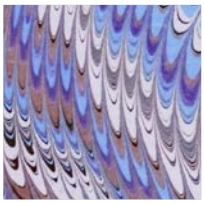
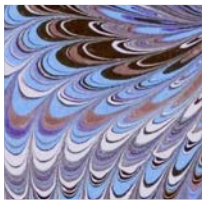
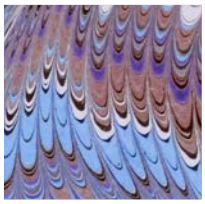
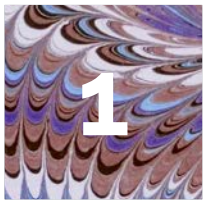
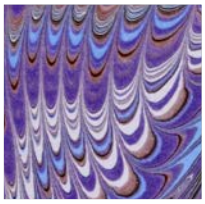


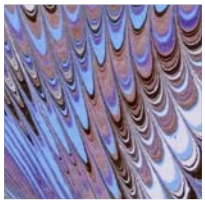


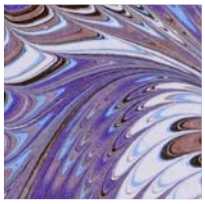


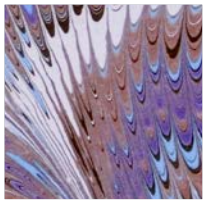


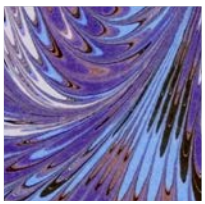
CGI.br BOOK SERIES Studies

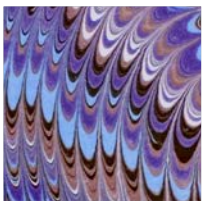












Fighting Internet spam in Brazil

Historical overview and reflections on combating spam and managing port 25, coordinated by the Brazilian Internet Steering Committee

Edited by

Cristine Hoepers
Henrique Faulhaber
Klaus Steding-Jessen

cgi.br

Brazilian Network Information Center (NIC.br)

Edited by
Cristine Hoepers
Henrique Faulhaber
Klaus Steding-Jessen

Report and interviews performed by
Carlos Affonso Pereira de Souza
Marilia de Aguiar Monteiro

CGI.BR BOOK SERIES Studies

Fighting Internet spam in Brazil

Historical overview and reflections on combating spam and managing port 25, coordinated by the Brazilian Internet Steering Committee

Brazilian Internet Steering Committee (CGI.br)
2017

Brazilian Network Information Center (NIC.br)

Chief Executive Officer
Demi Getschko
Chief Advisory Officer
Hartmut Richard Glaser
Chief Financial Officer
Ricardo Narchi
Chief Technology Officer
Frederico Neves
Director of Special Projects and Development
Milton Kaoru Kashiwakura

Advisory Team to the CGI.br Activities
Administrative Advisors
Paula Liebert, Salete Matias
Technical Advisors
Carlos Francisco Cecconi, Diego Rafael Canabarro, Jamila Venturini, Jean Carlos Ferreira dos Santos, Juliano Cappi, Marcelo Oliveira, Nathalia Sautchuk Patrício, Vinicius Wagner Oliveira Santos

Concept & Production
Coordinators
Cristine Hoepers
Henrique Faulhaber
Klaus Steding-Jessen
Report and interviews
Carlos Affonso Pereira de Souza
Marília de Aguiar Monteiro
Executive and Editorial Coordination
Carlos Francisco Cecconi and Juliano Cappi
Editorial Production
Caroline D'Avo and Everton Rodrigues (Comunicação NIC.br)
Editorial support for this edition
Jamila Venturini
Jean Carlos Ferreira dos Santos
Juliana Nolasco
Translation to English
Linnguagem Idiomas
English revision
Juliana Nolasco
Desktop publishing and illustrations
Papel Moderníssimo e Pilar Velloso
Pictures
Omar Paixão, Gettyimages e Istockphoto

This publication is available in digital format at the URL <http://www.cgi.br>

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Fighting Internet spam in Brazil - Historical overview and reflections on combating spam and managing port 25, coordinated by the Brazilian Internet Steering Committee / Núcleo de Informação e Coordenação do Ponto BR; [tradução Linguagem Idiomas]. -- São Paulo : Comitê Gestor da Internet no Brasil, 2017. -- (Cadernos CGI.br estudos)

Título original: Combate ao spam na Internet no Brasil : histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil
Vários colaboradores.
Bibliografia.
ISBN: 978-85-5559-036-8

1. Internet – Medidas de segurança 2. Políticas públicas – Brasil 3. Redes de computadores – Medidas de segurança 4. Spam (Mensagem eletrônica) – Combate I. Núcleo de Informação e Coordenação do Ponto BR. II. Série.

17-00738 CDD-005.8

Índices para catálogo sistemático:
1. Segurança de redes de computadores : Combate ao spam : políticas de Internet : Brasil
005.8

Brazilian Internet Steering Committee (CGI.br)

Composition as per december 2016

Committee members

Representatives from the Federal Government

Carlos Roberto Fortner
Francilene Procópio Garcia
Franselmo Araújo Costa
Igor Vilas Boas de Freitas
Luiz Carlos de Azevedo
Luiz Fernando Martins Castro
Marcelo Daniel Pagotti
Marcos Vinícius de Souza
Maximiliano Salvadori Martinhão

Representatives from the corporate sector

Eduardo Fumes Parajo
Eduardo Levy Cardoso Moreira
Henrique Faulhaber
Nivaldo Cleto

Representatives from the third sector

Carlos Alberto Afonso
Flávia Lefèvre Guimarães
Percival Henriques de Souza Neto
Thiago Tavares Nunes de Oliveira

Representatives from the scientific and technological community

Flávio Rech Wagner
Lisandro Zambenedetti Granville
Marcos Dantas Loureiro

Internet Expert

Demi Getschko

Coordinator
Maximiliano Salvadori Martinhão

Executive Secretary
Hartmut Richard Glaser

Preface

by HENRIQUE FAULHABER

> "Initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, private sector, civil society, academia and technical community"
>
> *NETmundial Multistakeholder Statement, São Paulo – 2014*

Dear reader,

This publication aims at reporting the efforts of the Brazilian Internet Steering Committee (CGI.br) and several people and organizations on fighting spam in Brazil since 2004. The unsolicited mass messages that reach our e-mail boxes represent a challenge faced by users, companies and by the entire access infrastructure and Internet services value chain.

The Anti-Spam Working Commission (CT-Spam), created within the scope of the Brazilian Internet Steering Committee (CGI.br) in 2004, aimed at the creation of a national strategy to address the problem of spam. Because spam is a major vehicle for malicious code distribution and a serious threat to the security of the Internet, CERT.br was a key player in the success of CT-Spam.

The importance of this publication is not just because it is a documentary approach to the activities carried out over the last 10 years in the combat of a particular problem. This report is valuable not only for purposes related to the combat of SPAM; by unveiling the process behind CT-SPAM, it also uncovers one of the main tasks of CGI.br: the multistakeholder coordination of actors in the development of a national Internet policy.

Many challenges still lie in the way of effective collaboration in the field. Education and engagement of decentralized groups, including governmental actors still go through obstacles.

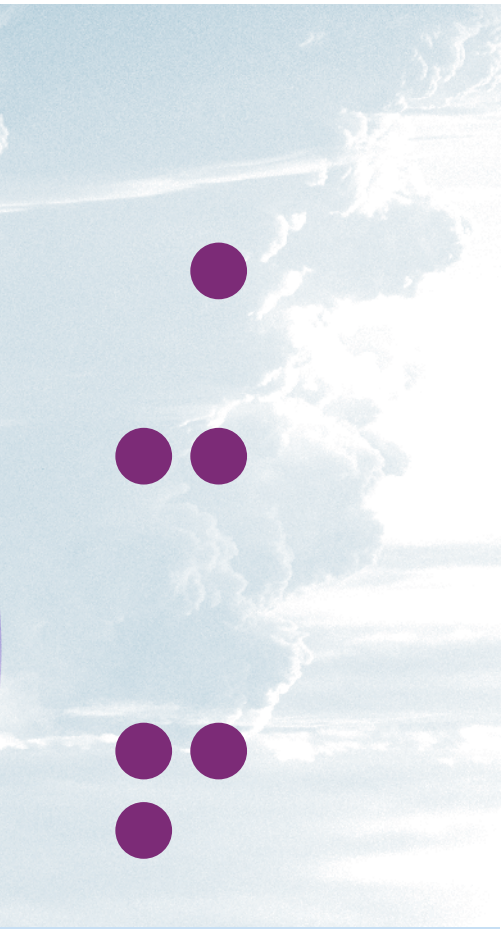
Among them, the difficulty of understanding the complexity of collaboration through various skills and of leaving behind en-

trenched management frameworks in favor of a multistakeholder mode of engagement that can be more innovative and inclusive.

This work went far beyond removing Brazil from the top positions of global lists of spammers. It is the result of a combination of security, freedom and network governance dynamics and collaborative dialogue between different decision makers.

Henrique Faulhaber
Board Member at CGI.br

Contents



I

Report

The brazilian experience of port 25 management

Introduction

Issues related to communication networks security have assumed critical importance on a national and international scale, while communication and information technologies have become essential elements for the attainment of rights such as freedom of expression and the expansion of access, either in terms of public policies or as intrinsic processes to various productive chains.

Given that networks significantly affect the Internet, and the daily affairs of citizens, businesses, and government, different actors legitimately focus their efforts on ensuring network safety and confidence. None the less, such issues exhibit different levels of political, technical, regulatory, economic, and social complexity. Part of this complexity derives from the very nature of the Internet: regulatory choices, business, decisions and even legal actions on net safety should always take into account the global nature of the network, as well as considerations abo ut its interoperability and the participation of different actors.

The majority of threats to network security has a systemic complexity, involving different actors at the same time. Therefore, cooperation between such different actors stands as the best effort for detecting and mitigating the effects of these threats.

Such complexity is not different from threats posed by spam, which, by in turn, also have peculiarities that do communicate, from time to time, with the development of network security practices.

Fighting spam has been currently discussed in forums on Internet governance and regulation for the past 15 years. Factors leading to such a persistent theme are as varied as the ways to investigate the problem, once efforts to discourage spamming can be implemented through perspectives of technological, legal, political and social natures. The aim of this paper is to present the coordinating work performed by the Brazilian Internet Steering Committee (CGI.br) in a project known as "Port 25 Management" as a successful case study in which initiatives pointing to multistakeholder collaboration are referred to as the best strategy for facing cyber security themes.

Various initiatives on the national and international level, as well as in the international forums, advocate cooperation among different actors as a means for combating outbreaks and mini-

mizing threats. The Netherlands have the Dutch Cyber Security Council, comprising 15 members from the government, scientific community, private sector, and industry. The Council acts by itself or on behest of civil society or the government, and is responsible for implementing the Dutch Domestic Cyber Security Strategy. In 2013, the Dutch Council published a best-practices recommendation for a new cyber security strategy that praised the importance of collaboration and coordination among actors for the achievement of an efficient level of protection, information exchange and response to security threats:

> The advice specifically focused on the need for close cooperation and coordination in the field of incident detection and response. Only through active information sharing, timely response and seamless collaboration can a secure digital environment be established[1].

