International Telecommunication Union

Country Case Studies: The Case of Brazil

ITU Workshop on Creating Trust
in Critical Network Infrastructures
Seoul, Republic of Korea

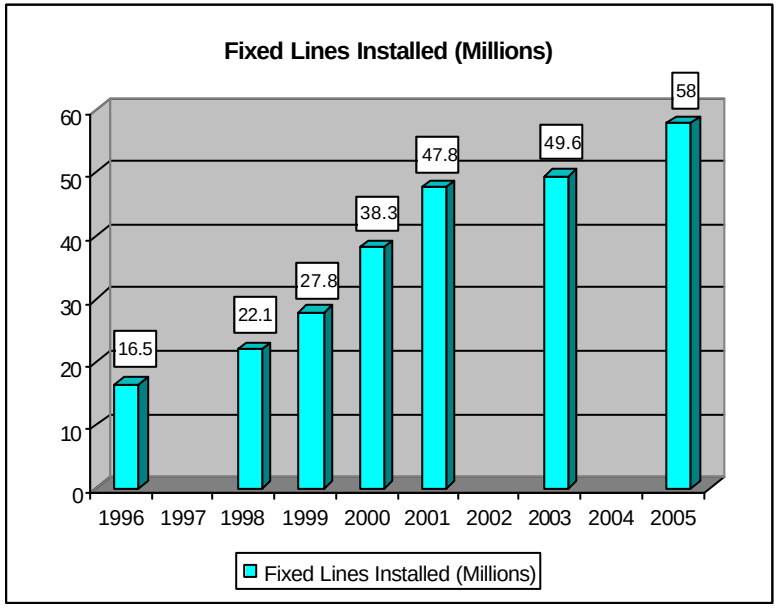
May 20, 2002

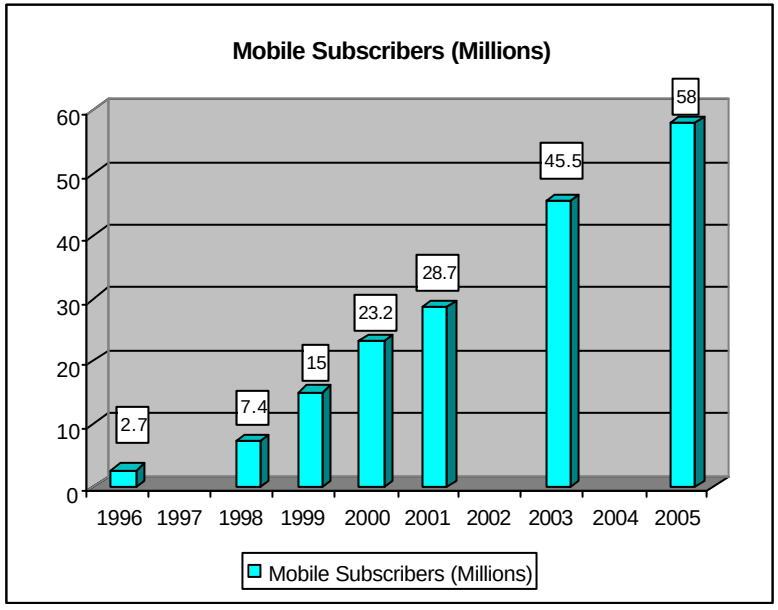
Robert Shaw
<robert.shaw@itu.int>
ITU Internet Strategy and Policy Advisor
International Telecommunication Union

The views expressed in this paper are those of the author and may not necessarily reflect the opinions of the ITU or its membership or the Federative Republic of Brazil.

