



INTERNATIONAL TELECOMMUNICATION UNION

**ITU WORKSHOP ON  
CREATING TRUST IN CRITICAL  
NETWORK INFRASTRUCTURES**

**Document: CNI/06  
20 May 2002**

Seoul, Republic of Korea — 20 - 22 May 2002

---

**CREATING TRUST IN CRITICAL NETWORK  
INFRASTRUCTURES: THE CASE OF BRAZIL**

Draft Version 1.2

This case study was prepared by Robert Shaw <robert.shaw@itu.int>, ITU Internet Strategy and Policy Advisor, Strategy and Policy Unit, International Telecommunication Union (ITU). The report is based on field research undertaken in São Paulo, Brasília, and Rio de Janeiro from 11-19 April 2002, as well as reports and articles identified as footnotes. A list of organizations and persons consulted during the field research is listed in Annex B.

“Creating Trust in Critical Network Infrastructures: The Case of Brazil” forms part of a series of telecommunication country case studies produced under the ITU New Initiatives Programme of the Secretary-General of ITU. Other country case studies may be found on the web page <http://www.itu.int/osg/spu/casestudies/>. Other case studies related to this workshop may be found at: <http://www.itu.int/cni/>.

The invaluable assistance and cooperation of the many organizations in Brazil who agreed to give input to the study is deeply appreciated. Particular mention should be made of the assistance in arranging interviews and access to information provided by ITU’s Americas Regional Office, the Agência Nacional de Telecomunicações do Brasil (Anatel), and the Ministério de Ciência e Tecnologia (MCT), without which this report could not have been prepared.

The views expressed in this report are those of the author and do not necessarily reflect the opinions of ITU, its members, or the Government of the Federative Republic of Brazil.

© 2002 ITU

International Telecommunication Union

Place des Nations

CH-1211 Geneva, Switzerland

## TABLE OF CONTENTS

	<i>Page</i>
1 Introduction .....	5
2 Country background .....	5
2.1 Overview .....	5
2.1 Demography .....	6
2.5 Political environment .....	6
3 Communications in Brazil .....	6
3.1 The telecommunications environment .....	6
3.2 The Internet environment .....	7
3.2.1 Historical development.....	7
3.2.2 Commercialization and growth .....	8
3.2.3 Number of Brazilian Internet users .....	9
3.2.4 Growth of Brazil as an Internet hub in Latin America and the Caribbean .....	10
4 The Brazilian Government as promoter and user of info-communication technologies .....	10
4.1 Introduction .....	10
4.2 Electronic Government programme .....	11
4.3 Main goals .....	11
4.4 Challenges of the digital divide.....	12
5 Current activities to improve trust in network infrastructure .....	13
5.1 Introduction .....	13
5.2 Telecommunications and Internet provider security groups .....	14
5.3 Brazilian Internet Steering Committee.....	15
5.4 Brazilian country code top level domain.....	16
5.5 Brazilian Computer Emergency Response Team (NBSO) .....	17
5.6 Academic and research security groups .....	18
5.6.1 Rede Nacional de Ensino e Pesquisa (RNP) .....	18
5.6.2 Other academic groups .....	19
5.7 SERPRO.....	19
5.8 International cooperation initiatives .....	20
5.9 New legislative initiatives .....	21
5.10 Policies and legislation related to a public key infrastructure.....	21
5.10.1 Implementation of the Brazilian Payment System .....	22
6 Conclusions .....	23
Annex A: Brazil basic indicators .....	25
Annex B: Organizations consulted .....	27
Annex C: The Federal Government Redegoverno portal .....	31



## 1 Introduction

The development of advanced info-communication networks is a key objective for governments around the world. Not only are these networks seen as an important determinant of national competitiveness in an increasingly globalized knowledge economy, they are also seen as offering new opportunities in areas such as education, health and social advancement. Brazil, a country of wide ranges of social and economic development, has put a high priority on improving access to advanced info-communications technologies, promoting digital literacy and improved access to government public services.

These laudable goals pose considerable challenges: there are social and economic limitations that currently hinder access by much of Brazil's population to technologies like the Internet. Yet, despite this "digital divide", Brazil has made some remarkable achievements. In only a few years, through telecommunication market liberalization and pro-competitive regulation, the government has dramatically increased access to basic telecom services for its citizens. After the privatization of its incumbent operator and opening of the market to new entrants, there has been extensive investment in expanding national networks and international connectivity. In just a few years, large commercial Internet backbone networks have been built throughout the country. Today, the Federal government offers a broad range of services through the Internet and has even more ambitious plans for the coming years to improve access and provide new applications to its citizens. In certain domains, such as online tax filing, Brazil is years ahead of other countries<sup>1</sup>.

This rapid transformation makes Brazil an interesting case to consider in terms of how it is addressing the problems of security of information systems and protection of network infrastructure. As in all countries, both the public and private sector are attempting to come to grips with the appropriate technology, processes, policies and laws to secure advanced info-communication systems. With the Brazilian Government's focus on providing its citizens with universal access to online services, it has accurately realized that it needs to pay closer attention to the topic of security and cyber-crime, including reviewing its legislative and regulatory frameworks. This report attempts to give a snapshot of some of the related current initiatives in the Brazilian public and private sectors.

Several caveats warrant a mention. First, any report on a topic as broad as information systems security and network infrastructure protection, particularly for a country as large as Brazil, is almost by definition incomplete. Second, in sensitive areas such as banking or other high-tech cyber-crime activities, there is typically little or no public information available. Third, this report is in draft form and is subject to follow-up review by the organizations and persons consulted during the field research for the study—hopefully they will provide any necessary additional information, corrections of fact or interpretation.

This report, *Creating Trust in Critical Network Infrastructures: The Case of Brazil*, is structured into the following sections: Section 2 of this report provides a basic country background on Brazil. Section 3 provides an overview of Brazil's telecommunications and Internet environment. Section 4 discusses the Brazilian Government as a promoter and user of info-communication technologies—particularly its ambitious Electronic Government (e-gov) Programme. Section 5 discusses some specific activities undertaken by the public and private sector to improve trust in usage of Brazil's info-communications networks. Finally, Section 6 makes some concluding remarks.

## 2 Country background<sup>1</sup>

### 2.1 Overview

Brazil is the fifth largest country in the world in terms of area, after Russia, China, Canada, and the United States. It makes up nearly half the total area of South America, bordering every country except Chile and Ecuador (see Figure 2.1). With a population of approximately 170 million people, it is ranked as the sixth most populous nation in the world. The only Portuguese-speaking nation in the Americas, Brazil has by far the largest economy in Latin America with an estimated GDP of USD 1,13 trillion and an annual growth rate of 4.2 per cent (2000 estimate).

---

<sup>1</sup> 15 million Brazilian citizens sent in their tax filings via the Internet in 2002, representing more than 95% of all filings.

Figure 2.1: Map of Brazil



Source: CIA World Factbook

In the late half of the 20th century Brazil has taken its place on the world stage as a considerable global economic force, a regional leader politically, and a coveted destination for foreign direct investment.<sup>2</sup>

## 2.1 Demography

Brazil is a diverse nation whose inhabitants trace their roots to the indigenous peoples of the Americas, Europe, Africa and Asia. Four major groups make up the Brazilian population: the Portuguese, who colonized Brazil in the 16th century; Africans; various other European, Middle Eastern, and Asian immigrant groups who have settled in Brazil since the mid-19th century; and indigenous people of Tupi and Guarani language stock. Subsequent waves of immigration have contributed to an extremely diverse ethnic and cultural heritage.

Urbanization has been a major driving force affecting the Brazilian landscape since the mid-20th century. By 1991, 75 per cent of the total population was living in urban areas. This urbanization has helped to concentrate the majority of the population in the industrialized Atlantic coastal areas of

the southeastern and northeastern states such as the megalopolises of São Paulo and Rio de Janeiro as well as the northeastern cities of Salvador (Bahia) and Recife. The southeastern states such as São Paulo, Rio de Janeiro, and Espírito Santo are much more industrialized and wealthier than the northeastern and interior states such as Bahia, Rio Grande do Norte, and Amazonas.

## 2.5 Political environment

Brazil is a federative republic made up of 26 states, each state having its own government and governor. The Brazilian Constitution has maintained the presidential system and three independent powers: the executive, legislative, and judiciary.

The Brazilian national legislature is the National Congress, which is composed of two houses, the Chamber of Deputies and the Federal Senate. The number of members from each State and Federal District in the Chamber of Deputies is proportional to its population. Deputies are elected for four-year terms by direct ballot. The Senate is composed of three Senators from each State and the Federal District and are elected for a term of eight years. Senatorial elections are staggered (one-third and then two-thirds) every four years, in elections held concomitantly with those for the Chamber of Deputies. A Deputy and a Senator can stand for re-election without restriction. In 2001, there were 81 Senators and 513 members of the Chamber of Deputies.