In Japan, the Japanese Cyber Clean Center (CCC) counts on the cooperation amongst government, the software industry and Internet service providers in order to prevent infection of personal computers by means of a structure organized by a steering committee and dedicated study groups[2].

On an international level, the Conficker Working Group (CWG) was created as a coalition of net security researchers to combat a malicious software known as "conficker", which affected users throughout the globe. This working group is acknowledged as a globally unprecedented cooperation among organizations and individuals from private and public sectors for combating a threat to the security of global critical resources:

> In an unprecedented act of coordination and collaboration, the cyber security community, including Microsoft, ICANN, domain registry operators, antivirus vendors, and academic researchers organized to block the infected computers from reaching the domains – an informal group that was eventually

---

1 E. Van Den Heuvel, G.K. Baltink. "Coordination and Cooperation in Cyber Network Defense: the Dutch Efforts to Prevent and Respond," p. 122, available at <https://www.ncsc.nl/english/current-topics/news/best-practices-in-computer-network-defense.html>, accessed July 4, 2014.

2 Cyber Clean Center, available at <https://www.ccc.go.jp/en_ccc>, accessed July 4, 2014. Translator's Note: the link was replaced by <https://www.telecom-isac.jp/ccc/en_index.html>, accessed March 8th, 2017.

dubbed the Conficker Working Group (CWG). They sought to register and otherwise block domains before the Conficker author, preventing the author from updating the botnet. Despite a few errors, that effort was very successful[3].

In a similar manner, DNS-Changer Working Group (DCWG) was created as an ad hoc group to remedy the effects of malicious Rove Digital DNS servers. The botnet operated by this company altered the parameters of the user's DNS by connecting them to malicious DNS servers in other countries, thus inducing users into a dangerous confidence game on the net that invited them to take part in a special survey. This group involved the coordination of the following institutions: Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhouse, Team Cymru, Trend Micro, and the University of Alabama at Birmingham. All these teams collaborated with the United States FBI, National Computer Emergency Response Teams (CERTs) and connection providers.

Accordingly, the work performed by CERT.br and by CGI.br, through the action of its Anti-spam Working Group, is acknowledged as one of the successful global initiatives of collaboration and multistakeholder coordination for the promotion of cyber security issues. Over a period of 20 years, Brazil has been developing a multistakeholder model for Internet governance guided by the work of CGI.br Internet. As one of the groups maintained by the Brazilian Network Information Center (NIC.br), a non-profit entity in charge of implementing CGI.br decisions and projects, CERT.br holds coordination as one of the essential elements of its security work and of its response to incidents on the Internet in Brazil, along with communication with and support for the Brazilian community regarding trends and threats.

Studying and documenting the Port 25 Management initiative on the Brazilian net aims, firstly, to demonstrate, based upon a well-established case, the development of the country's Internet policies in the last 25 years.

Furthermore, this paper points to the importance of collabora-

3 "Conficker Working Group: Lessons Learned," available at <http://www.confickerworkinggroup.org/wiki/uploads Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf>, accessed July 4, 2014.

tion and coordination among stakeholders as a pressing element for implementing security policies and establishing confidence on the Internet. By converging experience of dozens of telecommunication companies, thousands of ISPs, and representatives of civil society and academic communities, as well as that of CGI.br technicians, port 25 management process was an ample exchange of knowledge. The wide-ranging discussion promoted by CGI.br was especially important to make the process effective, in that it demanded, first of all, that e-mail providers transmit e-mail messages through a different port, migrating at least 90% of the users of different companies before the ISPs could block outgoing traffic from port 25. Because collaboration and coordination amongst actors constitute the main axis of this study, their testimonials provide us with a primary source of narratives about this initiative. Beyond any theoretical pragmatism regarding the multistakeholder aspect of the Internet policies, this study focuses both on the experience and collaboration of these actors in the specific process of managing port 25.

Coordinating port 25 management team was a task assumed by the Brazilian Internet Steering Committee (CGI.br), a multistakeholder organism created in 1995[4] as the result of an inter-ministerial initiative to discuss topics related to Internet policy in the country. In 2004, a special working group was created within the CGI.br to work specifically on spam. The group was an initiative of a steering committee member, Henrique Faulhaber, and was known as the Anti-Spam Task Force (CT-Spam). Therefore, the first part of this paper brings a brief account of the activities performed by this working group within CGI.br. CT-Spam activities reflect the distinctive number of solutions that a network security problem might involve: legal and regulatory requirements, business activities, and user education.

The second part deals with the management of port 25 itself, while the third exhibits the legal and regulatory issues that emerged during the process. The fourth and final part examines the coordination activity based on the history of Brazilian telecommunication and Internet services regulation. At this point, the reader will be provided

4 CGI.br history can be seen in <http://cgi.br/historicos/#1995>, accessed June 02, 2014.

with a brief presentation on Brazilian telecommunication regulatory model, as well as with the multistakeholder Internet governance model developed by Brazil over the past 25 years.

This paper will briefly narrate Brazil's regulatory choices since the process of privatization of its economy, which began in the 1990s, and was reflected in the development of Internet governance in the country's Internet. Therefore, this paper proves that effective solutions for Internet policies derive from the collaboration of different actors: telecom and Internet applications providers, technical organisms, academic and governmental groups, civil society entities, and consumer advocates. This report does not intend to deal with theoretical focus on the increasing global debates regarding multistakeholder solutions. However, it is intended to exhibit the perspectives of actors who have engaged in a successful decentralized, multi-participatory and voluntary process.

Brazil, "The King of Spam"

In 2009, Brazil topped the Composite Blocking List ranking of nations from which most spam originated, and was dubbed "The King of Spam" by international media. The list, updated on a daily basis, currently ranks Brazil in 25th position[5]. Brazil's success is the fruit of eight years of anti-spam policy implementation by the Brazilian Internet Steering Committee (CGI.br) and its Anti-Spam Task Force, CT-Spam[6]. CT-Spam was founded as much to design a national strategy against the abuse of the network by spammers as it was to articulate measures for fighting spam with the various stakeholders involved.

The major motivating agent for CT-Spam was the reputation of the Brazilian network. There had been extreme cases in which entire blocks of Brazilian IPs were blocked for incoming traffic in other

5 Composite Blocking List,available at <http://cbl.abuseat.org/country.html>, accessed October 12, 2013.

6 CGI.br, "Comissões de Trabalho - Antispam" (Anti-Spam Task Force) Available at <http://www.cgi.br/pagina/comissoes-de trabalho-antispam/121#a4>, accessed May 5, 2014. The first meeting of CT-Spam was held on January 14, 2005 to define the group's agenda and begin work.

countries exclusively because of their nationality[7].

The abuse of the Internet structure by spammers and the need of a solution were observed, once the risks of inaction would be directly experienced by the consumer, including: (i) a substandard performance of the bandwidth purchased by the consumer; (ii) consumers placement on blacklists, rendering impossible the full enjoyment of his freedom on the Internet and, in extreme cases, leading to limits on his freedom of expression; (iii) technical support costs unnecessarily dumped on the affected consumer; and (iv) a substandard performance of global communication services, in that the spam message is international in scope[8].

CT-Spam has worked as much to promote awareness amongst sectors involved as a role they had to play in the implementation of these policies, as well as to promote education for building awareness amongst consumers about the safe and efficient use of Internet services. These tasks, among others, make the work of CT-Spam a crucial and important leading case of the CGI.br multistakeholder model that has achieved ample international success and become a guiding theme in the history of the Internet in Brazil.

"Port 25 Management" became the most effective technology and policy for such purposes. Port 25 management was "the name given to an assortment of policies and technologies implanted in final user networks and domestic subscriber networks which sought to separate (1) the functionalities of message submission from (2) the functionality of message transportation between servers."[9]

The extensive time it took to execute Port 25 management shows that it was no trivial matter, whether for technical reasons – not even the corporate technicians were aware of the consequences or impact

7 This perspective was pointed to mainly by Rubens Kuhl, Eduardo Parajo, Klaus Jessen and CristineHoepers in various interviews conceded to the Project Memories of Combating Spam in Brazil.

8 MAAWG, "MAAWG Recommendation": Managing Port 25 for Residential or Dynamical IP Space Benefits of Adoption and Risks of Inaction, available at <http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf>, accessed October 12, 2013.

9 C. Hoepers, K. Steding-Jessen. Gerência de Porta 25: Motivação, Importância da Adoção para o Combate ao Spam eDiscussões no Brasil e no Mundo (Port 25 Management: Motivation, Importance of Adoption for Spam Combat, and Discussions in Brazil and in the World), 2009, available at <http://www.cert.br/docs/ct-spam/ct-spam-gerencia-porta-25.pdf>, accessed October 12, 2013.

of the measure – or for regulatory and legal reasons. A number of often conflicting interests had to be coordinated in the name of a successful result for the common good. In this manner, issues such as user protection and contractual guarantees emerged as arguments that complicated, and therefore delayed, the process.

The implementation of such measure was also impacted, though indirectly, by discussions over the Marco Civil da Internet do Brasil (Brazilian Civil Rights Framework for the Internet, termed the "MCI"), recently enacted as Law 12,965/2014. This law was the result of a consultation carried out by the Ministry of Justice, by means of a special web portal, between 2009 and 2010 and submitted to the National Congress in its final form in 2011. Among the central themes of the Marco Civil, the principle of net neutrality principle overlaps slightly the method of port 25 management.

Methodology of the present study

CT-Spam coordinator Henrique Faulhaber stated, in a preliminary interview for this paper, that beyond the technical importance of the port 25 management project, which was acknowledged by national and international experts, the implementation of such management in Brazil was due to the individual role of each of the actors involved. Had such actors not been united in a common will, perhaps port 25 management might not have been so efficiently adopted[10].

The main source of this paper was the testimony of these actors, once it enabled us to document the process by providing an understanding of the different ways actors and groups interacted, and by revealing the impact of individual actions and their working strategies. In addition, this methodology provides insight into how persons or groups elaborate and perform a given experiment, including learning and strategic decision-making situations[11].

This work aims, therefore, to offer a memoir of the combat against spam in Brazil, by means of port 25 management. The perspective is that of a historical documentation that will form a legacy not only

10 Henrique Faulhaber in an interview conceded to the project "Documenting Port 25 Management" on September 17, 2013.

11 V. Alberti. Ouvir contar: textos em História Oral (Hear Tell: Texts on Oral History). Rio de Janeiro: Editora FGV, 2004.

of a paradigmatic case and an international example, but also to contribute to the historical records of Internet development in the country. By doing so, we can preserve details of the process that would otherwise be impossible to derive from documents, such as individual points of view and personal efforts of each actor involved, which should yield intense, rich research material for present and future generations of the Brazilian Internet historians.