Telecommunications Environment

- Brazil telecommunication sector legislation and regulation widely regarded as very progressive

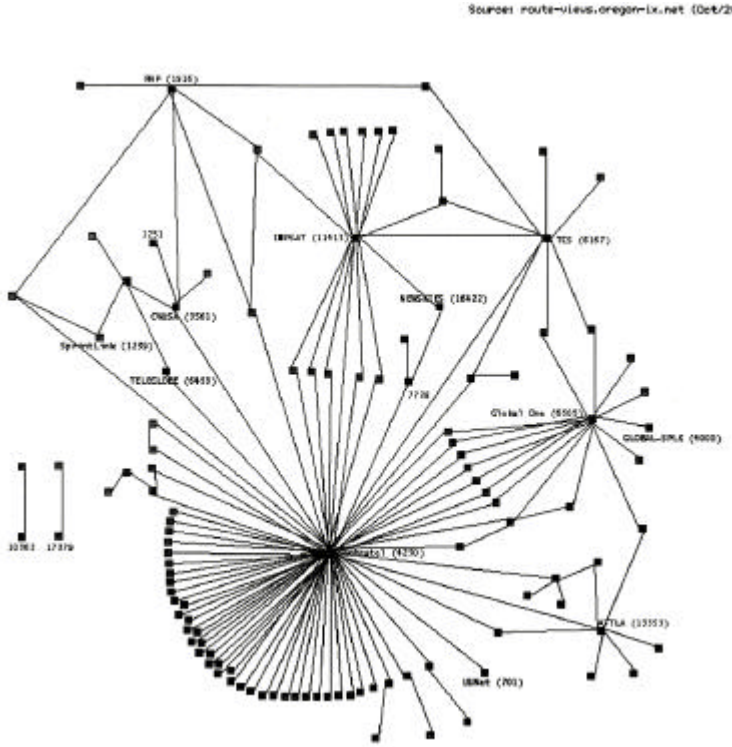




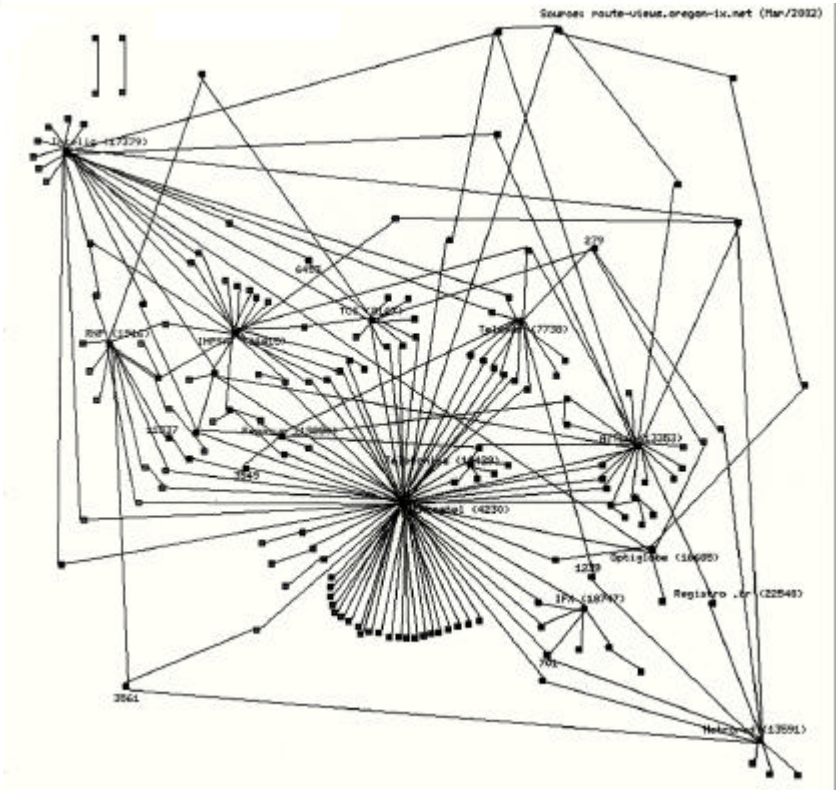
Security & Telecommunications Regulatory Framework