The Brazilian President, who is allowed a single re-election, heads the Executive Branch, which, in turn, consists of 18 Executive Branch agencies. The current President, Fernando Henrique Cardoso, was re-elected in the autumn of 1998 for an additional four-year term, meaning that new elections are due to be held at the end of 2002.

## 3 Communications in Brazil

### 3.1 The telecommunications environment

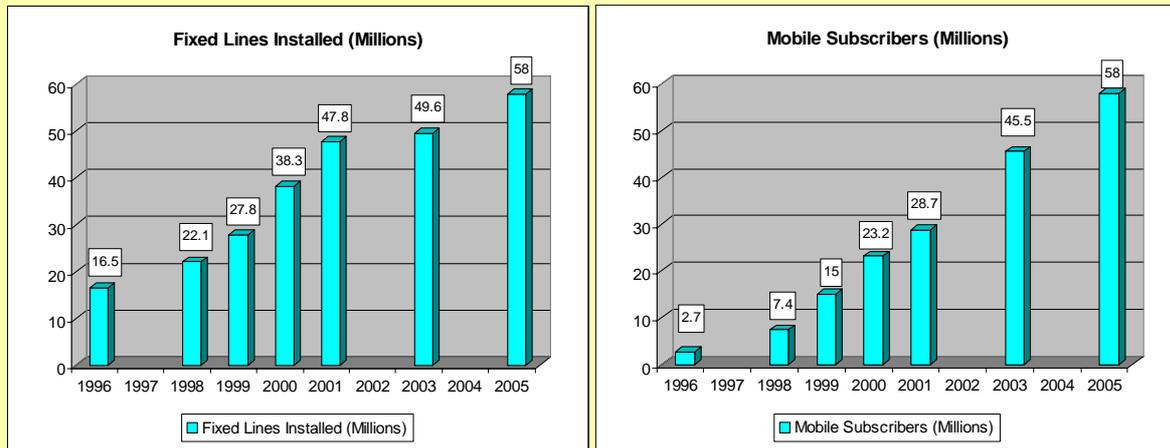
Today, Brazil's telecommunication sector legislation and regulation is widely regarded as very progressive due to large-scale privatization and pro-competitive regulation. This achievement began with the passage of the 1996 Minimum Law that liberalized mobile services. This was followed by the adoption of the General

<sup>2</sup> Foreign direct investment set a record of more than USD 30 billion in 2000 according to the CIA World Factbook 2001 at <http://www.cia.gov/cia/publications/factbook/>.

Telecommunications Law of 1997, which called for the creation of an independent regulator, the Agência Nacional de Telecomunicações (Anatel). It also established guidelines for the privatization of the monopoly incumbent telecommunications provider, Telebrás. This law effectively ended the State's role in the provision of telecommunications services, changing its role from supplier to a regulator of services. Telebrás was broken up into twelve separate holding companies and in 1998, the government sold off 100 per cent of its interests in Telebrás.

**Figure 3.1: Brazil: Growth in fixed lines installed and mobile subscribers**

*Growth in fixed lines installed and mobile subscribers 1996-2005 (2003-2005 estimated)*



Source: Anatel.

Anatel, Brazil's regulator, is often praised by industry and other regulators around the globe as one of the most transparent and independent in the world.<sup>3</sup> Under Anatel's initiatives, the number of fixed telephone lines has grown substantively to 47.8 million, to which can be added 28.7 million mobile subscribers (2001) (see Figure 3.1). A timeline series (1997-2001) of basic Brazil telecommunication indicators showing substantial growth can be found in Annex A.

## 3.2 The Internet environment

### 3.2.1 Historical development

The genesis of the Brazilian Internet can be traced back to 1988 when Brazilian researchers first obtained international network access.<sup>4</sup> Already in 1997, the importance of interconnecting computer networks for the academic community had been recognized and a number of independent projects had been initiated. The first initiative was a 9600 bps BITNET<sup>5</sup> link from the Laboratório Nacional de Computação Científica (LNCC)<sup>6</sup> in Rio de Janeiro to the University of Maryland in the USA. This was followed by a second international link of 4800 bps between FAPESP<sup>7</sup> in São Paulo to Fermilab in Chicago. This was followed by a third 4,800 bps link established between the Federal University of Rio de Janeiro (UFRJ)<sup>8</sup> and the University of California in Los Angeles (UCLA).

<sup>3</sup> See <http://www.itu.int/itudoc/itu-d/publicat/74954.html>.

<sup>4</sup> For a history of the development of networking in Brazil, see *Non-Commercial Networking in Brazil*, Michael A. Stanton, INET '93 Proceedings and <http://www.rnp.br/rnp/rnp-historico.html>.

<sup>5</sup> See <http://www.cren.net/cren/cren-hist-fut.html>.

<sup>6</sup> LNCC was created by CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) in 1980. See <http://www.lncc.br>.

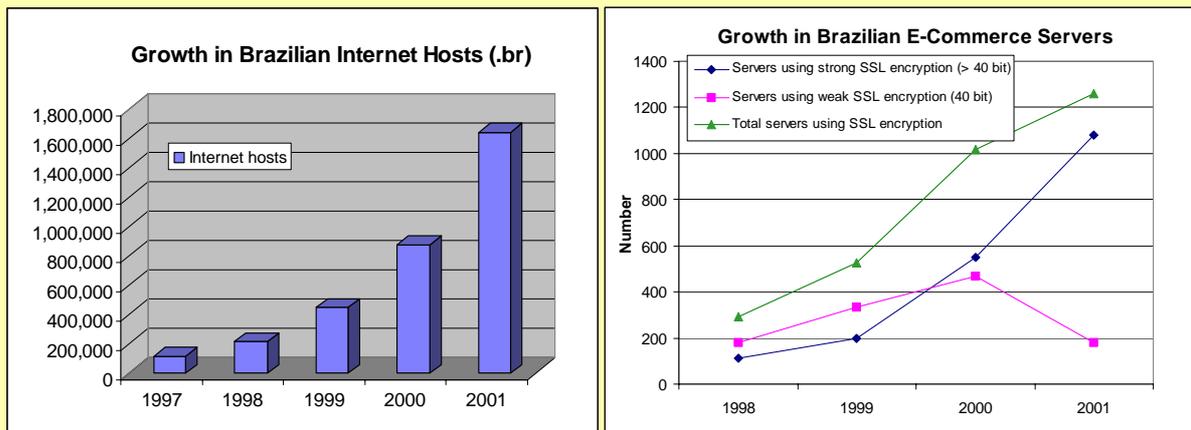
<sup>7</sup> Fundação de Amparo à Pesquisa do Estado de São Paulo (The State of São Paulo Research Foundation). See <http://www.fapesp.br/>.

<sup>8</sup> <http://www.ufrj.br/>

Realizing it would be better to coordinate separate initiatives and secure integration of regional networks into a national network, the Ministry of Science and Technology created the Rede Nacional de Ensino e Pesquisa (RNP)<sup>9</sup> in 1989. RNP's mission was to operate a backbone network dedicated to teaching and research institutions and government agencies. The period from 1991 to 1993 was dedicated to the construction of the RNP backbone network, as well as to fostering related education initiatives in networking. From 1994 onwards, there was a rapid increase in the number of connected institutions, which in turn drove further demands on the backbone network. During the 1994-1998 timeframe, the backbone was continuously upgraded with higher speed connections. This network became the basic platform for the early development of Internet technology and applications in Brazil.

**Figure 3.2: Brazilian Internet: Rapid Growth**

*Brazilian Internet growth in Internet hosts and Growth in secure Brazilian e-commerce servers*



Source: ITU World Telecommunication Indicators Database, Internet Software Consortium, Netcraft Secure Server Survey.

### 3.2.2 Commercialization and growth

In May 1995, commercial Internet activity began in Brazil. At that time RNP went through a temporary redefinition of its role, where it no longer restricted access to its backbone to academia, but also to other sectors of society, in particular commercial users. This provided an important stimulant to the growth of the commercial Brazilian Internet. After the opening of the Internet service provider (ISP) market in 1995, Brazil sustained continuous high growth rates in Internet deployment and usage. Today, in 2002, there are more than 1,200 ISPs operating in Brazil.

After the privatization of Telebrás and deregulation in 1998 (see Section 3.1), new carriers began to invest in fiber optic networks, submarine cables and other telecommunications infrastructure. The privatized companies simultaneously initiated ambitious programmes to expand and improve their networks. Embratel, now owned by WorldCom, was the first operator of a commercial Internet backbone network. Likewise, Telefónica built an IP network covering the state of São Paulo and interconnecting all the states included in its concession area to its own Internet backbone. Although Embratel previously dominated the Brazilian Internet backbone, a number of new providers, network access points and meshing of infrastructure have added to the backbone during the last few years (see Figure 3.3).