Interviews were performed with actors representing the main sectors of the Internet: the government, civil society, the private sector and academia. Reports allowed us to clarify not only efforts to negotiate strategic decision-making, but also legal and regulatory issues faced by individuals in a context that lacked dedicated legislation and that would also touch upon fundamental rights such as privacy, freedom of expression, consumer protection, and competition.

The first part of this work presents a brief history of actions leading to the implementation of port 25 management. Identification of the problem, the first approaches to a solution, and strategic decision-making processes regarding blockage of port 25 are highlighted. Effective political, legal, and regulatory elements are discussed in the second part, derived from the collection of interviews.


CT-Spam
UCE

1. Brief history of CT-Spam war on spam

CT-Spam is the Anti-Spam Task Force of the Brazilian Internet Steering Committee (CGI.br)

As it will be explained in greater detail in the second part of this work, the Brazilian Steering Committee (CGI.br) is an agency that deals with Internet governance in Brazil. One of the major effects of its creation was to ensure a multistakeholder character to the governance and structure of the Internet, that is, to domain names and IP addresses, by separating its attributions from those usually assigned to governmental regulation of the telecommunication sector.

With the evolution of discussions about Internet governance, particularly in the World Summit on the Information Society in 2004, preexisting internal demands advocated that CGI.br should deal with other layers of Internet governance rather than those of a merely structural nature[12].

CGI.br Anti-Spam Task Force (CT-Spam) was created in 2005 as an initiative to deepen CGI.br role beyond network infrastructure management. An initiative of CGI.br board member Henrique Faulhaber, the combat against spam began as a response to the flagrant problems spam represented: In 2005, 90% of e-mail messages were unsolicited, consisting of so-called spam[13]. Besides harassing users, the abuse of the Brazilian network affected not only its international credibility, but also the performance of its telecommunication operators and Internet Service Providers (ISPs), and urgently needed to be addressed. Inexperienced customers' use of their contracted broadband was impaired and, in some cases, financial losses could result from messages with fraudulent content.

12 Henrique Faulhaber in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

13 zApproximate estimate revealed by Henrique Faulhaber in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

Much effort has been employed to define the term "spam" in such a way as to encourage combating it[14].

CERT.br safety tips list advocates the unsolicited nature of a message as the fundamental element for defining spam. According to this list, spam is "a term used to refer to unsolicited e-mails generally sent to a large number of people. When such messages exhibit exclusively commercial content, they are also known as an Unsolicited Commercial EMail (UCE)."[15]

Thus, definitions – normative or not – of this term are based on subjective aspects due to the usefulness or convenience of the message for the consumer. In addition, the presence of such messages can be amplified by means of other forms of electronic messages such as SMS, IM or messages on social networks. Since subjectivity makes it harder to determine common denominators, CT-Spam carried on a study on the regulatory aspects of spam,

---

14 The term "SPAM" itself is an American brand of processed, canned meat, manufactured by Hormel Foods. How it came to be used in a computer silence context is uncertain and the subject of curiosity. Many believe the term was coined primarily by the celebrated comedy team Monty Python in a skit from the 1970s, which takes place in a bar in which all the available dishes are prepared with canned meat: the spam. While some costumers try to decide on what to order a group of Vikings is chanting the phrase "Spam" to exhaustion, causing general embarrassment. In information systems, the controversy is even more acute, but that it applies to the sending of unsolicited messages to addressees on a mass scale, independent of the term. According to information from the antispam.br web site: "The controversy over the official date of birth of the expression is March 5, 1994". On that day, two attorneys, Canter and Siegel, sent a message about a lottery of American "green cards" to a discussion group on Usenet. The act of sending the message was to advertise services that had nothing to do with the subject matter of the group and angered many participants. Despite this, the worst intrusion came on April 12, 1994, when the lawyers sent the same message simultaneously to members of a variety of message boards on Usenet. A program capable of automating the sending of e-mail was used to distribute the advertising on a broad scale. Reactions were immediate and universally negative. The messages were deemed a violation of "Netiquette" – a list of good manners for network users. The large amount of messages that have been exchanged compromised the performance of the network and that has caused the well known side effects of spam. These historic messages can be found at WebArchive.org: <http://web.archive.org/web/20011214024742/math-www.uni-paderborn.de/~axel/BL/CS941211.txt>. During the inflamed discussion of events, someone brought up the term spam, recalling a scene from Monty Python, the British TV Program"".. To learn more, access<http://antispam.br/historia/>.

15 CERT.br, "Cartilha de Segurança para Internet" (A Spam Primer): 5. Spam: <http://cartilha.cert.br/spam/>; accessed March 8, 2014

establishing some basic criteria for its classification,[16] such as:

(i) its commercial character;
(ii) its mass distribution;
(iii) its uniformity of content; and
(iv) the fact that it has not been solicited by the addressee.

Over the years, CT-Spam has devised a number of solutions that have helped reverse Brazil's position as one of the countries in the world where most spam was sent from. From educational awareness campaigns for individual users and companies, to the production of the above mentioned study; from the creation of a website which became a reference on spam to a stimulus encouraging self-regulation, there are numerous CT-Spam activities that could be analyzed.

Since this study focuses on port 25 management, these initiatives will be only briefly touched upon, where pertinent, in order to demonstrate that the implementation of port 25 was not an isolated activity, but rather an additional step in a series of CT-Spam efforts to attack the problem of mass e-mailing originating from Brazil. Likewise, we point out how these activities relate to one another and differ from the challenges faced by the development of port 25 management.

Email Marketing Self-regulatory Code

One of the activities CT-Spam encouraged was the creation of an email marketing self-regulatory code. This initiative emerged from the working group's perception that besides proposing legislation to regulate the subject, it would be necessary to establish standards to guide companies that use e-mails as commercial vehicles for their products and services. As former CGI.br member Jaime Wagner said:

> I always say that there are several kinds of spam. One is a "bandit" spam, that was being fought00via port 25 management; the other is a "naive" spam, dressed up as marketing.

16 CGI.br - D. Doneda, R. Lemos,C.A. Souza, C. Rossini..Estudo sobre a Regulamentação Jurídica do Spam no Brasil (A Study of the Legal Regulation of Spam in Brazil), April 2007. Available at <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>, accessed on October 12, 2013..

> That is the guy who buys a database and sends out messages to everyone, with the best of intentions and hope for better sales. That's the case of several small businesses that see this as cheap marketing. They have a legitimate premise, but end up as spammers[17].

The aim of email marketing self-regulation was indeed to prevent a legitimate commercial activity, sending advertisements to consumers, from getting inappropriately caught up in a general attack on spam, given that such practices, in many respects, exhibit the subjective characteristics of a spam, as it will be discussed below.

On the front lines of the combat against spam, former board member Jaime Wagner was responsible for coordinating the actors involved in the email marketing chain. The differences of coordination amongst actors in an email marketing self-regulation and those demanded by port 25 management depend upon technological advances and detachment from the consumer.

That is to say, email marketing self-regulation is an activity only undertaken by actors who use the Internet as a platform for delivering products or services; i.e., publicity for a given product or service. Besides, customers clearly notice the convenience and usefulness of the product and can, almost automatically, identify the source of the problem – the supplier. Port 25 management coordinating efforts, on one hand, are molded by the management of net resources and those of the various agents responsible for providing Internet services. In this case, consumers may not have a clear perception of the problem, nor realize who is responsible for service failure.

The antispam.br web site

CT-Spam set out to fight spam by acting on various fronts. In order to promote education for final users and for providers and telecom operators, antispam.br web site was created to publicize defense tips and general information about spam for final users, network administrators, and communication operators. As a product of the Anti-spam Working Group, the site is still important to port 25 blockage, in that it represents a legacy of consumer

17 Jaime Wagner in an interview conceded to the project "Memories of Combating Spam in Brazil" on March 11, 2014.

information and education on basic rights according to relevant consumer protection regulations[18].

As Henrique Falhauber stresses:

> "It was the antispam.br site that supported all this awareness in regard to the spam problem. Spam has not gone away; we have left the list of top spam producing nations, but spam is still a problem. And it is still a problem in other media: social networks, SMS. And so this task of educating, raising awareness, and alerting users is of utmost importance, it is a byproduct that is still out there. We have campaigned to make the site known and it has become a reference that ended up as a great help to the implementation of port 25 management."[19]

Therefore, the relationship between the antispam.br site and port 25 management points to the need of coordinating activities of a complex technological nature, such as the management itself is complex, to the development of an informational platform that can offer the public the information needed to ensure the best results for their activities. In this way, the anti-spam web site seems to have worked not only as a tool that stressed the importance of port 25 management, but also as a means of recruiting and educating a diverse group of actors.

The Anti-spam Bill

CT-Spam promoted a comparative study of anti-spam laws from around the world, and analyzed the bills still under discussion in the Brazilian national congress regarding their criminal aspects. At the close of this study, a bill draft was presented. This study, elaborated by Ronaldo Lemos, Danilo Doneda, Carlos Affonso Pereira de Souza and Carolina Rossini, was, in 2007, one of the

18 Federative Republic of Brazil, Consumer Defense Code, Article 6: "The basic rights of consumers are: (...)
II – education and general information about the proper consumption of products and services, ensuring freedom of choice and equality in hiring;
III – clear, adequate information about different products and services, correctly specifying the quantity, characteristics, composition, quality, tax liability and price, as well as eventual risks (...)". Brazil, Law 8,078; Sept. 09, 1990.

19 Henrique Faulhaber in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

first investigations on legal and regulatory challenges to be faced while implementing an effective anti-spam policy in the country[20].

The study proposed the following criteria[21] for a legislative technique for fighting spam:

1. Adoption of the "opt-in" system as a model for the qualification of electronic messages on the Internet – then, spam messaging will not be legitimate as a means of communicating with consumers on the Internet. Before sending advertisements, a previous commercial relation is required, so consumers can opt whether they wish to receive advertisements from that supplier. The establishment of a legitimate moment for such messages also allows technological neutrality in regard to the media through which advertisements can be sent: electronic mail, cell phones, and other forms of electronic communication;

2. Possibility of invoking a collective protection of rights to combat spam based on its diffuse harmful character;

3. Explicit definition of parameters for damage assessment by judges in lawsuits regarding spam. Given the subjective definitions and difficulties in valuing damages after establishing responsibilities, the bill draft sought to include mechanisms to aid judges decide how to consider damage when facing technical situations;

4. Redefining criminal misrepresentation in order to include messages sent over digital or analogue networks aiming to obtain economic advantage or to cause harm.

The work did not intend to criminalize the act of sending advertisement to consumers. Rather, it sought to develop legitimate, compatible criteria regarding consumers' rights and economic development. This project subsidized former CGI.br board member Jaime Wagner in a 2009 project to develop an advertisement mailing code of conduct, as mentioned above. Consequently, email marketing self-regulation legitimates this form of communication with consumers, creating limits concerning customers' privacy and convenience.

---

20 D. Doneda, R. Lemos, C. Rossini, C.A Souza..Estudos sobre a Regulamentação Jurídica do Spam no Brasil (A Study of the Legal Regulation of Spam in Brazil), April 2007. Available at <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>, accessed on October 12, 2013.