- Generally applies only to “public services”
  - provisions framed within context of Quality of Service licensing provisions
  - Internet services are considered to be value-added services and not regulated
- Even if treated different from regulatory perspective, interests of telecom and Internet providers in operating secure networks are clearly inter-related
- Latter depends almost entirely on the former for backbone infrastructure and access networks

Growth in Brazilian Internet

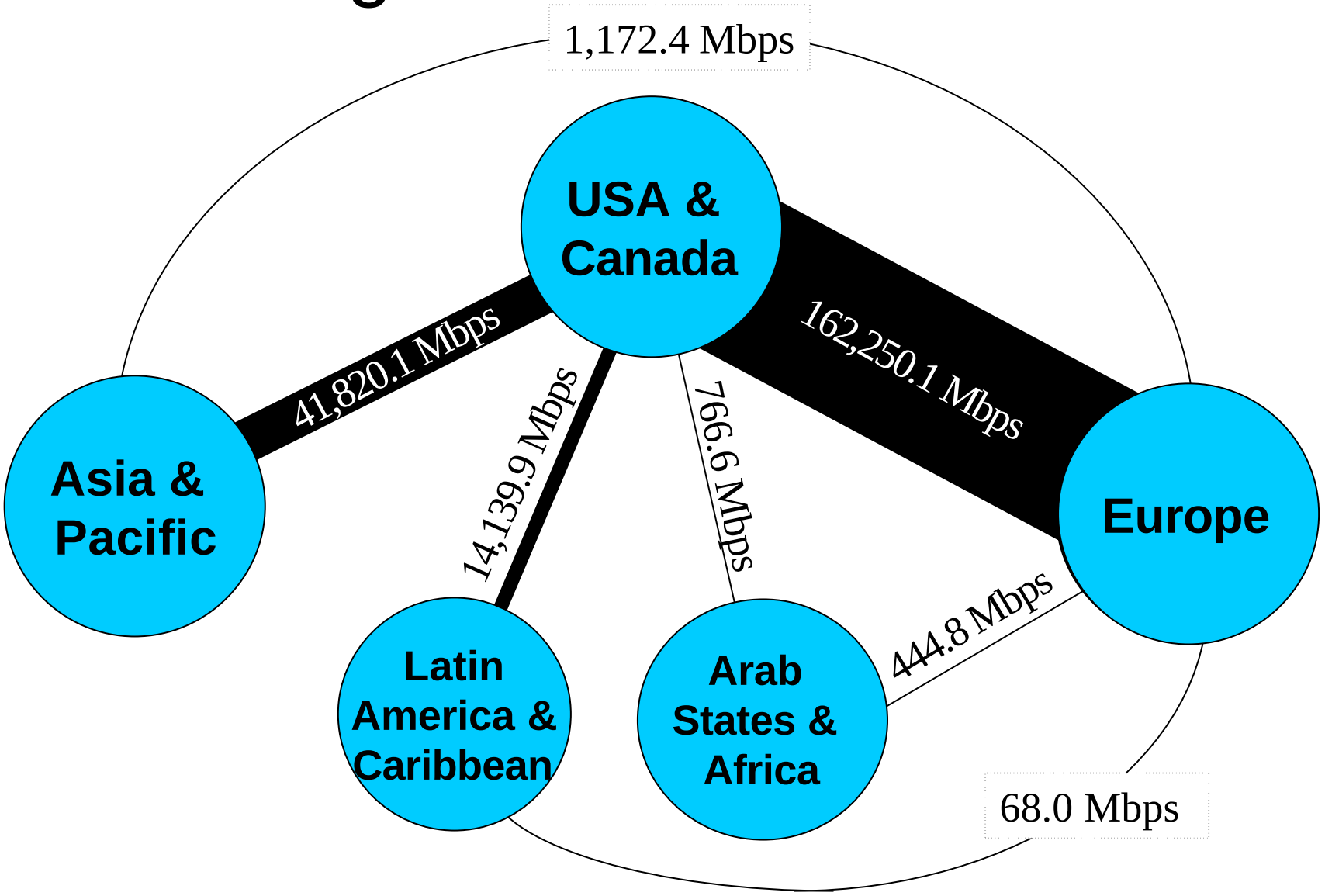


2000



2002

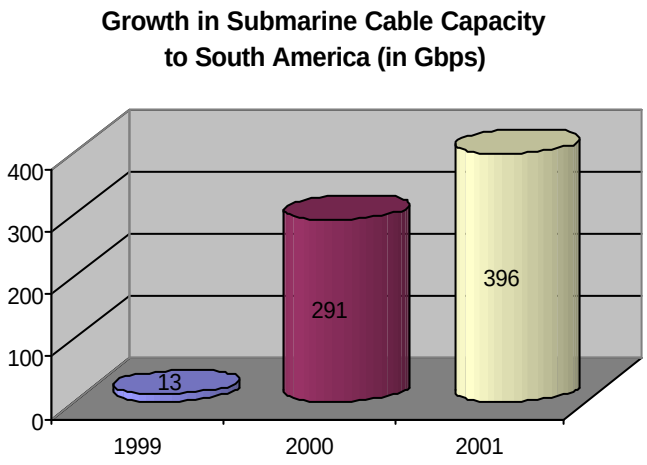
Interregional Internet Bandwidth



Source: TeleGeography Inc., data valid for Mid-2001.

International Internet Connectivity LAC

- mid-2000 to mid-2001, international Internet connectivity to Latin America & Caribbean grew 500%
- Growth twice as fast as any other world region
- 2,500% growth between Latin America countries
- Fastest growth of any intra-regional bandwidth



Source: Telegeography, Packet Geography 2001

The Brazilian Government as Promoter and User of Info-Communication Technologies

- Electronic Government (e-gov) Action plan:
  - to provide through the Internet all government services
  - To promote convergence among governmental information systems, networks & databases;
  - to broaden citizens' access to information
  - to implement an advanced communications & service infrastructure
  - to encourage access to the Internet, mainly by means of public access points
  - to establish a legal and normative framework for electronic communications and transactions
  - to facilitate Internet access throughout Brazil

Some e-gov Goals for 2003

- Provision of more services through the Internet
- Implementation of digital citizen's card
- Electronic payment scheme