Statistics show that a large percentage (75-80%) of Brazilian Internet traffic is internal to the country (driven by local Portuguese-based content), which argues for the build-out of Network Access Points (NAPs) for localized traffic exchange (e.g. see Ambranet NAP reference in Section 5.2).

RNP has now returned to its academic and research roots and is focused on the development of the next generation of Internet networks, connecting the entire nation through a high performance academic network

<sup>9</sup> <http://www.rnp.br>

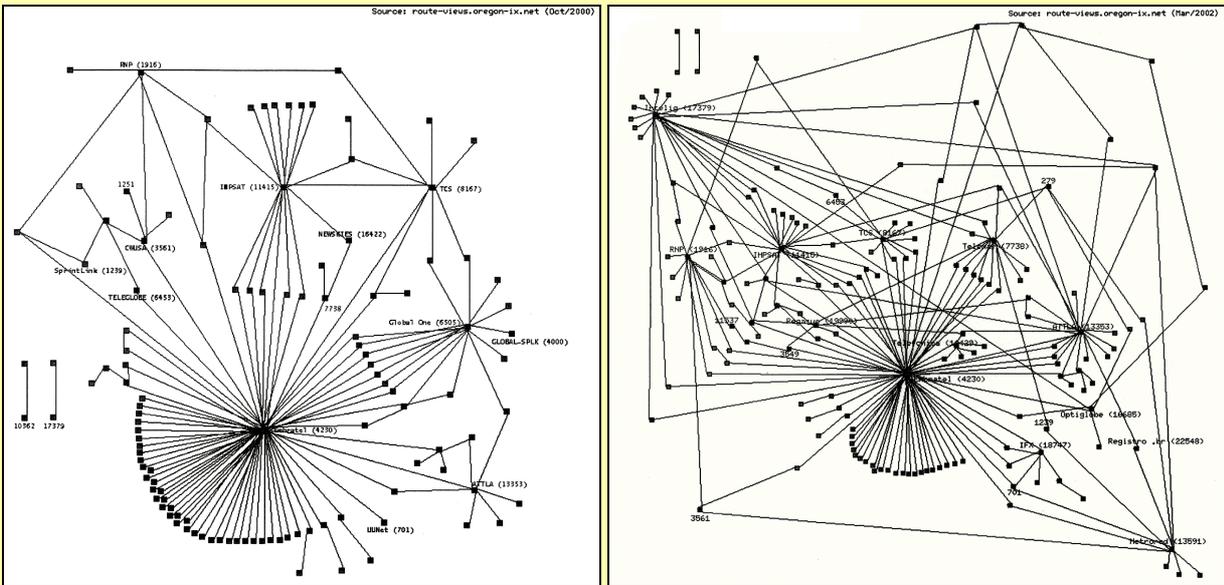
called RNP2 that will interconnect with the US Internet2 initiative. In May 2000, the new RNP2 backbone was launched, which reaches all Brazilian states and has a capacity of up to 155 Mbps. RNP is further discussed in Section 5.6 in the context of its security-related initiatives.

**Figure 3.3: Brazilian Internet backbone: 2000 and 2002**

Snapshots of Brazilian Internet backbone in 2000 and 2002<sup>10</sup> The backbone in 2000 shows Embratel's network (bottom centre) as a clearly dominant provider. On the right side, in 2002, there are many new providers, more coverage, as well as much more complex interconnection relationships.

Brazil Backbone 2000

Brazil Backbone 2002



Source: Frederico Neves, Registro.br.

### 3.2.3 Number of Brazilian Internet users

There are different estimates for the exact number of Internet users in Brazil. The ITU World Telecommunication Indicators Database estimates that there were 8 million Internet users in Brazil at the end of 2001. Anatel has given estimates of 15-16 million Internet users during the same period, equivalent to roughly half the number of all Internet users in Latin America. A recent presentation on the Electronic Government (e-gov) Programme (see Section 4.2) from the Executive Committee of the Electronic Government Secretariat of Logistics & Information Technology Ministry of Planning, Management and Budget, gives a figure of 23 million.

<sup>10</sup> These maps were produced by Otter, a network visualization tool. See <http://www.caida.org/tools/visualization/otter/>.

### 3.2.4 Growth of Brazil as an Internet hub in Latin America and the Caribbean

Because of the Internet's historical origins, its architecture means that a major portion of international Internet traffic continues to transit via the United States.<sup>11</sup> For example, Internet traffic between Peru and Brazil could easily transit via the United States through Miami.<sup>12</sup> However, with the growth of new regional and international connectivity and exchange points, this phenomenon is rapidly changing. As an example, from mid-2000 to mid-2001, international Internet connectivity to Latin American and Caribbean (LAC) countries grew 500 per cent in terms of deployed bandwidth: twice as fast as any other region in the world. Even more impressive, during the same period, Internet connectivity *between* LAC countries grew at the rate of 2,500 per cent. The same data suggests that São Paulo has now emerged as a major hub for international traffic exchange in the LAC region<sup>13</sup>, trailing only Miami (see Table 3.1).

**Table 3.1: Top Latin America & Caribbean Internet hub cities in 2001**

Rank	City, country	Internet bandwidth (Mbps)
1	Miami, USA	7,825
2	São Paulo, Brazil	4,984
3	Buenos Aires, Argentina	4,017
4	Mexico City, Mexico	2,182
5	New York, USA	2,003
6	Santiago, Chile	1,770
7	Dallas, USA	1,546
8	Monterrey, Mexico	1,077
9	Rio de Janeiro, Brazil	1,029
10	Los Angeles, USA	975

Source: Packet Geography 2001, Telegeography

## 4 The Brazilian Government as promoter and user of info-communication technologies

### 4.1 Introduction

The Brazilian Government has placed a high priority on the adoption of advanced information communication technologies for its administrative processes and delivery of services to citizens. This has already produced remarkable achievements. For example, the Federal Government already offers a broad range of services through the Internet; most of them are available through the Redegoverno portal<sup>14</sup>, which includes more than 2,000 services and 20 thousand different categories of information (see Annex C). Some of the more notable services available to citizens over the Internet include:

<sup>11</sup> See slide 3 at [http://www.itu.int/osg/spu/spuactivities/2001/17-20OctoberConnect2001\[1\].ppt](http://www.itu.int/osg/spu/spuactivities/2001/17-20OctoberConnect2001[1].ppt).

<sup>12</sup> For example, currently RNP's two major international links are to the United States (155 Mbps to New York City and 45 Mbps to Miami). See Section 5.6.

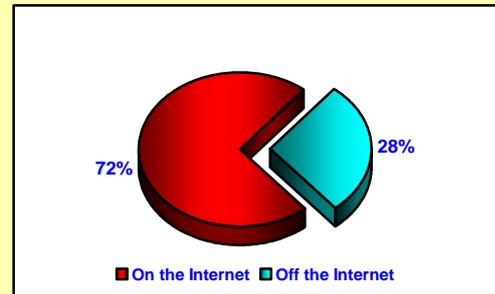
<sup>13</sup> Packet Geography 2001, Telegeography

<sup>14</sup> <http://www.redegoverno.gov.br>

- filing income-tax returns;
- issuing statements on the payment of taxes;
- publicizing notices related to government procurement;
- enrolling in school for elementary education;
- follow-up of court cases;
- accessing economic and social indicators and census data;
- delivering information on retirement and social-security benefits;
- long-distance learning programmes;
- sending messages by mail, through public kiosks;
- information on Federal Government programmes.

**Figure 4.1: Federal Services Online**

*Percentage of Brazilian Federal Government services available on the Internet*



*Source:* Ministério do Planejamento, Orçamento e Gestão, Secretariat de Logística e Tecnologia da Informação

### 4.2 Electronic Government programme

To articulate and focus the different initiatives and projects providing universal access to services delivered by the government, an Electronic Government (e-gov) Programme was launched, under the leadership of the Presidency of the Republic. The e-gov Programme is coordinated through an interministerial committee and complements the Ministry of Science and Technology's Information Society programme<sup>15</sup>. The e-gov programme main action plans include:

- to provide, through the Internet, all services rendered to the citizens, with improved quality standards, cost reduction and easy access;
- to promote convergence among governmental information systems, networks and databases;
- to broaden citizens' access to information, in appropriate formats;
- to implement an advanced communications and service infrastructure;
- to make use of the Federal Government's purchasing power on the procurement side;
- to encourage access to the Internet, mainly by means of public access points hosted by public, private and community institutions;
- to establish a legal and normative framework for electronic communications and transactions;
- to facilitate Internet access throughout Brazil.