21 Ibidem, p. 62.

Direct publicity suppliers were unbending and critical regarding the regulation that was being drafted by CT-Spam. That being said,, suppliers and providers were invited into the debate in order to make a consensus possible through a proposal from their sector that would not impair their businesses and also comply with standards for consumers' rights.

> Then we created a way to deal with the problem that didn't depend on legislation, but rather on a consensus among the actors involved in this activity. Instead of seeking to define what spam is, as legislators were doing, we chose to define what would legitimate email marketing be and everything that was out would be affected by the law that would eventually pass. Just because trying to define spam is very complicated."[22]

It is important to recognize how port 25 management relates to the activities so far mentioned, since it represents a coordination effort that is closely involved in a sequence of activities in other areas, either related to legal and legislative techniques or to the coordination of different sectors. This is not the moment to elicit any debate on the eventual preponderance of legal over technological criteria or vice-versa; however, to appreciate the mosaic of the activities carried out by CT-Spam, it is relevant to notice how evident is the multidisciplinary character of measures from both legal and technological points of view.

Even though Port 25 management may seem a more technological matter, issues of a legal nature notably imposed themselves for consideration as relevant elements in its implementation. Contractual aspects and consumers' defense are but a few of such issues. On the other hand, the understanding of CT-Spam and its previous work on activities of a legal nature to combat spam helps to illustrate its multidisciplinary character.

Honeypots and Spampots

Since 2003, CERT.br (Brazilian National Computer Emergency Response Team), maintained by CGI.br, has been running a project known as Distributed Honeypots, whose task is to furnish metrics

22 Jaime Wagner in an interview conceded to the project "Memories of Combating Spam in Brazil" on March 11,2013.

and information about abuse in networks based on inputs from 50 machines spread all across the Brazilian network. Using machines that simulate certain operating systems and computer services, the system can identify how these machines could be abused, i.e. by detecting attempts to disclose passwords[23].

Based on the use of this technique to develop metrics on net abuses, the SpamPots program – a kind of honeypot specifically dedicated to analyze abuses by spammers – was created in 2006[24]. Ten honeypots were installed. That is: ten computers were configured to simulate those of real residential computers, vulnerable to abuses.

Volunteers to measure bandwidth

For the perspective of a center dedicated to security incidents, the spam problem was an issue of great interest. More than merely exhibiting unsolicited content, spam is, above all, an abuse of the Brazilian Internet structure.

With the help of ten volunteers, five of whom were CGI.br board members, and all using one of the five main Brazilian Internet providers, sensors were installed in their homes. In addition to capturing spam, the sensors also detected broadband stability and low quality. Spammers consumed so much bandwidth by their uploading that even CERT.br servers were unable to collect data[25].

Spammers scan the entire network searching for open ports and proxies from which they run various tests to determine whether such computer is fit to carry out certain actions as forwarding network traffic. In such case, the honeypots would issue a positive response to spammers in order to make them believe their action was deemed valid, and then they would start sending spam to these honeypots.

Over the course of 466 days, 524,585,779 e-mails were collected, originated from 165 different countries and destined for more than four billion users. Brazil was not even among the two main final addresses of such e-mails: Taiwan and China. A study by the

23 CERT.br. "Distributed Honeypots Project", available at <http://honeytarg.cert.br/honeypots/index-po.html>, accessed October 12, 2013

24 CERT.br. "SpamPot Project", available at <http://honeytarg.cert.br/spampots/>, accessed October 12, 2013.

25 Cristine Hoepers and Klaus Steding-Jessen in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013.

University of Minas Gerais (UFMG), commissioned by CT-Spam, showed that 90% of the spam collected as having been originated in Brazil had Chinese content[26].

It was then concluded that spammers and spam were not Brazilian; machines of Brazilian users were being systematically abused by international spammers, which was impairing the user's enjoyment of services and their connection experience[27].

The development of metrics devised by members of CERT.br, mainly by Klaus Steding-Jessen and Cristine Hoepers, with the support of former CGI.br board member Marcelo Fernandes, was crucial to convincing actors who often mistakenly regarded numbers and data on spam as a result of manipulation by the software industry and its antivirus and anti-spam software sect.

Based on the above-mentioned experiences, a decision was made to move forward with the Port 25 Management program, considered the most efficient way of altering the situation in which the country could be found in spam blacklists. The topic below describes how this activity took place.

---

26 Cristine Hoepers and Klaus Steding-Jessen in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013

27 NIC.br. Taiwan e China lideram ataques de spams aoBrasil (Taiwan and China are leading spam attacks on Brazil), available at <http://nic.br/noticia/na-midia/taiwan-e-china-lideram-ataques-de-spams-ao-brasil/>, accessed October 12, 2013. According to the press release publicizing the SpamPots initiative, released to the public on July 11, 2007: "The list of the ten countries that most abuse Brazil, according to preliminary results, is topped by Taiwan, from which 281,601,310 e-mails were captured, or 76% of all occurrences. China came in second with 58,912.303 e-mails, representing 16% of the volume collected. The U.S., Canada, Korea, Japan, Hong Kong, Germany, Brazil and Panama are the others who appear on the list, and together account for less than 8% of the activity."

2. Port 25 management

Port 25 is the standard TCP/IP protocol port used for sending e-mails among servers that use SMTP – Simple Mail Transfer Protocol. Port 25 is implemented by a logical connection for data transmission. A physical port that transmits data, for example, is the slot of a user application that is connected to a network cable. As Rubens Kuhl explains:

> "Port 25 is used for communication amongst mail servers on the Internet. When users submit e-mails over the Internet, they don't need to use port 25. Only after the message is submitted to the server is that the server uses port 25 to deliver it to the server of the addressee."[28]

Port 25, as such an "open road,"[29] was subject to to all sorts of abuse. In this context, "abuse" consisted in the use of machines belonging to Brazilian users, without their awareness, to send unsolicited, anonymous e-mails from foreign senders, and in massive amounts, to users the world over.

In Brazil, the Principles of Internet Governance and Use[30] state that the network must be free, open and immune. That said, limiting the use of open functionalities must not only be justified in technical terms, but also by the objective identification of an abuse that limits the use of the network, its adequate functioning and its users' free enjoyment. As Demi Getschko explains:

> "We didn't know whether there was abuse or not, so we did some research on what was happening with Brazilian spam. (...) The e-mail hit the machine and was forwarded to many, depending on the list of addressees in that e-mail box, and was sent back there. We saw that the e-mail was

28 Rubens Kuhlin an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

29 Demi Getschko in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013.

30 CGI.br. Resolution CGI.br/RES/2009/003/P: Princípios para a Governança e Uso da Internet no Brasil, (Principles for the Governance and Use of the Internet in Brazil) available at <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>, accessed on October 12, 2013.

not national – it had no national origin, no national destiny; we were functioning as a mere reflector, and so the simplest procedure would be to change that port for another with password protection."[31]

The SpamPots program proved the existence of abuses, while CERT.br identified the best technologies and policies to deal with them. It was up to CT-Spam to try to reverse this situation with its Port 25 Management program. This initiative marked the committee work and represented an important leading case for the Internet in Brazil in terms of multistakeholder coordination.

As CERT.br technical director Klaus Steding Jessen, one of the engineers responsible for the implementation of the SpamPots said:

> "(...) something that became crystal clear was that, while various proxy ports were being abused, the objective of the attack was always the same: to get to port 25; this was what the spammer wanted. He would break in using malware or leveraging the misconfiguration of the user's e-mail address; he would try everything, but they all had the same destination: port 25. There he would find an e-mail server from which he could spam. And this was sort of a bombastic result for us to show: managing port 25 would be devastating for this hack.
>
> In the beginning, some operators said it was better to block incoming connections destined to the proxy, and we discouraged them by saying, "Look, I had 30 today!" And sometimes, the malware can be installed in any machine, but its destination has to be port 25 so it can interact with an e-mail server on this port, which is the SMTP standard."

(See Klaus Steding-Jessen Interview[32])

Blockage of port 25 by residential users already was recommended by IETF (Internet Engineering Task Force) – an international organization responsible for formulating standards for various functioning aspects of the net through RFCs (Request for Comments). Though voluntary, these RFCs are acknowl-

---

31 Demi Getschko in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013.

32 Klaus Stending - Jessen in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013.

edged by the whole international community as standards for network functioning, once they are formulated by consensus among participating agents.

The RFC regarding the submission of e-mail messages[33] recommended a division between tasks of submitting and transferring e-mails as the best technique for network effective management, and identified its main benefits: (i) a decrease in massive unsolicited e-mail traffic; and (ii) the inclusion of security and privacy aspects as requirements for certification:

> Implement security policies and guard against unauthorized mail relaying or injection of unsolicited bulk mail.
> Implement authenticated submission, including off-site submission by authorized users such as travelers.
> Separate the relevant software code differences, thereby making each code base more straightforward and allowing for different programs for relay and submission.
> Detect configuration problems with a site's mail clients.
> Provide a basis for adding enhanced submission services.

Simply put, it may be said that all e-mail services serve two main functions: (i) submission, which involves the sending of a message by the e-mail client to the e-mail server; and (ii) transport, that is, the actions of an e-mail server communicating with another in order to deliver the message sent. Port 25 Management, therefore, represents a clear distinction between the two functions.

Once Port 25 Management was implemented, and based on the ability to distinguish between the two basic functions of an e-mail, the resident user could only send e-mails indirectly through an e-mail server and not directly to other users, since the transport activity must now be handled by dedicated e-mail servers.

Thus, submissions to port 25 are blocked for residential users and are performed by an exclusive, dedicated port, 587/TCP, which requires authentication, leaving all transport typical of port 25 open only to authorized entities. Port 25 management offers a control on and elicits a responsibility from residential network users which is not manifest through legal codes, but rather by the architecture of the network.

---

33 IETF, RFC 6409, November 2011. Available at <http://tools.ietf.org/html/rfc6409>, accessed March 14, 2014.

In charge of the technical aspect of network management, CT-Spam moved closer to technically qualified people in order to effectively block port 25 and migrate users to port 587: telecommunication operators that provide Internet connection services and major e-mail providers. As Cristine Hoepers and Klaus Steding-Jessen explain:

> "It was a technical measure, but in general not complex at all. Today they (multimedia communication services operators) implement various filters in their structures; we have attended several meetings.
>
> As we see it, maybe in general, there are several good networking practices that they adopt and we guessed it was the same implementation of a good practice: to stop home users machines from getting infected and sending spam. We believed that half a dozen meetings with a more technically aligned group – who would see that as a waste of networking, a bandwidth waste: what was bad for them – would make them join the initiative, would make them turn the key. But the opposite happened, even when we talked to people from a technical background."[34]

Coordination of technical stakeholders alone did not yield the results CT-Spam hoped for. A certain reluctance was noticed mainly amongst actors regulated by telecommunication rules, such as multimedia communication services providers,[35] even though it was an internationally accepted technical implementation, with its own dedicated RFC on file with the IETF. This led some CGI.br actors who were responsible for the coordination to suggest the recruitment of media executives instead of technicians to negotiate port 25 management.