- Integrated government online services network
- Electronic Points of Presence (kiosks)
- Wiring schools
- Integrated public safety system over Internet (law enforcement)

Activities to Improve Trust in Network Infrastructures

- Telecommunications and Internet Provider Security Groups
- Brazilian Internet Steering Committee
- Brazilian Country Code Top Level Domain
- Brazilian Computer Emergency Response Team (NBSO)
- Academic and Research Security Groups
- International Cooperation Initiatives of Security Incident Response Teams
- SERPRO
- New Legislative Initiatives
- Policies and Legislation Related to Public Key Infrastructure

Telecommunications and Internet Provider Security Groups

- Depending on size, all providers have either their own internal security policies, security incident response teams or are dependent on “upstream” providers
- For example, large Brazilian ISPs such as UOL, IG and AOL depend extensively on the infrastructure and/or data centers leased from large providers like Embratel, Telemar or Telefónica.
- Cooperation on security issues tends to be minimalist and based on direct personal contacts between technical staff

Brazilian Internet Steering Committee

- Created 1995 by Ministry of Communications & Ministry of Science & Technology:
  - to encourage development of Internet in Brazil;
  - to recommend technical and operational procedures for Internet in Brazil;
  - coordinate attribution of Internet addresses, registration of .br domain names, backbone interconnections;
  - to collect , organize and disseminate information on Internet services.
- Members are government agencies, representatives of providers, industry, users academic community
- Sub-groups on security, produce voluntary recommendations