The Brazilian policy for electronic government forecasts governmental action on three fundamental fronts: interaction with citizens; improvement of its own internal management, and integration with partners and providers. In addition, the Federal Government is developing policies for the secure authentication and management of information, which includes putting into place standards and enabling legislation for electronic certification and authentication, including a public key infrastructure (PKI) framework called ICP-Brasil<sup>16</sup> (discussed in Section 5.10).

### 4.3 Main goals

Some of the e-gov Programme goals to be implemented by 2003 include:

<sup>15</sup> See <http://www.mct.gov.br/Temas/Socinfo/Default.htm>.

<sup>16</sup> See <http://www.icpbrasil.gov.br>.

- **The provision of services and information through the Internet.** All governmental bodies are to define and publicize their policy for information and delivering services to the public, through the Internet or other means of electronic communication. This includes providing a list of services and information to be provided through electronic means, the definition of officials in charge of these services and information, the development of standards on confidentiality and privacy, and the definition of the procedures for obtaining services or information.
- **The implementation of digital citizen's card,** by means of which citizens may have access to all information and services required, such as social security, health and employment, in addition to the payment of benefits. The Federal Government will be the certifying authority (see Section 5.10).
- **The implementation of an electronic payment scheme.** To put in place a service for the receipt of electronic payments of fees, taxes, contributions, real-estate transfer fees and others, allowing the delivery, through the Internet, of the full cycle of services to citizens (see references in Section 5.10.1).
- **The implementation of an integrated multi-service network for the Federal Government (Br@sil.gov<sup>17</sup>),** integrating its Ministries and other administrative units (see discussion in Section 5.7).
- To put in place an **auction system for Federal Government procurement.**
- **To put in place electronic points of presence (PEP),** allowing free access to services delivered by the Federal Government, through the Internet, encompassing, particularly, the domains of education, health, social security, labour, safety and human rights.
- **To put in place an IT programme for educational actions,** coordinated by the Ministry of Education, aimed at equipping citizens for the use of technological resources and services provided by electronic means, with the following targets, including, *inter alia*:
  - to connect all secondary public schools (approximately 13,000);
  - to connect all 62 thousand public schools served by TV School;
  - to connect all public and school libraries (target date of 2006);
- **To put into place a national network for information on health** for the exchange of information and other health services, a health portal, a national health card, long-distance training programme, support for tele-medicine initiatives.
- **To support states and municipalities in the development of an integrated public safety system,** coordinated by the Ministry of Justice, allowing citizens to report police events through the Internet. This system would be reinforced by equipping street police patrols and police precincts, allowing the police authorities to sensor and locate police cars for the purposes of answering calls, including electronic ones.

#### 4.4 Challenges of the digital divide

The Brazilian electronic government initiatives are challenging, as there remain many social and economic limitations that currently hinder access by much of Brazil's population to advanced info-communication technology such as the Internet. In many aspects, the e-gov initiative seems to be somewhat in advance of the capabilities of Brazil's citizens.

Currently, estimates of the number of users of the Internet in Brazil run from 8 to 23 million<sup>18</sup> out of a population of 170 million. Government initiatives geared to facilitating universal access to info-communication technology depend greatly on universal service funds (FUST) coming from the

---

<sup>17</sup> See [http://www.anatel.gov.br/comites\\_comissoes/comites/infra\\_estrutura/brasil\\_gov.pdf](http://www.anatel.gov.br/comites_comissoes/comites/infra_estrutura/brasil_gov.pdf).

<sup>18</sup> The ITU World Telecommunication Indicators Database gives a figure of 8 million for 2001. Anatel estimates there were 16 million Internet users in 2001. An April 2002 presentation from the Executive Committee of the Electronic Government Secretariat of Logistics & Information Technology Ministry of Planning, Management & Budget uses a figure of 23 million.

telecommunication sector.<sup>19</sup> Towards that goal, Anatel has articulated, in cooperation with other Federal Government bodies, a number of specific projects in areas such as education, health and public security. In particular, with the goal of making access to the Internet in Brazil more universal, a number of targeted measures to overcome “digital divide” obstacles are under way:

- According to Anatel, 93 per cent of current Internet users use fixed telephone services as their means of connection to the Internet. While there has been great progress towards the provision of basic telecommunication services following privatization, access is still limited to about 40 per cent of the population. Therefore, this brings additional impetus to Anatel’s goal of providing wide universal access to basic telecommunication services.
- One of the barriers to Internet access is the price of conventional telephone services vis-à-vis Internet usage patterns and the access points provided by ISPs. Specifically, there are no differentiated categories of tariffs tailored to the longer call times typical with dial-up Internet usage. This is a critical issue as, according to Anatel, 44 per cent of Brazil’s population (around 75 million people) do not have access to local dial-up access to an ISP and therefore would incur long-distance charges for Internet use. To address this problem, Anatel has recently issued a public consultation outlining various possible scenarios to facilitate access by the general public to the Internet, including an unusual “Direct IP” access model<sup>20</sup>.
- The general low levels of per-capita income and cost of information-technology equipment such as PCs and connectivity remain a stumbling block. The government is taking a number of initiatives including, *inter alia*, tax incentives, low-cost personal computer initiatives, provision of lines of credit for the acquisition of equipment and installation of kiosks to enable access to Federal Government Internet-based services. For example, Brazil’s postal agency, Correios<sup>21</sup>, will install computer kiosks for all 5,561 municipalities where people will be able to access the Internet and use e-mail. Another goal is provide every Brazilian citizen with a free private e-mail account and electronic payment delivery mechanisms.
- Finally, much of the population lacks the necessary education and familiarity with new information-communication technologies and services. Of a number of government initiatives, particular mention could be made of the initiatives to wire schools (see Section 4.3), education programmes in computer science and the Ministry of Science and Technology’s Softex programme<sup>22</sup>, which is fostering the development of a Brazilian software industry. The latter has already demonstrated some clear benefits with the rapid growth of the northeast of Brazil as a high-tech region<sup>23</sup> that is attracting considerable foreign direct investment.<sup>24</sup>

## 5 Current activities to improve trust in network infrastructure

### 5.1 Introduction

Generally, within the Brazilian telecommunication regulatory framework, there is a key differentiation between those who provide services in the private environment and those who provide them in the public context. Only in the latter case does the general telecommunications regulatory framework apply. In the context of network security, telecommunications regulation is generally focused on provision of certain broad levels of quality of service (QoS), rather than specific details related to network security. In particular,

---

<sup>19</sup> See [http://www.connect-world.com/past\\_issues/latin\\_america/2001/fourth\\_quarter/a\\_p\\_c\\_netto\\_ANATEL\\_2001.asp](http://www.connect-world.com/past_issues/latin_america/2001/fourth_quarter/a_p_c_netto_ANATEL_2001.asp) for an excellent review of how the FUST fund is being used to address digital divide issues.

<sup>20</sup> See <http://200.252.158.173/sacp/Contribuicoes/TextoConsulta.asp?CodProcesso=C263&Tipo=1&Opcao=realizadas>.

<sup>21</sup> <http://www.correios.com.br/>.

<sup>22</sup> <http://www.softex.br/>.

<sup>23</sup> <http://www.wired.com/news/business/0,1367,49649,00.html>.

<sup>24</sup> The Brazilian software market currently totals about USD 4.2 billion of which about 75 per cent is developed solely for the Brazilian market. There is little exportation of software developed in Brazil (estimated USD 100 million).

when an operator is granted a concession by Anatel, it needs to comply with certain QoS standards which are specified in contracts, with conditions related to emergency services, prioritization of traffic, reporting on downtime, etc.<sup>25</sup>

From a regulatory perspective, Internet services are considered to be value-added services and are generally not regulated by Anatel. However, even if treated as formally different from a regulatory perspective, the interests of the telecommunication providers and Internet providers in operating secure networks are clearly synergistic: in fact, the latter depend almost entirely on the former for both backbone infrastructure and access networks.<sup>26</sup> Some of the ways in which private sector telecommunication and Internet providers are addressing security are further discussed in Section 5.2.

As mentioned earlier (Section 4.2), one of the objectives of the Electronic Government (e-gov) Programme is to establish a legal and normative framework for electronic communications and transactions. There is some existing legislation concerning cyber-crimes against the government (Law 9.983), a policy for information security management (Decree 3.505<sup>27</sup>), and a decree concerning electronic documents delivery (Decree 3.585). Additional cyber-crime and privacy of communications legislation is under debate and is discussed in Section 5.8.

Perhaps one explicit recognition of the common interests of the government, telecommunication and Internet sectors in promoting secure usage of advanced networks is that several Federal Government agencies, including Anatel, are involved in what might be characterized as “co-regulation” activities in the organizational form of a public-private sector body, the Brazilian Internet Steering Committee. This Committee, a somewhat innovative construct, performs several important roles. For example, it has spawned subgroups on security, has oversight over the allocation of Internet names and addresses, and oversees the management of the Brazilian country code top level domain “.br”, which should be considered crucial to Brazil’s national critical infrastructure. That said, some of the Steering Committee’s activities, discussed below in Section 5.3, appear to be somewhat overtaken by some areas of Internet-related regulation and legislation (see Section 5.8).