In 2009, as a result either of the unsuccessful initial discus-

---

34 Cristine Hoepers and Klaus Steding-Jessen in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013.

35 "Multimedia Communication Service" is the term used by ANATEL, the national telecommunication agency, to designate the provision of service which "promises capacity needed to transmit, emit and receive multimedia information, including the provision of an Internet connection," according to Article 3 of ANATEL Resolution 614/2013. The relationship between multimedia content, which is a telecommunication service, and Internet connectivity, which is a value-added service, will be explained in more detail in Chapter 4.

sions and technical recommendations, Brazil was given the title "The King of Spam" by the international press, since at the time it topped the list in various global blacklists of spam sources[36]. Though the solution for this problem had already been identified, this was now a pressing need, which ended up allowing CT-Spam to move forward with its activities.

Again in 2009, two other relevant events occurred to favor CT-Spam. At CGI.br, the representative of the telecom operators, who at the time was a specialist in pay TV, was voted out in favor of Eduardo Levy, who immediately began discussions with the multimedia communication services operators.

Still in 2009, debate began in Congress over the bill that would become Law No. 12,965/2014, known as the Marco Civil (Brazilian Civil Rights Framework for the Internet). Among other provisions, this law contained an article dedicated to regulate net neutrality in the country. It implied the participation of companies' attorneys in the debate to elucidate doubts concerning net neutrality and the way it would relate to port 25 management activities.

Sitting down with representatives of various sectors in CT-Spam meetings was a natural activity for the CGI.br, something intrinsic to its manner of operation . Management of network resources, as fighting spam had proved, requires a multistakeholder approach. The creation of sound and effective solutions depends on cooperation between key actors, with the critical knowledge and the competencies necessary to operate the measure.

In port 25 management implementation, the separation of message submission from message transportation required a negotiated arrangement amongst the telecom operators; multi-

36 Responsible for the sending of 7.7 trillion spams, according to a report in Forbes magazine, with information from Cisco. "Brazil's spam boom is no mystery. The country, says Cisco security researcher Patrick Peterson, is suffering the same junk mail epidemic that other fast-growing nations have experienced as they plug into the Internet. (...) Neither Brazil nor India is directly responsible for the flood of spam that has emanated from the two countries as their digital economies come online. Both nations are likely being exploited by global cybercriminals who see cheap domains and large numbers of unprotected PCs as an opportunity to funnel junk mail around the world."FORBES. Brazil: The New Spam King, available at <http://www.forbes.com/2009/12/08/spam-china-cisco-technology-cio-network-brazil.html>, accessed October 4, 2013.

media communication services[37] (broadband Internet) providers; and Internet Services Providers (ISPs) (specifically web hosting and e-mail providers).Also involved in the arrangement were ANATELl, the regulator of telecom operators; the Ministry of Justice, through the Department of Protection and Defense of the Consumer (DPDC, in its Portuguese acronym); and civil society groups representing the national consumer defense system. We should also mention the work of the technical sector in the preliminary data collection and the researchers experienced in construction of metrics, who proved enlightened and informative throughout the process.

Despite the apparent simplicity of technical issues for the technicians involved, especially given their international experience in setting up autonomous solutions for e-mail service providers, the Brazilian reality made solutions more complex. SCM telecom operators, the first actors approached by CT-Spam, had no control over, e.g, how many of their customers used web mail or programs such as Outlook or Thunderbird. That is, each SCM operator hosted various e-mail providers in its structure.

For this reason, coordinating all agents involved proved to be a crucial strategy for implementing port 25 management. It was necessary to listen to all interested parties and make them follow each step of the process to avoid a situation in which a significant number of net users in Brazil, for some reason, would find themselves unable to send e-mails just because they had not been warned about port 25 closing and about the need of reconfiguration before sending messages. It was therefore first necessary to migrate providers and users to an authenticated port, and only after that, to effectively block port 25. As a result, telecom operators could not act before e-mail providers did.

The coordination of multimedia communication services providers, which is a regulated sector, required including the govern-

37 In Brazil, under the General Telecommunication Statute and Rule No 4 of the Ministry of Communications, from 1995, Internet connection service is a Value-Added Service (VAS) that does not depend on any public concession, permission or authorization from ANATEL, for which reason the value-added provider is defined as a user of a telecommunications provider that supports it; in the case of Multimedia Communications Services (SCM – Serviço de Comunicação Multimídia), this relationship will be explained below in Chapter 4.

ment in the effort to legitimate collaboration. In 2010, CT-Spam reached a cooperation agreement with ANATEL, the National Telecommunications ommunication Agency (ANATEL), to implement port 25 management recommendations. The agreement involved the adoption of the measure by the operators once 90% of the user base for e-mail providers had been relocated.

Official letter 195/2010-PR-ANATEL, on its cooperation with CGI.br and its spam- combating activities made operators commit to a timeline for adopting the measures, and they were followed by Internet services providers. As will soon be seen, the document of cooperation sent previously to ANATEL played a crucial role in legitimating the committee's activities and telecom operators' effective commitment to them.

In 2011, the Ministry of Justice's consumer protection department (DPDC/MJ) was the next government agency to join the debate,[38] as demanded by telecom and e-mail services operators who feared a negative interpretation of a forced implementation of the measure by the National Consumer Defense System[39].

DPDC/MJ then issued a Technical Note – NT No. 65 CGSC/DPDC/SDE30[40] – discussing port 25 management consequences and benefits for the consumer, and alerting Procon (The Department for Consumer Protection and Defense -PROCON) offices all over Brazil. In case of complaints regarding Internet connections, it should be verified whether it was related to the blockage of port 25. After consulting with the operator and in the event that particular user had a legitimate prerogative to use port 25, it should remain open to fulfill the sound and legitimate need.

---

38 At the time, the DDPC – Departmento de Defesa e Proteção do Consumidor (Department of Consumer Defense and Protection) was part of the Secretariat of Economic Defense. Starting in 2012, the Department became part of the National Consumer Secretariat, created by Decree 7,738 of May 28, 2012.

39 The National Consumer Defense System (Sistema Nacional de Defesa do Consumidor) incorporates the "pro-consumers" Procons (state and municipal), the Public Prosecutor´s Office, the Public Defender´s Office and various civil society organizations for the defense of the consumer, whose work is closely integrated with the National Secretariat of the Consumer (Secretaria Nacional do Consumidor).

40 Technical Note No. 65/CGSC/DPDC/SDE, available at <http://www.antispam.br/porta25/brasil/notatecnica65.pdf>, accessed March 5, 2014.

The position of the DPDC/MJ,[41] backed by the entire National Consumer Defense System, turned out to be of crucial relevance to ensuring a trustworthy fulfillment of consumer defense rules for both telecoms and e-mail providers.

The Port 25 Management implementation Agreement, along with the Technical Note previously referred to, opened the way for implementing this antispam campaign in Brazil. Individuals interviewed for this study stressed that the two documents cited above and the coordinating efforts of CGI.br were of utmost importance in making the various interested parties feel confident about carrying out port 25 management activities.

In this respect, it is important to emphasize the extremely relevant role played by ANATEL and the Ministry of Justice in providing affected parties, who were subjected to them, with legal reassurances that they could implement the required activities. CGI.br was responsible for connecting the sectors involved, assuring the implementation of the different process phases and providing a permanent discussion and follow-up forum for the port 25 project as it advanced.

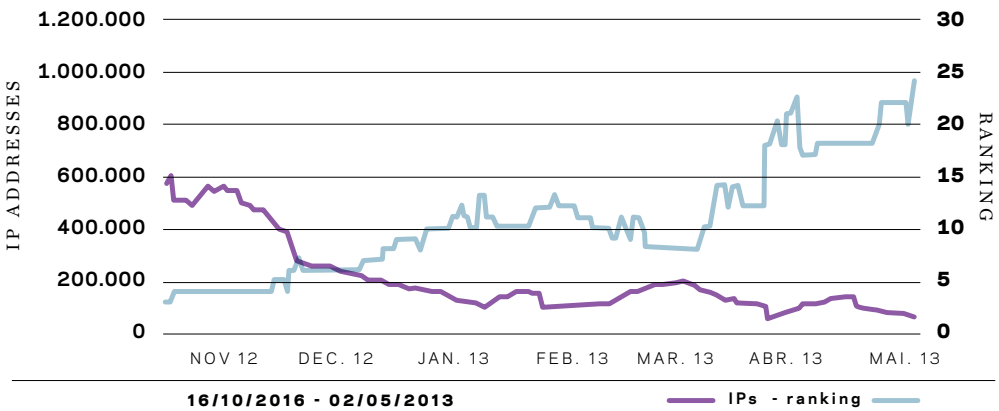
When asked whether another entity could have coordinated port 25 management initiative in Brazil, the individuals interviewed in this study agreed that a multistakeholder instance such as CGI.br was decisive for the process. Though many respondents have remarked that ANATEL and the MJ played a relevant role in creating confidence in companies, associations and other actors from specific sectors, CGI.br's role was crucial when it concerned the exchange, between agents, of realities, interests and concerns, as well as in achieving strategic decisions that helped attain a common goal: reducing spam volume from Brazilian machines through port 25 management.

41 CT-Spam did not primarily seek out the DPDC/MJ, but rather reached out to the Procons and civil society groups, who demanded that the Department take a position on the subject: "CT-Spam sought out consumer defense groups and came to us demanding that we manifest publicly whether or not it made sense to proceed with port 25 management, whether there were potential impacts to the consumer or not and whether we actually had something to worry about. It was at this very moment that we became aware of all the work done by CT-Spam and all the technical and engineering aspects of implementation surrounding the port 25 project." Danilo Doneda, Coordinator-general of Research and Market Monitoring at the DPDC/MJ, in an interview conceded to the project "Memories of Combating Spam in Brazil", September 27, 2013.

Port 25 management implementation by the actors involved was undeniably responsible for a dramatic decrease in spam volume sent from Brazilian machines. So much so that the country traded its leading position, in 2009, for a 25th place finish in 2013, according to the Composite Blocking List rank. See graphic below[42].

BRAZIL (BR) IN THE CBL

IPs and ranking evolution



Source: CBL/Highcharts.com

This result was achieved through debates in several technical meetings. As a result, collaboration was elicited from representatives of interested sectors; through a broad public information campaign, and dedicated government bodies carefully followed the progress of the project. The following section highlights relevant regulatory and legal aspects of this initiative in order to analyze any identified peculiarities and obstacles faced by CGI.br multistakeholder management approach.

42 CERT.br.Port 25 Management in Brazil: Overview and Results, available at <http://www.cert.br/docs/palestras/certbr-lac-csirts-medellin2013-1.pdf>, accessed October 12, 2013.

3 • Legal and regulatory issues

Difficulties in articulating sectors were not due to issues affecting individuals or to problems regarding convergence of interests. All the stakeholders involved demonstrated that they were convinced that the public interest governed the implementation of such measure. What remained controversial were the legal and regulatory issues to be faced. For that reason, intermediating among various sectors has proved to be a critical resource of expertise for both government and private agents when it came to issues related to emerging technologies and social practices.