Brazilian Country Code Top Level Domain (.br)

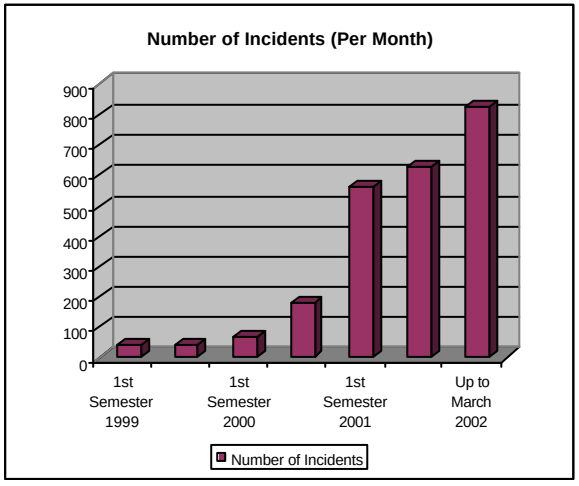
- Operated under the oversight of the Brazilian Internet Steering Committee
- Part of Brazil critical infrastructure
- 450,000 active domains making it one of largest ccTLD registries in world
- Under transfer to new secure faculties, 7 x 24 ops, controlled access, etc.
- Same site to host operations center for LACNIC Regional IP Address Registry

Brazilian Computer Emergency Response Team (NBSO)

- Service-focused organization responsible for receiving, reviewing, and responding to computer security incident reports and activity related to Brazilian Internet:
  - Incident Handling
  - Collaboration
  - Incident Tracking
- NBSO's impression is that growing hacker community in Brazil but mostly "script kiddies" with little sophistication.

Academic and Research Security Groups

- RNP Security Incident Response Team group (CAIS-RNP)
  - Increased number of network security incidents—most recently rapid increase in denial of service attacks
- Many other Brazilian academic Computer Security Incident Response Teams (CSIRTs)



International Cooperation Initiatives

- NBSO and RNP-CAIS Computer Incident Response Teams (CSIRTs) have become members of International Forum of Incident Response and Security Teams (FIRST)
- Brazilian federal law enforcement officials have some cooperation with Interpol on information technology crimes

SERPRO

- Private company owned by the Brazilian government providing networking services to government agencies
- Runs large IP-based government network and IBM SNA network throughout Brazil
- Brazil's electronic tax filing is probably the most important application run by SERPRO

SERPRO Cont.

- Security committee of 35 people who develop government systems security policies
- With integration of government systems, preparing broader Federal security policy to replace individual agency security policies.
- Since 1999, SERPRO has a computer incident response team Grupo de Resposta à Ataques (GRA) that performs:
  - vulnerability analysis of government systems
  - 24 x 7 monitoring.
  - Monitoring provides evidence there are systematic attempts to break into government networks, originating from both commercial service providers and academic networks.

Legislative Initiatives

- One of the objectives of e-gov programme is legal and normative framework for electronic communications & transactions.
- Some existing legislation on cyber-crimes (against government systems) and information security, public key infrastructure provisions
- Much current activity on infosec legislation including much stronger provisions on cyber-crime, privacy, logging

Policies and Legislation Related to Public Key Infrastructure

- Government developing policy and legislative framework for Public Key Infrastructure (PKI) framework (“ICP-Brasil”)
  - extensive legislative activity
- Since January 2002, all official documents exchanged between President, Ministers and other top officials are encrypted and signed with 2048-bit RSA keys
- Goal is that PKI framework will be used to issue digital IDs to all citizens

Some Conclusions

- With government focus on citizen access to online services, realization of need to pay close attention to information and systems security and cyber-crime
- Necessary so citizens will have confidence in use of network infrastructures
- Will include “enabling hand” legislation and regulatory initiatives
- Also involves sustained cooperative initiatives with the private sector, educational community and civil society