### 5.2 Telecommunications and Internet provider security groups

Depending on their size, all telecommunications and Internet providers in Brazil either have their own internal security policies and security incident response teams, or are dependent on “upstream” infrastructure providers for security services. For example, large Brazilian ISPs such as UOL, IG and AOL depend extensively on the infrastructure and/or data centres leased from large providers like Embratel, Telemar or Telefônica. Where there is cooperation on security issues between backbone or access providers (who are often competitors), this tends to be minimalist and typically based on direct personal contacts between technical staff rather than on formal arrangements. Several of the organizations interviewed in the field research for this report suggested that more formal arrangements were needed.

Large trade associations, such as the Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet (Abranet)<sup>28</sup>, made up of 350 Brazilian ISPs, ASPs<sup>29</sup> and content providers, play an important role in representing and coordinating the interests of this sector, including in the Brazilian Internet Steering Committee (see Section 5.3). Abranet also runs a NAP where its members can securely exchange traffic. Perhaps even more important, Abranet has played a key role in formulating and disseminating security practices for users and providers, which are further promulgated by the Brazilian Internet Steering Committee to other industry sectors.

Abranet’s general public policy stance is one of preference for minimalist regulation. It spends a considerable effort in education of users and legislators. Its members tend to cooperate in following the self-

---

<sup>25</sup> See Articles 30 and 31 of the General Regulations of Telecommunication Services.

<sup>26</sup> According to Anatel, 93 per cent of current Internet users use the fixed telephone services as their means of connection to the Internet.

<sup>27</sup> [http://www.presidencia.gov.br/ccivil\\_03/decreto/D3505.htm](http://www.presidencia.gov.br/ccivil_03/decreto/D3505.htm).

<sup>28</sup> <http://www.abranet.org.br/>.

<sup>29</sup> Application Service Providers.

regulation security-related recommendations made by the Steering Committee—such as the retention of logging records of user activities for three years<sup>30</sup> for the eventual needs of law enforcement<sup>31</sup> (see Section 5.3). All the providers interviewed indicated that such requests were extremely rare.

Commercial backbone providers and ISPs that are known to have active formal security groups include AT&T Latin America, COMSAT, Diveo, Embratel, EQUANT, Matrix, Telefónica, UOL, and Telemar.

### **Box 5.1: Telemar tracks down a hacker**

Telemar, a major telecommunications provider in Brazil operating in 16 states, has two dedicated security incident response teams: one for its customer networks and one for its internal corporate network. Several months ago, Telemar received a number of complaints that its network was being used to probe other networks for weaknesses. If the weaknesses were found, a virus was introduced which allowed a hacker to take over the remote machine with full access privileges. The Telemar security teams reset their firewall systems to specifically look for this attack and using call line identification were able to track down the hacker to the Pernambuco area in the northeast of Brazil. The hacker had been using a dial-up connection to break into the Telemar corporate network from which he was able to move successfully out onto the public Internet. With the information provided by the cooperating Telemar security teams, the Brazilian federal police arrested him. One of the hacker's attempted break-ins had made it a federal crime: a failed attack on the Brazilian Central Bank.

There is a general view among providers that, since the terrorist attacks of 11 September 2001 in the United States, much more attention has been paid by upper management to security issues and contingency planning. As an example, AT&T Latin America is now considering establishing a Security Operations Centre (SOC) for its Latin American and Caribbean operations. Most of the major operators cooperate with NBSO (see Section 5.5) on discussion and formulation security policies. In some cases, for special customer needs, providers are working with outsource companies for security services.

### **5.3 Brazilian Internet Steering Committee**

In a Joint Declaration of May 1995<sup>32</sup>, the Brazilian Ministry of Communications<sup>33</sup> (MC) and the Ministry of Science and Technology (MCT)<sup>34</sup> announced the creation of the Brazilian Internet Steering Committee (Comitê Gestor da Internet no Brasil).<sup>35</sup> Its purpose is to promote strong participation by society in the decisions, administration and implementation of the Internet in Brazil. The Committee is made up of members of government agencies, backbone operators, representatives of the Internet service provider industry, users and the academic community. The Steering Committee's main objectives include<sup>36</sup>:

- to encourage the development of Internet services in Brazil;
- to recommend technical and operational procedures for the Internet in Brazil;
- to coordinate the attribution of Internet addresses, the registration of domain names and backbone interconnections;
- to collect, organize and disseminate information on Internet services.

---

<sup>30</sup> The availability of which would only be subject to a court order. Of the providers interviewed, only one could recall an incident where a request for logging records had been made.

<sup>31</sup> <http://www.cg.org.br/acoed/desenvolvimento.htm>

<sup>32</sup> <http://www.cg.org.br/regulamentacao/notas.htm>

<sup>33</sup> <http://www.mc.gov.br/>

<sup>34</sup> <http://www.mct.gov.br/>

<sup>35</sup> <http://www.cg.org.br/>

<sup>36</sup> <http://www.cg.org.br/sobre-cg/apresentacao.htm>

The Committee was created by Interministerial Ordinance Number 147.<sup>37</sup> The particular constituencies represented, as well as specific appointees, have been modified by a series of subsequent Interministerial Ordinance Numbers.<sup>38</sup> For example, a representative of Brazil's telecommunications regulator, Anatel, was later added to the Committee. The current eleven members of the Committee<sup>39</sup> and minutes<sup>40</sup> of their meetings are listed on the Committee's website.

Of particular interest is a Committee-created working group on network security (Grupo de Segurança de Redes (GT-S)). This group previously formed two subgroups: one on *backbones*, focused on Internet backbone security and the other on Internet *access* providers.<sup>41</sup> Shortly after its creation in 1996, the Grupo de Segurança de Redes produced a document recommending that an independent Brazilian national centre for network security coordination be created.<sup>42</sup> This resulted in the establishment of the NIC BR Security Office (NBSO) further discussed in Section 5.5.

The Steering Committee is releasing a series of "best practice" publications with security-related recommendations. The first, released in October 2000, is targeted at Brazilian Internet users.<sup>43</sup> A second, intended for network administrators, is currently under preparation. These recommendations are widely disseminated through large trade associations such as Federação e o Centro das Indústrias do Estado de São Paulo (FIESP)<sup>44</sup> and the Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet (Abranet).<sup>45</sup>

The Steering Committee has also made a series of voluntary security-related recommendations for Brazilian Internet backbone and service providers concerning identification of the origin of Internet connections, codes of ethics, protection of users, configuration of domain name services, identification of users and retention of log records concerning user activities<sup>46</sup> for the needs of law enforcement.<sup>47</sup> To assist in providing precise time-stamped logging activities, the Steering Committee has also supported the provisioning of radio-controlled network time protocol (NTP) servers that provide the official time in Brazil.

### 5.4 Brazilian country code top level domain

The Brazilian country code top level domain (ccTLD), ".br", is operated under the oversight of the Brazilian Internet Steering Committee. The first .br domain was allocated in 1989: today, there are approximately 450,000 active domains managed by the registry<sup>48</sup>, making it one of the largest ccTLD registries in the world. Rules for allocation of .br domain names were first instigated in 1995 and beginning in 1997, fees were assessed for registrations. These fees subsidize other activities (e.g. the NBSO discussed below).

The .br registry and support operations centre is currently (April 2002) being transferred to a larger data centre facility, support for round-the-clock (or "7 x 24") operations, and additional security measures. These include secure access control both to the building and data centre, separate double backup power with generators in the building, uninterruptible power supply, and biometric control cards for access to high-

---

<sup>37</sup> <http://www.cg.org.br/regulamentacao/port147.htm>

<sup>38</sup> <http://www.cg.org.br/sobre-cg/history.htm> .

<sup>39</sup> <http://www.cg.org.br/sobre-cg/membros.htm> .

<sup>40</sup> <http://www.cg.org.br/acoes/realizadas.htm>.

<sup>41</sup> <http://www.cg.org.br/grupo/grupos.htm#Grupo> .

<sup>42</sup> <http://www.cg.org.br/grupo/historico-gts.htm> .

<sup>43</sup> <http://www.cg.org.br/acoes/cartilha.htm> .

<sup>44</sup> <http://www.fiesp.org.br/> .

<sup>45</sup> <http://www.abranet.org.br/> .

<sup>46</sup> The availability of which would only be subject to a court order. Of the providers interviewed, only one could recall an incident where a request for logging records had been made.

<sup>47</sup> <http://www.cg.org.br/acoes/desenvolvimento.htm> .