One of the first legal obstacles discussed in CT-Spam meetings was the possibility that port 25 management would be contested as a violation of business freedom. As the committee work proceeded, it was proved that the suggested migration of e-mails to port 587 solely because its authentication requirement, never meant to curtail any liberties. Authentication, besides offering higher security (given that it is password-protected), would discourage indiscriminate spamming, therefore contributing to reduce the volume of such messages sent from Brazilian machines into the global network. Such a measure would not make sending messages more costly nor impose any limitations[43].

Undue spamming from port 25 caused losses to users that could be perceived in various fronts. Firstly, users rarely attributed their technical vulnerability to spammers' abuse of their machines, which led to poor performance of their machines and inferior quality of their contracted broadband. But even though this was the reason for the bad performance of their machines, users always tended to relate it to general network problems, and frequently suffered losses in the form of additional maintenance costs, machine or software replacement costs, or even contracting higher broadband velocities. For this reason, consumers first notice spam as being time-costly,

43 Interview with Cristine Hoepers and Klaus Steding-Jessen to the project "Memories of Combating Spam in Brazil", conceded on September 25, 2013.

and not as something that affects their whole connection experience.

Broadband is an asymmetrical resource that gives users limited capacities for downloads and uploads. It was noticed that international spammers were using all Brazilian users upload capacities, that is, all outgoing traffic, and that was making it impossible for users to have a stable connection and send any content to, for instance, social networks[44].

Port 25 implementation was considered beneficial to consumers by Ministry of Justice's Consumer Defense Department. Besides providing previous information about the process, it also offers a communication channel in which technical issues on the implementation process can be clarified. Risks were identified for e-mail users who used out of date e-mail clients or other means for data exchange when communicating with net servers that would depend on port 25. A market analysis revealed that the amount of such consumers was miniscule in relation to the mass of users that would not be affected by port 25 management[45].

For this reason, DPDC/MJ considered the number of people likely to be affected as being considerably smaller than the global number of consumers who would benefit from the measure. In addition, any harmed consumers could remedy their situation by contacting their Internet provider or by seeking orientation from consumer defense organisms when properly warned.

As Danilo Doneda explains:

> The Consumer Defense Code has an article that is often overlooked: the defense of the consumer must keep up with and adjust to technological developments. It was this very article that provided a nearly ontological argument for our Technical Note; one that would allow us to face such technical change, the management of port 25. Though it could affect a small number of consumers, it was essential to create a more favorable environment for all consumers. Consumers who faced eventual losses would not be seriously harmed, because they could easily revert such situation and enjoy all benefits that port 25 blockage was to bring to consumers in general[46].

---

44 Cristine Hoepers and Klaus Steding-Jessen in an interview conceded to the project "Documenting Port 25 Management" on September 25, 2013.

45 Antispam.br.Technical Note 65-CGSC/DPDC/SDE/MJ: <http://www.antispam.br/porta25/brasil/notatecnica65.pdf>, accessed October 13, 2013.

46 Danilo Doneda in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 27, 2013.

Some operators' legal departments raised questions about contractual obstacles to port 25 management. This argument was discarded after a detailed CT-Spam analysis of each service contract. It was concluded that contracts did permit this type of management as long as it was communicated to consumers.

Other issues raised during CT-Spam's work evoked implementation costs to port 25 management operators and the possibility of civil suits targeting operators in case they failed to comply with regulations or contractual obligations. After ANATEL has signed the Cooperation Agreement, this argument was no longer valid, since ever the regulatory organization stood for the closing of port 25. In economic terms, management of port 25 yet enabled operators to save bandwidth capacity that had previously been improperly used for spamming[47].

Considerations on Net Neutrality

In order to achieve its goal of substantially reducing the volume of spam sent by Brazilian machines, the parties to Port 25 Management, have coordinated efforts to close this port. This measure clearly achieved its goals, and also provoked an important reflection for maturing debates on net neutrality in the country.

Debates on the principles of net neutrality have assumed major importance in national and international forums on Internet governance and regulation for at least the past ten years, once interest for the matter has grown either amongst specialized audiences and opinion-makers or in the press in general.

CGI.br committee member Carlos A. Afonso defined the net neutrality principle, in a frequently quoted synthesis, as the precept that determines that "all datagrams are equal to the network."[48] Thus, the rule guarantees that all data traffic on the network should not be discriminated, preventing operators from privileging some data traffic over others, no matter the reason. The very rule aims

47 Interview with Eduardo Parajo, CGI.br Councelor and Director of ABRANET (Associação Brasileira da Internet) , in an interview conceded to the project "Memories of Combating Spam in Brazil" on September 25, 2013.

48 CGI.br. C. A. Afonso. Todos os Datagramas são Iguais Perante a Rede! (All Datagrams are Equal Before the Network!), available at <http://www.cgi.br/publicacao/todos-os-datagramas-sao-iguais-perante-a-rede/>, accessed September 30,.2014.

to fight any discriminations that could arise either from commercial factors (by privileging access to one's own content and, at the same time, blocking access to or impairing the quality of the content advertised by competitors) or even through political, religious or cultural contexts (preventing any type of discourse from circulating on the net).

CGI.br has elected neutrality as one of its ten principles for Internet Governance and Use in Brazil. It was drafted as follows:

> **"6.** Net neutrality. Traffic filtering or privileging must only respect technical and ethical criteria; political, commercial, religious, cultural or any other form of discrimination or favor is inacceptable."[49]

There are many experts who defend the net neutrality principle as a founding element for keeping the net an open and innovative space, by guaranteeing its potential freedom through communication transformation, access to knowledge, and individual and group identities formation, besides offering business models for companies of all areas.

On the one hand, there seems to be a consensus among great part of the interested parties on the debate about the importance of such principle; however, on the other hand, the need for occasional punctual interventions that might elicit exceptions to net neutrality rule have fostered debate throughout the world.

The opposite of net neutrality would be allowing any intermediaries that make net data transmission possible to adopt whatever criteria they wished to discriminate whatever is sent through the net. As a counterpoint to this scenario, Vint Cerf, acknowledged as one of the "fathers" of the Internet, claims that "allowing broadband providers to control whatever people see and do on-line can erode the principles that made the Internet a success."[50] And yet:

> "A series of justifications was created to support operators

---

49 CGI.br, Resulution CGI.br/RES/2009/003/P: Princípios para a Governança e Uso da Internet no Brasil (Principles for the Governance and Use of the Internet in Brazil), available at <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>, accessed October 12, 2013.

50 U.S. Senate Committee on Commerce, Science, & Transportation,.Prepared Statement of Vinton G. Cerf, available at <http://www.commerce.senate.gov/pdf/cerf-020706.pdf>,accessed on October 12, 2013. V. G. Cerf presentation to a Public Hearing on "Net Neutrality", held in the U.S. Senate's Commerce, Science and Transportation Committee on February 7, 2006.

control over consumer on-line choices, but none of those stand up to close scrutiny. Giving operators the option of discriminating data traffic on a broad scale is not necessary to protect users against viruses, neither is it for blocking spam, or preserving the integrity of the network, or to ensure that your VoIP traffic and your video features will function properly – they won't even guarantee that the operators are paid for their broadband investments. We are firmly and particularly convinced that operators will manage to define market prices for Internet access and be well paid for their investments – just as broadband operators have successfully done in other countries."[51]

In Brazil specifically, Law No. 12,965 (MCI - Marco Civil da Internet) of 2014 identifies neutrality as one of the cornerstones of the Internet law. Article 9 of the draft bill reads:

> **Article 9** Those responsible for the transmission, switching or routing have the duty to provide equal treatment to any and all data packets, regardless of content, origin, destination, service, terminal, or application.
>
> **§1** – Discrimination and degradation of traffic will be regulated in terms of the executive attributions of the President of the Republic as provided in Item IV of Article 84 of the Federal Constitution, to ensure the faithful execution of this Law after consulting the Brazilian Internet Steering Committee – CGI.br and the National Telecommunications Agency – ANATEL , and shall only apply in cases of:
>
> **I** – Indispensable technical requirements for adequate services and applications delivery; and
>
> **II** – Prioritization for emergency services.
>
> **§2** – In the event of discrimination or degradation of traffic quality as in §1, the responsible party mentioned above must:
>
> **I -** Refrain from causing damages to users, as defined in Article 927 of Law No. 10,406 of January 10, 2002 – Civil Code;
>
> **II** – Act proportionality, with transparency and equality;
>
> **III** – Previously inform users, in a clear, transparent and sufficiently descriptive manner, about the management and mitigation practices adopted, including those related to Internet security; and

51 Idem.

IV - Offer services in a nondiscriminatory commercial condition and refrain from anti-competition practices.

§3 – In providing Internet connection, as well as data transmission, switching or routing, whether costly or free of charge, it is forbidden to block, monitor, filter or analyze data packets' contents, respecting the principle set hereby[52].

Discussions on port 25 management may well come about in this context because, by coordinating activities to close this port, access to some data traffic is being denied. Deputy Alessandro Molon, former sponsor of the bill, had noticed such issue and referred to it in the report annexed to his amendment to the final draft:

> "In §1 we mentioned the possibility of traffic discrimination or degradation if, and only if, it arises from technical requirements indispensable to adequate fruition of services and applications. We therefore admit that in specific cases originated by technical requirements indispensable to adequate fruition of services and applications by final users, there can be traffic discrimination or degradation, since provisions in the following paragraphs are respected – that is, refraining from causing unjustified harm to users, respecting free competition and transparency.
>
> Thus, paragraph 1, combined with the other paragraphs from the same Article, makes it possible that spam is not redirected to user's inboxes. In case of security attacks, once Article 9 requirements are fulfilled, differentiated treatment may also apply in order to provide adequate fruition to users. Differentiated treatment to real-time videos and even VoIP, for example, can also be justified and prioritized without violating the neutrality principle – as long as the other provisions of Article 9 are enforced."[53]

In this context, both the Marco Civil and the CGI.br Decalogue texts seem to indicate that exceptions to net neutrality principles must follow "technical criteria". Thus, port 25 management would perfectly fit the example of a technical exception adopted in the country through an ample consensus amongst interested agents and by establishing a technical, legal and regulatory structure to support such decisions.

---

52 Law No. 12,965/2014, Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet)

53 Report by Congressman Alessandro Molon on Proposed Law No. 2126/2011, dated July 4, 2012.

Most individuals interviewed for this study see port 25 management as a successful exception to net neutrality, adopted with appropriate precautions, and observed a rigorous follow-up and strategic multistakeholder decision-making process.

Some respondents even remarked that it was CGI.br by thinking of situations as port 25 management when its CGI.br Decalogue restricted exceptions to the net neutrality principle only to "technical and ethical criteria", ruling out "political, commercial, religious, cultural or any other forms of discrimination or favor."[54]

In an interview for the elaboration of this tudy CGI.br board member and CEO of Brazilian Network Information Center Demi Getschko stressed that port 25 management "does not eliminate any Internet characteristics. On the contrary, messages continue to be sent. Such measure just creates difficulties for whoever intends to abuse port 25 to send unsolicited messages."[55]

In this respect CGI.br Board member Carlos Afonso remarks: "Relocating logical ports does not affect packet transfers; that is, services continue to be used in the same way. All it takes is changing port configurations (something always transparent in web mail– that is, users don't have to worry about which port is being used by providers."[56]

Discrimination of content is mentioned in various testimonials collected for this study. CERT.br members Cristine Hoepers and Klaus Steding-Jessen reflected on whether Port 25 Management could really be considered an issue related to net neutrality. "What appears to exist is a word game. Net neutrality means not to privilege any traffic over other traffic. What we seek to combat is the violation of equality. Regarding port 25, the same rule applies to all. In addition, the content of the packet is not investigated."

