity


Cyber security
(1) What is cyber security?
Freedom from harm or danger
Minimizing threats to the cyber environment
What causes?
intentional threats
unintentional threats
Risk analysis
Protective Measures
Detection Measures
Remedial Measures
(2) Who or what is affected (cyber environment)?
Persons
Objects
Resources and assets
Extrinsic actions and consequences
Infrastructure including SCADA
(3) What measures enable protection
Real-time data availability
Data retention and auditing
Identity Management
Routing & resource constraints
Encryption/ VPN (esp. for signalling)
Network/ application integrity
Resilient infrastructure
(4) What measures enable threat detection
forensic analysis
Provide data for analysis
Provide basis for actions
(5) What measures enable thwarting and other remedies
Blacklist/ whitelist
Investigatory measures
Reputation sanctions
deny resources
(6) What legal remedies exist?
intergovernmental agreements and cooperation
tort
contractual service agreements and federations
regulatory/ administrative law
criminal law

All technical implementation components exist today

- Trusted SPID requirements can be readily implemented on many different technical platforms
- Highest performance platform is found in the past seven years of work on for telephone numbers and product codes on Domain Name System
- Standards activity now underway in ITU-T and regional/national standards bodies
- All of the “running code” is available, open-source with no intellectual property constraints
- Highly synergistic with ongoing trust “federation” activities, NGN, and other industry developments
- The work incents an existing developer community to produce new “trust applications”

All legal system implementation components exist today

- ITU Constitution Art. 42 obligates signatories (nearly every nation) to take steps to avoid harm to facilities and telecommunications
  - ❑ Maintaining the integrity of telecommunication infrastructure and services goes back to earliest treaty instrument in 1850
  - ❑ The obligation became a core component of the 1903 draft wireless radio convention
  - ❑ Became integrated in 1920 as an obligation to “organize as far as possible in such a manner as not to disturb the services of other Administrations…”
  - ❑ Reflected in later instruments as an obligation “to avoid harmful interference”
  - ❑ Expanded in 1989 in the ITU Constitution to avoid "technical harm…to the operation of other telecommunication services of other Member States”
- Every nation has the authority to implement registration capabilities for those constituting public ICT/telecommunication networks or offering services to the public over those networks
  - ❑ Registration authority is widely implemented by telecom regulatory, justice, infrastructure protection, consumer protection, tax, and business agencies
- A requirement to register is not “regulation”

Is history repeating itself

- One hundred years ago
  - ❑ New wireless digital networks and services were operating in chaos and harming each other's communications
  - ❑ Nations joined together to adopt basic global norms and mechanisms
    - Cooperate to minimize harm to another party’s infrastructure and communications
    - Facilitate interoperation
    - Institute trusted service provider identity
  - ❑ Agreement was finally achieved immediately after Titanic sinking