<sup>48</sup> <http://www.registro.br> .

security areas. The .br registration system core database is backed up offsite with three copies held outside the building. A live backup is also performed offsite to one of their upstream provider's data centre. The registry is multi-homed with two separate upstream providers.

The authoritative name server for .br will shortly be transferred to the new site. Redundant secondary name servers for “.br” are located in France at AFNIC<sup>49</sup> and in California. There is some consideration of deployment of secure DNS (DNSSEC - see Box 5.2) but a final decision has yet to be taken.

### Box 5.2: What is secure DNS (DNSSEC)?

The DNS is the world's largest distributed database using text files containing *resource records*. These resource records provide the set of database values allowing the DNS to operate (such as the association of domain names with Internet protocol addresses). Like any client-server database system, clients send queries and servers return replies. However, generally there is very little security in the Internet Domain Name System (DNS). It is possible for the DNS to be *spoofed* though tampering with DNS packets *en route* between client and server or by using routing tricks to redirect traffic to a name server that imitates a genuine server for the zone. Secure DNS (DNSSEC) could prevent these problems.

DNSSEC uses public key encryption to generate *digital signatures* for every DNS resource record in a zone. The public keys are also signed and included in the zone, allowing the signatures to be validated. A client receiving a signed reply can validate the signature of each DNS resource record in the answer. If the signatures match, all is well. If not, it means that either the records were signed with another private key or else the data was tampered with after the answer left the DNS name server.

In principle, a hierarchy of trust can be set up. The key(s) used to sign a zone can be signed by the key(s) used to sign the parent zone. This process can be repeated all the way to the DNS root zone. For example, a lookup of [www.redegoverno.gov.br](http://www.redegoverno.gov.br) can be proven to have come from a genuine name server for the [redegoverno.gov.br](http://www.redegoverno.gov.br) zone. The answer will have been signed with the [redegoverno.gov.br](http://www.redegoverno.gov.br) key, which could be signed by the “gov.br” zone key. That in turn could be signed by the “br” and *root* zone key.

Nevertheless, considerable challenges still hamper the widespread deployment of DNSSEC. For example, signing a DNS zone and validating signatures can be extremely computational-intensive. Care needs to be taken over the choice of cryptographic algorithms, key lengths, the signing policies and key management as well as sizing and scaling considerations for the zone.

The new secure facilities used for the Brazilian ccTLD registration services will also host the operational centre for a new Latin American and Caribbean IP address Regional Registry (LACNIC)<sup>50</sup>. This new organization will administrate the Latin American and Caribbean Region (LAC) IP address space, Autonomous System Numbers (ASN), reverse resolution and other resources for the Latin American and Caribbean region. The administrative headquarters for LACNIC will be located in Montevideo, Uruguay. The Internet Corporation for Assigned Names and Numbers (ICANN)<sup>51</sup> has provisionally recognized<sup>52</sup> LACNIC. Formal recognition may take place at the next ICANN meeting in Bucharest, Romania, in June 2002.<sup>53</sup>

## 5.5 Brazilian Computer Emergency Response Team (NBSO)

The recommendation of the Brazilian Internet Steering Committee's Group on Network Security resulted in the establishment in June 1997 of the NBSO (NIC BR Security Office); also known as the Brazilian Computer Emergency Response Team. NBSO is funded by Brazil country code top level domain (ccTLD) registration services<sup>54</sup> (“.br”).

---

<sup>49</sup> <http://www.afnic.fr> .

<sup>50</sup> <http://lacnic.org/> .

<sup>51</sup> <http://www.icann.org> .

<sup>52</sup> <http://www.icann.org/minutes/prelim-report-14mar02.htm#LACNICApplicationandTransitionPlan> .

<sup>53</sup> <http://www.cg.org.br/acoec/2002/rea-2002-02.htm> .

<sup>54</sup> <http://www.registro.br> .

NBSO is a service-focused organization responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet. During the past three years, besides performing incident handling activities, they have begun several education awareness programmes to assist Computer Security Incident Response Teams (CSIRTs)<sup>55</sup> in establishing their activities. NBSO's range of services includes:

- **Incident handling:** Providing a focal point for reporting computer security incidents that provides coordinated support in response and dissemination to others of such reports;
- **Collaboration:** Establishing collaborative relationships with other entities such as law enforcement, service providers and telephone companies;
- **Incident tracking:** Support for tracing intruder activities.

NBSO attempts to act as a clearinghouse for information for network incidents in Brazil. It runs workshops on security issues whose participants include major backbone and access providers as well as those from other sectors (e.g. banks). NBSO's impression is that, while there is a growing hacker community in Brazil, for the most part, they are "script kiddies"<sup>56</sup> with little sophistication. The NBSO maintains contacts with law enforcement officials such as a cyber-crime unit recently set up by the Federal police of São Paulo. NBSO is instrumental in providing input into the security-related recommendations released by the Brazilian Internet Steering Committee (Section 5.3)

## 5.6 Academic and research security groups

### 5.6.1 Rede Nacional de Ensino e Pesquisa (RNP)

Realizing it would be better to coordinate separate initiatives and secure integration of regional networks into a national network, the Ministry of Science and Technology created the Rede Nacional de Ensino e Pesquisa (RNP)<sup>57</sup> in 1989. RNP's mission was to operate a backbone network dedicated to teaching and research institutions and government agencies. This network became the basic platform for the early development of Internet technology in Brazil (see Section 3.2.1) and because of this historical role, RNP continues to play an important role in security issues.

---

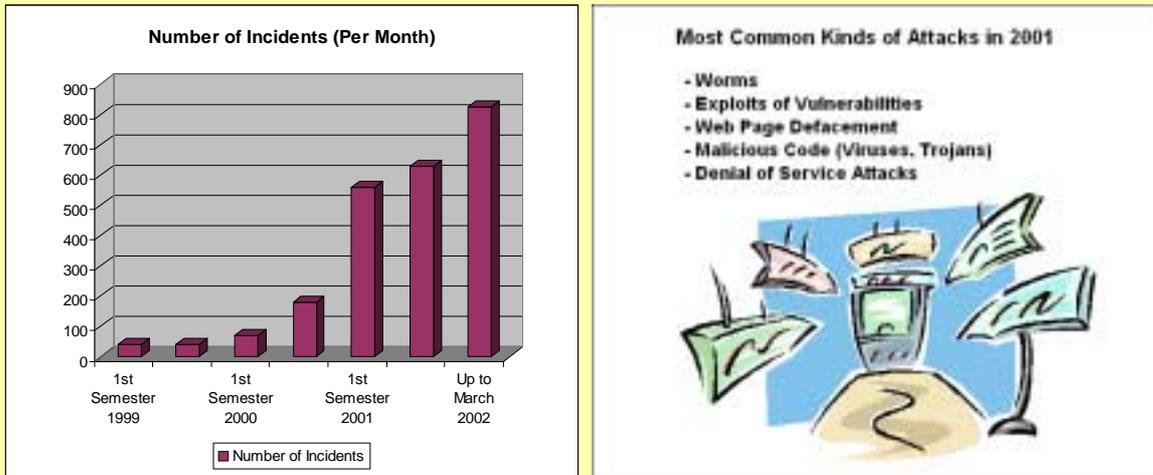
<sup>55</sup> For an overview discussion of CSIRTs, see [http://www.cert.org/csirts/csirt\\_faq.html](http://www.cert.org/csirts/csirt_faq.html).

<sup>56</sup> "Script kiddies" is commonly-used Internet jargon for unsophisticated hackers who typically use scripts or programs written by others that are widely distributed over the Internet and that exploit known software bugs and networking vulnerabilities. Script kiddies often have little or no understanding of how these programs work or what damage they are likely to inflict.

<sup>57</sup> <http://www.rnp.br>.

**Figure 5.1: Network attacks are growing**

*Number of incidents on RNP's network per month and Most common kinds of attacks in 2001*



Source: RNP-CAIS.

In particular, RNP's Security Incident Response Team group (CAIS-RNP) focuses on prevention and has created discussion forums discussing security techniques, organizes regular security training and disseminates security bulletins and information on best practices. RNP is seeing an increased number of network security incidents—mostly recently a rapid increase in denial of service attacks (see Figure 5.1). Like NBSO, the impression of RNP is that this currently represents activities of “script kiddies” rather than an organized hacker community.