Addressing the issue of inspecting content, which would constitute an undue net neutrality violation, the respondents added:

"TCP/IP data encapsulation model gives us envelopes within envelopes. Metaphors about post offices are often controversial because the Net is not a postal service, but they may be helpful

54 Interview with Rubens Kuhl, Products Manager at NIC.br, conceded to the project "Documenting Port 25 Management" on September 25, 2013.

55 Interview with Demi Getschko for the project "Documenting Port 25 Management" conceded on September 25, 2013.

56 Interview with Carlos A. Afonso for the project "Documenting Port 25 Management" conceded on October 8, 2013.

here: What are the contents of a pouch? Letters. But to deliver the letters I have to open the pouch. I do not open the letters, I just check addresses to make letters reach their destination. There is no content analysis either for letters or for e-mails to find out whether their contents are advertisement or anything else. There is no analysis for content or information. And that's why port 25 management works so well."[57]

Concerns about net neutrality in port 25 management have to do with not allowing abuse of the exceptions. Regardless of the improvements resulting from such an exception, the creation of ever broader exceptions could strip the net neutrality principle of its own content.

Such an argument has been frequently heard in debates over the Brazilian Marco Civil. Port 25 management and the war on spam are always mentioned as successful examples in the dispute of opposing views on how the present Law's Article 9 should consider the neutrality principle and its exceptions.

CGI.br board member and current CEO of SindiTelebrasil, Eduardo Levy, during an interview by the site Convergência Digital, stated that "regarding neutrality, there is the expression – 'to monitor' – that we would like to suppress because it is important to manage a net so it can offer the best quality for the lowest final cost. It means that we should have elements within the network which could allow us to interfere for the benefit of all, as we did regarding port 25"[58].

Although recognizing port 25 management for its benefits for the community and considering it as an exception to the neutrality principle, Levy questions whether it would be worthwhile to incorporate this principle in law, according to his interview for this project:

> "(Port 25 management) is a good example of how similar cases, or even new ones, yet to come, and to which some net action be demanded, can be approached so that it would benefit society as a whole.

---

57 Interview with Cristine Hoepers and Klaus Steding- Jessen conceded to the project "Documenting Port 25 Management" on September 25, 2013.

58 Convergência Digital. L.O. Grossmann, L. Queiroz. Teles tratam neutralidade de rede como tema prioritário (Telecoms address network neutrality as a priority issue)availableat<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34357&sid=4#.Ulh-XmQ0i1Q>, accessed on October 13, 2013.

> We, from the telecommunication sector, fear the very existence of such a rigid law. We are very fond of the Decalogue, but we often understand that some dichotomy might arise between what we praise, a simpler, freer net for all, and us bringing along a law that might cause us to lose control over such freedom.
>
> I perfectly understand that the Internet most active groups should react against excess of regulation. I do the same, and the telecommunication sector is extremely regulated by ANATEL. Because society must benefit from the service, ANATEL cannot allow companies to operate without regulation. But freedom is much greater on the Internet. Taking away such level of freedom by issuing a law in Congress can contradict whatever is praised about net freedom."

In a presentation to a public hearing in the Chamber of Deputies on June 12, 2012, SindiTelebrasil defended the need to reformulate the text on net neutrality in the Marco Civil in order to make possible such initiatives as port 25 management, and the offering of affordably priced broadband to users who do not use all Internet resources. In its presentation, the port 25 management project is pointed to as a form of "reasonable blockage or discrimination of traffic"[59].

59 Federal House of Representatives (Câmara dos Deputados). E. Levy, "Marco Civil da Internet – A Visão dos Provedores de Acesso Fixo e Móvel: Audiência Pública", available at <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/54a-legislatura/pl-2126-11-principios-do-uso-da-internet/reunioes-1/audiencias-publicas/apresentacoes-digitais-das-audiencias-publicas/apresentacao-eduardo-levy-12.06.2012>, accessed on October 13, 2013. A presentation by SindiTelebrasil to the Public Hearing on the Marco Civil, held in the Federal House of Representatives on June 12, 2012.

If blockage of port 25, on the one hand, is not necessarily a novelty born in Brazil, since other countries[60] have adopted the measure, as have large international providers and operators[61], debates over net neutrality have assumed special relevance in Brazil, given that ts eventual exceptions are about to be regulated as stated in the Marco Civil da Internet

As mentioned above, this study on port 25 management seeks to reflect on its implementation process, its impacts, and on the lessons that can be drawn from a moment of such intense transformation in network governance and regulation through testimonials and the analysis of the most relevant issues presented by the initiative.

Just because port 25 management is viewed by its actors as an exception to net neutrality, it is necessary to clarify (i) the reasons that led to its adoption; (ii) the multistakeholder process employed to ensure against arbitrary, unilateral or decisions harmful to third parties; and (iii) constant process follow-up to encourage evaluations of its impacts.

Thus, it is important to track the evolution of debates to map the way such a winning multistakeholder coordination strategy will be employed in future fronts. Debates on net neutrality are just examples of the port 25 management importanceand explicit need of deeply understanding such an initiative.

---

60 See, for example, the work performed by Japan's E-Mail Anti Abuse Group, available at <http://jeag.jp/index.html>, accessed on October 13, 2013. For comments on the practices adopted by other countries, see also N. Rubenking. Port 25 Block Stalls Spam After All, available at <http://securitywatch.pcmag.com/spam/290791-port-25-block-stalls-spam-after-all>, accessed October 13, 2013.

61 Akamai.com. R. Beverly; S. Bauer; A. Berger, "The Internet's not a Big Truck: Towards Quantifying Net neutrality", available at <http://www.akamai.com/dl/technical_publications/truck-pam07.pdf>, accessed on October 12, 2013.

4. A multistakeholder model for public policies management

CT-Spam activities primarily reflect the governance model implemented by CGI.br. It was practically one of the first, if not the very first time, that a model like this was used as an Internet management policy in the country.

Since the beginning of theimplementation of this policy, the need for inviting nontechnical stakeholderas into the process as well as governmental subsidiary and complementary importance were noticed. Yet, net architecture characteristics were deemed relevant for political debates on the net itself, given port 25 management influenced discussions regarding the Marco Civil.

This process moved slowly, and participants pointed out various factors for delays, from the novel character of the coordination to unnecessary postponements by certain actors. However, all parties undoubtedly celebrated the success and relevance of the process for the future of Internet governance in the country.

Understanding how this multistakeholder model was created is fundamental for understanding how port 25 management implementation became possible, and for reflections on the future of new multistakeholders initiatives for public policies development.

Multistakeholder Internet Governance in Brazil

In 1995, a series of privatizations of public companies took place in Brazil, and the country's public telecommunication services were the first to be privatized. The Ministry of Communications then issued Rule No. 004/05, which defined the relationship between Internet connection and telecommunication services provided by "Active Public Telecommunication Entities in the Market". This rule, which continues in force to the present day, determines that the provision of an Internet connection is not a telecommunication service, but rather a "Value-Added Service," defined as:

> A telecommunication service that adds new services, ways or means which create specific new utilities or other novel

products relating to access, storage, transport and recovery of information[62].

And, in turn, "Internet Connection Services" were defined as follows:

(...) a generic term designating a value-added service that enables Internet Access to users and Information Services providers[63].

Such definitions are still uncertain for net regulation and governance in Brazil even decades after their creation. According to respondent Marcelo Bechara:

"(...) the provision that defines Value-Added Services states that relationships between value-added services and telecommunication services providers are regulated by ANATEL. Then, there really is some justified confusion about how far ANATEL can go, once the ambient it has regulated since 1995 has changed enormously to present day.

There existed a specific regulation for this matter – the Multimedia Communication Services Regulation[64] – and that was the direction providers, the former connection providers, ended up migrating to. In some cases, they are

---

62 ANATEL Ordinance No. 148 of May 31, 1995, which approves Norm No. 004/95 regarding the Use of the Public Telecommunication Network for Internet Access, available at <http://legislacao.ANATELanaltel.gov.br/normas-do-mc/78-portaria-148>, accessed on March 5, 2014. Translator's Note: the link was replaced by <http://www.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148>, accessed March 8th, 2017.

63 Ibid.

64 In the analysis of CGI.br committee member Marcelo Bechara in a report on the Proposal to Regulate Multimedia Communications Services (SCM) and the Regulation of Costs to the Public for Telecommunications Services for the Right to Exploit Satellite Service, after society had submitted its commentary through Public Consultation No. 45, dated August 8, 2011: (...) 2. Because it involves a broad range of services endowed with countless uses, including support for broadband, the SCM presents itself as an instrument of democratization of access to information technologies, a reduction of inequalities in this access and the instrumentalization of such fundamental guarantees as education, health, information and communication.

The SCM created by Resolution 272/2001, as a result of the rapidity of technological innovation in the IT sector and the convergence of telecom services and the Internet. (...)

5.2.Therefore, SCM emerged as a means of broadening access to data transmission, including Special Limited Service in the submodalities of the Specialized Network, and a Specialized Circuit, closely resembling the authorizations of the Networked Telecommunications Transport Service (SRTT), which also comprised the Dedicated Line, the Packet-Switching Network, and the Closed Circuit Network.

both telecommunication services and value-added services providers, sometimes as single companies within an overall business structure."[65]

Therefore, as important as it as in defining Value-Added Service and Internet Connection Services, Rule No. 004/95 was the first decentralizing sign towards Internet development in the country, establishing an autonomous relation between Internet connection services providers and public telecommunication services companies, which stimulated competition and private initiative.

In the same year, the Ministries of Justice and Science, Technology and Innovation issued a Joint Statement on the development of the Brazilian network which marked the end of state management of Internet connection, as well as the creation of a steering committee to organize the national network (CGI.br) with representatives from the two Ministries, and from backbones' operators, connection providers, users and academia. Among the rule's provisions, the following stand out:

> "1.4 Corporations and public organisms' participation in providing Internet services will be complementary to private initiative participation and will be limited to situations in which the public sector be needed to stimulate or induce the emergence of providers and users;
> (...)
> 7.1 In order to make society's participation effective in decisions involving Internet implantation, management and use, an Internet Steering Committee will be created. Such committee will count on the assistance of the Ministries of Justice and Science, Technology and Innovation, and of backbone operators and managers, as well as representatives from access or information providers, users, and the academic community.
> 7.2 The steering committee will be in charge of responsibilities such as:
> (a) fostering the development of Internet services in Brazil;
> (b) recommending technical and operational standards and procedures for the Internet in Brazil;
> (c) coordinating the assignment of Internet domains, the reg-

65 Marcelo Bechara, in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

istration of domain names, and backbone interconnection; (d) collecting, organizing, and distributing information on Internet services."[66]

Brazilian Internet regulatory environment has not been developed by any political centralization, though this does not mean that it occurred without control. Creation of the Brazilian Internet Steering Committee resolved the lack of a specific regulator by assuming the main characteristics of a network: decentralization, colaborativism , technicality, and policy.