RNP is a member of a subgroup of Federal Government's Information Security Committee (Comitê de Segurança da Infomação do governo federal-CGSI).<sup>58</sup>

### 5.6.2 Other academic groups

The Brazilian academic community has a number of other Computer Security Incident Response Teams (CSIRTs) that have cooperative activities with NBSO. These include the Brazilian Academics and Research Institutions Security Incident Response Team (CAIS-RNP)<sup>59</sup> and the CERT-RS (Rede Tche Incident Response Team).<sup>60</sup> Other academic or research related security groups exist at the: INPE (National Institute for Space Research)<sup>61</sup>, Rede-Rio (Academic Network of Rio de Janeiro)<sup>62</sup>, UNESP (São Paulo State University)<sup>63</sup>, UNICAMP (University of Campinas)<sup>64</sup> and USP (University of São Paulo).<sup>65</sup>

### 5.7 SERPRO

One of the goals of the Federal Government's Electronic Government (e-gov) Programme (see Section 4.3) is to implement a common government advanced communications and service infrastructure from which it

<sup>58</sup> <http://www.presidencia.gov.br/gsi/cgsi/> .

<sup>59</sup> <http://www.rnp.br/cais/> .

<sup>60</sup> <http://www.cert-rs.tche.br> .

<sup>61</sup> <http://www.inpe.br/> .

<sup>62</sup> <http://www.rederio.br/> .

<sup>63</sup> <http://www.unesp.br/> .

<sup>64</sup> <http://www.unicamp.br/> .

<sup>65</sup> <http://www.usp.br/> .

will offer a broad range of government services through the Internet, also known as Br@sil.gov<sup>66</sup>. More than 2,000 services are available through the government's Redegoverno portal<sup>67</sup> (see Annex C).

Playing a major role in the government's goal is SERPRO<sup>68</sup>, a private company owned by the Brazilian Government. SERPRO's main mandate is to provide networking services to government agencies: it supports about 6,800 Federal government IT systems. SERPRO runs a large IP-based government intranet as well as IBN SNA network throughout Brazil.

SERPRO has extensive physical and logical security arrangements in place. There are detailed regulations on access to physical facilities with some sensitive areas requiring biometric access. Access to data centres is strictly controlled and all areas are monitored by cameras. Key services are isolated and run in "demilitarized zones" (DMZs) behind firewalls with active security monitoring.

Electronic tax filing is probably the most important application run by SERPRO. 15 million Brazilian citizens sent in their tax filings via the Internet in 2002, representing more than 95% of all filings. Currently, access to the tax system is based on authentication using a citizen's tax number. However, the eventual goal is that every citizen will use his or her own digital ID (see discussion in Section 5.10). Tax returns can be completed online or forms downloaded for offline completion and later upload. SERPRO's security team has to deal with systematic attacks on this particular network yet there has never been a successful break-in.

SERPRO has a security committee of about 35 people who develop government system security policies. The coordinator of the committee is a member of the Federal Government's Information Security Committee (Comitê de Segurança da Infomação (CGSI)<sup>69</sup>, which is structurally under the Brazilian National Defense Council. With the ongoing integration of government systems, SERPRO is preparing a broader Federal security policy to replace individual agency security policies.

Since 1999, SERPRO has a computer incident response team named Grupo de Resposta à Ataques (GRA). GRA has two key responsibilities: vulnerability analysis of government systems and round-the-clock monitoring. Its monitoring activities provide evidence that there are systematic attacks to break into government networks, which originate from both commercial service providers and academic networks. SERPRO cooperates on security issues with NBSO (Section 5.5) and the Brazilian Internet Steering Committee (Section 5.3).

### 5.8 International cooperation initiatives

With the support of the Brazilian Internet Steering Committee, NBSO (Section 5.5) is joining the international Forum of Incident Response and Security Teams (FIRST)<sup>70</sup>. FIRST, which was established in 1990, has over 100 international members and brings together computer security incident response teams from government, commercial, and academic organizations. It fosters cooperation and coordination in incident prevention, to prompt rapid reaction to security incidents and promote information sharing among members. NBSO membership in FIRST was sponsored by the Australian CERT<sup>71</sup>. CAIS-RNP is also a member of FIRST and has partnerships with Argentina and Mozambique for security initiatives. It is also involved in partnerships with Renater<sup>72</sup> in France, who sponsored their FIRST membership.

Brazil government representatives participate in related intergovernmental forums including the International Telecommunication Union (ITU), the World Intellectual Property Organization (WIPO) and the ICANN

---

<sup>66</sup> See Footnote 17.

<sup>67</sup> <http://www.redegoverno.gov.br>.

<sup>68</sup> <http://www.serpro.gov.br/> .

<sup>69</sup> See Footnote 58.

<sup>70</sup> <http://www.first.org>. NBSO is a member of FIRST.

<sup>71</sup> <http://www.auscert.org.au> .

<sup>72</sup> <http://www.renater.fr/>.

Governmental Advisory Committee (GAC). Brazilian federal law enforcement officials also cooperate with Interpol<sup>73</sup> on information technology crimes.

### 5.9 New legislative initiatives

Brazil has a number of pieces of draft legislation related to computer network security and critical infrastructure protection. One of the most relevant is a new bill focused on cyber-crime. This draft legislation generalizes the law already in place vis-à-vis government cyber-crime (Law 9.983) and has stronger provisions. There is no differentiation in the pending legislation between cyber-crime and cyber-terrorism acts.

The first part of the bill defines principles that regulate all service providers and defines what constitutes private and public information. There is a section on crimes, including intentional damage to data or software programs, unauthorized access, modification of passwords or access mechanisms, non-authorized access to data, violation of secret information and introduction of viruses. If the crime is performed in a professional capacity (e.g. corporate espionage), penalties are even stronger. If the crimes are committed against government systems, penalties are even higher with up to six-year prison terms. In the case of cyber-crimes against military facilities, these will be judged by the military justice system.

When drafting the legislation, there were attempts to align the provisions with those in the Council of Europe's Convention on Cybercrime, in order to facilitate Brazil eventually becoming a party to the Convention.<sup>74</sup>

#### **Box 5.2: The Council of Europe's Convention on Cybercrime**

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. The Convention is the product of four years of work by Council of Europe experts, but also by Canada, Japan, the United States and other countries, which are not members of the organization. It is open to signature and accession by non-EU member states.

Source: Council of Europe, Legal Affairs, Treaty Office

Another bill under consideration relates to requirements for Internet providers to do record keeping and logging of Internet protocol (IP) traffic. In this bill, all Internet access providers will need to maintain a registry of users including basic information such as name, national ID numbers, associated company and address. Logs will need to be kept of user IDs, the time the user logged in and out, the IP address used, and the calling telephone number. The data must be retained for three years and is only available for law enforcement purposes. There is no requirement to log specific websites visited. According to the draft bill, the data logged is considered to be private and must be kept confidential by providers subject to financial penalties and/or closure of the provider. If this project becomes law, it will supersede the less stringent voluntary guidelines promulgated by the Brazilian Internet Steering Committee (discussed in Section 5.3).

### 5.10 Policies and legislation related to a public key infrastructure

The Federal Government is also developing policies for the secure authentication and management of information, which includes establishing standards for electronic certification and authentication, including a public key infrastructure (PKI) framework. As in other countries, there is a general view that authentication technologies require the enabling hand of appropriate legislation. One goal is to remove any existing legal obstacles to the recognition of electronic signatures and records. Another objective is to ensure that electronic signatures and records fulfill existing legal requirement for signatures or transactions. Another

---

<sup>73</sup> <http://www.interpol.int>.

<sup>74</sup> The convention is open to non-EU signatories.

objective is to establish a legal framework for the operation of a Brazilian PKI—an area where countries have taken broadly different national approaches.<sup>75</sup>

The Brazilian Government's stance is that, in order to facilitate the adoption and use of asymmetric cryptography as well as to ensure the national public interest, appropriate legislation is required and a great deal of legislative activity is taking place in this domain. The umbrella framework policy on government information security is defined in a Presidential Decree dating from June 2000<sup>76</sup>. More specifically, the interim arrangements for a "Brazilian Public Key Infrastructure – ICP-Brasil"<sup>77</sup>, where the Brazilian Information Technology Institute (ITI) manages the "root", are defined in Provisional Law N° 2.200-2, adopted in August 2001. A Presidential Decree from October 2001 further requires that Federal bodies must use ICP-Brasil for the purposes of digital certificates and in the context of the exchange of encrypted and digitally signed documents.<sup>78</sup> Four grades of certificates are currently issued roughly corresponding to profiles used by the US Department of Defense.

Under intensive development for the past year is draft legislation intended to replace the Provisional Law N° 2.200-2. It will deal with asymmetric cryptography from the point of view of supporting digital authentication and signatures, e-commerce and PKI providers. The bill provides a definition of digital certificates and concepts related to e-government services, the legal status of digital signatures, provisions related to authentication and certificate revocation lists (CRLs), and defines rules for e-commerce and consumer protection. There is also a definition of private data, the obligations of providers vis-à-vis private data, and sanctions for transferring private data to third parties without user consent.

As an example of the practical application of this framework, since January 2002, all official government documents exchanged between the Brazilian President, Ministers, Executive Secretaries and legal advisors<sup>79</sup> are digitally encrypted and signed with 2048-bit RSA keys. The challenging problem of key management is facilitated through use of Gemplus<sup>80</sup> smart cards. Before the end of 2002, there are plans to implement a biometric (fingerprint-based) smart card solution.

A longer term goal is that all Brazilian citizens will be issued digital certificates which will also be used to access personalized government services and a government electronic payment systems (see below and Section 4.3).

### 5.10.1 Implementation of the Brazilian Payment System

The Brazil PKI infrastructure provides integral support to the new Brazilian Payment System (SPB), which was recently deployed in April 2002. This is a closed system among approximately 180 Brazil financial institutions, which will allow banks to automatically deposit funds and have those funds available immediately, as well as to promptly check and approve deposits from other Brazilian banks. Compliance certification is handled by the Brazil Central Bank, which will guarantee the authenticity of other banks through the use of digital certificates.

The Brazil Payment System is an important component of a planned electronic payment scheme for Brazilian citizens, a near-term goal of the Electronic Government Programme (see Section 4.3). This will put in place a government service for the receipt of electronic payments of fees, taxes, contributions, real-estate transfer fees and others, allowing the delivery, through the Internet, of the full cycle of services to citizens.

---

<sup>75</sup> For an extensive discussion of the topic of electronic signatures and certificate authorities and how different countries approach this topic, see <http://www.itu.int/osg/spu/ni/esca/index.html>.

<sup>76</sup> [http://www.presidencia.gov.br/ccivil\\_03/decreto/D3505.htm](http://www.presidencia.gov.br/ccivil_03/decreto/D3505.htm) .

<sup>77</sup> [http://www.presidencia.gov.br/ccivil\\_03/MPV/2200-2.htm](http://www.presidencia.gov.br/ccivil_03/MPV/2200-2.htm).

<sup>78</sup> [http://www.presidencia.gov.br/ccivil\\_03/decreto/2001/D3996.htm](http://www.presidencia.gov.br/ccivil_03/decreto/2001/D3996.htm) .

<sup>79</sup> A closed user group of approximately 160 people.

<sup>80</sup> See <http://www.gemplus.com> .

## 6 Conclusions

As mentioned in the introduction, Brazil has taken its place on the world stage as a considerable global economic force, a regional leader politically, and a coveted destination for investment. Brazil has also put a high priority on improving access to advanced info-communication technologies, promoting digital literacy and improved access to government public services. This is considered pivotal to improving social and economic development for society at large.

The field research for this report revealed the notable clear demonstration of political will, the dedication of many public officials and the numerous efforts within the government to overcome any possible barriers. This is particularly true in the government's many initiatives and support for promoting wide access to telecommunication facilities and info-communication networks such as the Internet. Considerable advances have already been made and Brazil has emerged as a major centre of advanced networking activity.

With the Brazilian Government's drive towards providing its citizens with universal access to Federal online services, it has appropriately realized that it needs to pay closer attention to the topic of information and systems security and cyber-crime, so that its citizens will have the necessary confidence in public and private network infrastructures. While this may include "enabling hand" legislation and regulatory initiatives, it has also involved considerable and sustained cooperative initiatives with the private sector, educational community and civil society.



**Annex A: Brazil basic indicators**

	Units	1997	1998	1999	2000	2001
Population	10 x 3	159,880	165,851	167,987	169,799	171,827
Households	10 x 3	41,100	42,600	42,851	45,021	45,559
Main telephone lines in operation	10 x 3	17,038	19,986	24,985	30,926	37,430
Main telephone lines per 100 inhabitants		10.66	12.05	14.87	18.18	21.69
Cellular mobile telephone subscribers	10 x 3	4,550	7,368	15,032	23,188	28,745
Internet hosts	10 x 3	117	215	446	876	1,644
Estimated Internet users	10 x 3	1,310	2,500	3,500	5,000	8,000 <sup>81</sup>
Internet users per 100 inhabitants		0.82	1.51	2.08	2.94	4.64
Number of Personal Computers	10 x 3	4,200	5,000	6,100	8,500	10,800
Personal computers per 100 inhabitants		2.63	3.01	3.63	5.00	6.26

Source : ITU World Telecommunication Indicators Database

<sup>81</sup> Anatel estimates there were 15-16 million Internet users in 2001. An April 2002 presentation from the Executive Committee of the Electronic Government Secretariat of Logistics & Information Technology Ministry of Planning, Management & Budget gives a figure of 23 million.



## Annex B: Organizations consulted

The author visited Brazil from 11 to 19 April 2002, to carry out interviews. Given below is a list of the organizations and a partial list of individuals interviewed.

### São Paulo

---

Representatives from FAPESP and Brazilian Internet Steering Committee:

- *Frederico Neves, Technical Advisor – Registro.br*
- *Cassio J.M. Vecchiatti, Representative of the Entrepreneur Community*
- *Cristine Hoepers, NIC BR Security Office (NBSO)*
- *Klaus Steding-Jessen, NIC BR Security Office (NBSO)*

Representatives from Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet (ABRANET):

- *Roque Abdo, Conselho Diretor Executivo, Diretor Presidente, Abranet and Picture Internet Providers*
- *Cassio J.M. Vecchiatti, Conselho Consultivo Superior, Diretor Presidente, Abranet*
- *Cyro Ovalle Jr., Director of Operations, AOL Brasil*
- *Milton Kaoru Kashiakura, Internet Group (IG)*
- *Roberta Cezar Bourgogne de Almeida, Abranet Legal Counsel*

Representatives of private sector providers:

- *Valden Flávio Paes, Networking Supervisor, AT&T Latin America*
- *Alexandre Curzi Junior, Operation Support Manager, AT&T Latin America*
- *Hugo Mizukami, Operations Manager, AT&T Latin America*
- *Marcelo Pucci Bessa Lima, Director of Network Planning, Diveo*

### Brasília

---

Agência Nacional de Telecomunicações do Brasil (Anatel):

- *Helio de Lima Leal, Head Office of International Affairs*
- *Marcos Bafutto, Superintendente*
- *Jarbas José Valente, Superintendente*
- *Luis Tito Cerasoli, Conselheiro*
- *José Alexandre Novaes Bicalho, Assessor do Conselho Diretor*
- *Marconi Thomaz de S. Maya, General Manager for Licensing of Services*
- *João Carlos Fagundes Albernaz, Head, Technical Advisory Unit*
- *José Gonçalves Neto, Gerente Geral de Planejamento e Contratação de Obrigações*
- *Moisés Gonçalves, Gerente de Planejamento*
- *Cerminiano Sebastião Arêas de Mello, Operational Manager*
- *Andrea Grippa, Assessora Internacional*

National Academic Research Network (RNP):

- *Nelson Simões da Silva, Director General*

Ministério do Planejamento, Orçamento e Gestão, Secretariat de Logística e Tecnologia da Informação:

- *Elisabeth Braga, Diretora*
- *Oswaldo Noman, Diretor*
- *Alexandre Santana, Diretor*
- *Claudio Miccieli, Diretor*
- *Renata Vilhena, Secretária-Adjunta*
- *Marcos Ozorio de Almeida, Assesor*

Ministry of Science and Technology

- *Vanda Scartezini, National Secretary, Secretariat for Information Technology Policy*
- *Antenor C.V. Corrêa, Software and Services General Manager*
- *Miguel Teixeira de Carvalho*
- *Jeferson Nacif*

Brazilian Congress:

- *Deputy Narcio Rodrigues, President of Science and Technology, Communication and IT Committee*
- *Deputy Julio Semeghini*
- *Deputy Jorge Bittar*
- *Luiz Antonio Eira, Telecom Advisor*

SERPRO:

- *Raimundo Nonato da Costa, Assessor da Diretoria*

Presidential Office:

- *Murilo Marques Barboza, Diretor de Telecomunicações*
- *Otávio Carlos Cunha da Silva, Diretor-Presidente*

International Telecommunication Union (ITU)/Telecommunication Development Bureau/Americas Regional Office:

- *Juan Zavattiero, Head*
- *Vera V. Zanetti*
- *Ana Jamily Veneroso*
- *Luciana Tavares*

## **Rio de Janeiro**

---

Embratel:

- *Mário Ferreira Cabral Jr., General Manager Regulatory Affairs*
- *José Fausto Magalhães Alves, Business Support Manager*

Telemar:

- *José Marcos Rafael Magalhães, Diretoria de Gerenciamento de Rede*
- *Fabio Luiz de Oliveira Guimarães, Security Team IP Backbone*

- *Ricardo Dastis, Infosec Team*
- *Gilberto Elias da Silva, Telemar IP Network Manager*
- *Marco Antônio Continho, Supervisor, Network Engineering Team*

MCT Information Society Program:

- *Tadao Takahashi, Coordinator of the Information Society Program of the MCT*



Annex C: The Federal Government Redegoverno portal