Following the Joint Statement above-mentioned, the Inter-ministerial Ordinance No. 147[67], dated May 31, 1995, created the Brazilian Internet Steering Committee with the mission of: supervising the availability of Internet services in the country; establishing recommendations for the strategy of implementing and interconnecting networks; both analyzing and selecting technological options, as well as the functional roles of companies and institutions of education, research and development (the IEPDs in its Portuguese acronym); recommending both technical and operational standards and procedures, and a code of ethics, for all Internet services in Brazil; coordinating the assignment of Internet Protocol (IP) addresses, and of registering domain names; and recommending operational procedures for network management, among others.

With that, multistakeholder representation to CGI.br initially comprised: (i) one representative of the Ministry of Science, Technology and Innovation, in charge of its coordination; (ii) one representative of the Ministry of Communications; (iii) one representative of the Telebras system; (iv) one representative of the National Council on Scientific and Technological Development (CNPq, in its Portuguese acronym); (v) one representative of the Rede Nacional de Pesquisa (National Research Network); (vi) one representative of the academic community; (vii) one representative of service providers; (viii) one representative of the business community; and (ix) one representative of Internet services users' community.

---

66 CGI.br. A Joint Statement by the Ministries of Communications and the Ministry of Science, Technology and Innovation, May 1995. Available at <http://cgi.br/about/>, accessed on March 5, 2014.

67 CGI.br. Portaria Interministerial nº 147/95, available at <http://www.cgi.br/regulamentacao/port147.htm>, accessed on March 7, 2014.

Marcelo Carvalho stresses the contribution of the Working Groups within the sphere of CGI.br regarding the accomplishmentof its attributions:

> "In order to develop its activities and increase society's participation into them, one of the objectives of its creation, since the first meeting, CGI.br began to establish working groups and improve their organization aiming to foster Internet services development in Brazil[68].

In such context, the active support of CGI.br became essential for the port 25 management project, as stated by various actors who also remarked on its role in coordinating decision-making process regarding Internet policies implementation. There is no consensus, however, about what would be considered a specific definition for a multistakeholder principle.

DeNardis and Raymond affirm that such a multistakeholder aspect should not be applied as a principle in itself, but rather as a management goal that would help achieve an optimal point by promoting balance and stability amongst objectives and priorities. According to the authors:

> "(...) the multistakeholder approach should not be seen as a value per se to be homogeneously applied to all Internet governance functions. On the contrary, the appropriate approach towards a more efficient and responsible net governance demands reflection on what sort of arrangement would be the best to balance innovation, interoperability, freedom of expression, and operational stability in each functional and political context."[69]

DeNardis and Raymond also state that the legacy of a governance model based on standardizing agencies and business decisions generates governance models with two main characteristics: (i) government-free decision-making processes; and (ii) Internet governance decision-making processes that take into account only technical aspects and market choices. Thus, one can see that coordination problems are more common than collaboration problems.

---

68 M. S. Revoredo de Carvalho. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição de mecanismos de governança (The Trajectory of the Internet in Brazil: From the Rise of Computer Networks to the Institution of Governance Mechanisms). COPPE/UFRJ, Rio de Janeiro, 2006, p. 142.

69 Social Science Research Network.L. DeNardis; M. Raymond. Thinking Clearly About Multistakeholder Internet Governance, available at <http://ssrn.com/abstract=2354377>, accessed on March 8, 2014..

Reaching a satisfactory level of coordination has proven, to be as complex as combating the threats the network faces every day. And yet, reaching a standardized level of coordination is not only impossible, but also undesirable. Beyond achieving an optimal coordination model, certain basic premises are beyond question, such as those listed by the Conficker Working Group, in its "Lessons Learned" report from 2011. Such premises do not specifically mention a multistakeholder model; however, they praise cooperation among various levels of actors and governmental involvement and support as a counteraction to the volatility and velocity of threats, as well as the need for a fast, easy and effective communication.

Regardless of terminology, the port 25 management process was characterized by an intense collaboration coordinated by the Brazilian Internet Steering Committee - CGI.br among actors seeking to satisfy the public interest. The implementation of such a Brazilian multistakeholder and multi-participative Internet governance model left no doubts about its success. Councillor Eduardo Levy acknowledged this result in his interview to this project:

> "Well, this is complex; yet it is beautiful from a democratic point of view and for the various forces that acted in it; and it's better still because it was the whole society who benefited in the end. Nothing was strong enough to prevent society from gaining. To me, personally, and to the whole telecom sector, being part of this process and being able to publicize it, made us very proud I guess that CGI.br actions were very important in a multistakeholder point of view, in which everyone participates. But if we lacked that, if some branches were missing, we wouldn't be enjoying all the shade. In fact, we are missing a telecom branch there, which could have been of greater or lesser importance depending on the moment. CGI.br discussions were enormously rich due to each of its participants' segment characteristics."[70]

To Port25 Management process participants, the Brazilian Internet Steering Committee - CGI.br showed that there is no leadership vacuum regarding Internet policies in the country. CGI.br implemented a model that was able to efficiently identify technical problems and elicit collaborative and coordinated solu-

70 Eduardo Levy in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

tion efforts by various actors, which made it the most democratic arrangement possible for sustainable net governance. To some, such a model must guide future Internet policy coordination. As Marcelo Bechara says:

> "I guess that port 25 was the first time that the Brazilian Internet Steering Committee - CGI.br acted more as a steering committee then as (NIC.br) because NIC.br[71] has a life of its own, managing IPs and domain names. (...) CGI, on the other hand, is more debating oriented than management oriented. This time it acted as a steering committee. But it is not a part, and I think it should be a part of its routine. It has happened in a very gradual way."[72]

CGI.br multistakeholder characteristics do not reveal the imposition of any model per se regarding coordination of Port 25 Management. However, as can be deduced from respondents' statements, such a multistakeholder model derives from the fundamental characteristics of the network. Without coordination among actors, the process would not have developed accordingly – and nongovernmental imposition would have been effective, in that one of the Internet's main characteristics is its democratic and decentralized multistakeholder aspect.

As Rubens Kuhl recalls:

> "(...) the result of a multistakeholder process will always be seen as superior to others because it takes into account propositions from all participants. It can be the best or the worst, but will always be perceived as superior. That's an advantage from a political point of view. But there was also some education for all the actors not to stand only for a particular item, nor to stick to a specific issue of their own. Then, the process might have taken a while, but I take it as a sign of our political maturity to behave so before deciding."[73]

---

71 NIC.br – the Brazilian Network Information Center was created to implement decisions and projects of the Brazilian Internet Steering Committee (CGI.br), which for its part coordinates and integrates network initiatives and services in Brazil. To learn more: <http://nic.br/about-nic-br/>, accessed June 2, 2014.

72 Marcelo Bechara, in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

73 Rubens Kuhl in an interview conceded to the project "Memories of Combating Spam in Brazil" on January 17, 2014.

5 • Conclusions

Brazilian Internet Steering Committee works on a daily basis with Internet issues that are intrinsically related to its multistakeholder characteristics. By maintaining such characteristics, CGI.br not only erected its own structure, but also elaborated its decision-making processes.

Port 25 management may seem a dry topic, too technical to grasp. This work attempts to shed some light both on the management process and on what fundamental reflections can be drawn so far from Brazil's experience in the war on spam. Ensuring democracy does necessarily mean ensuring the best interests of the public through a more democratic decision-making processes. Entities such as CGI.br can serve as an example that will foster the testing of the future potential of such programs.

Hence, CT-Spam's work, mainly through the implementation of port 25 management, demonstrated that such a multistakeholder decision-making process model is successfully operational when the best practices of all participants converge on the public interest.

By virtue of having played such role, CGI.br occupies a privileged position for the coordination of future multistakeholder challenges, which will aim to improve Internet governance and use in Brazil. As one of the respondents to this study said, its next challenge might involve the transition from IPv4 to IPv6, given that port 25 management has provided the experience needed for a new multistakeholder coordination initiative by CGI.br[74].

To the extent that it involved telecommunication operators and providers, the experience of managing port 25 made evident how different companies may work together despite their diverse interests when focusing on the same net governance and regulation issue. Because various actors have increasingly advocated multistakeholder decision-making processes, it becomes relevant to observe different perspectives within each of the sectors, how

74 Interview with Eduardo Parajo, CGI.br Councelor and Director of ABRANET (Associação Brasileira da Internet) , in an interview conceded to the project Documenting Port 25 Managementl" on September 25, 2013.

they are identified and solved in a consensus-building process that enables discussions to advance.

From the consumer's point of view, it is worth noting that Brazilian Consumer Defense Code has oriented the national consumer defense system's works through its collaboration for the strategic multistakeholder decision-making process. Likewise, the Brazilian Consumer Relations National Policy aims to fulfill consumers' needs by improving their enjoyment through its own standards of consumer protection and technological development[75].

Although this new technical design could negatively affect a small number of consumers, it was essential for the creation of a friendlier environment for the vast majority. Blocking port 25 might cause occasional damages to some consumers. However, that would be a temporary situation and those users would not really suffer great harm, particularly in comparison to the benefits to the entire community of users[76].

A primary conclusion about port 25 management of Brazilian networks is that multistakeholder coordination is an absolute requirement for Internet policies. CGI.br coordination of actors from business, technical, government, civil society and academia is unparalleled. Regarding the need for a highly technical and specialized solution, it was extremely unlikely that any public agency could have performed such task on its own, the respondents said. Thus, the public-private partnership based on collaboration of actors has proven to be the best way to effectively respond to Internet security and policy.

---

75 Consumer Defense Code, Article 4, the National Policy of Consumption Relations has as its objective to serve the needs of consumers regarding their dignity, their health and security, the protection of their economic interests and the enhancement of their quality of life, as well as the transparency and the harmonization of consumption relations. The following principles should be therefore met: (Law number 9.008, of 21.3.1995)
(...) II. harmonizing the interests of all involved in consumption relations as well as seeking to promote the compatibility between the protection of the consumer to the needs for economic and technological development, ensuring that the principles in which the economic order is embedded are made feasible (art. 170, from the Federal Constitution), always based on good faith and balance in the relations between consumers and suppliers.

76 Interview with Danilo Doneda, Head Coordinator of the Coordination of Market Monitoring and Studies from the National Secretariat for the Consumer - Ministry of Justice. This interview was conceded to the project Documenting Port 25 Management on September 27, 2013, in the city of Brasília.

Thus, based on our interviews and the reflections they elicited, we expect that a memoir of such process, which has already borne fruit by reducing the volume of spam sent from the country, can also promote debates on governance and regulation in Brazil, so that similar multistakeholder experiments can be reproduced on a national and international level, and reinforce our country's role in the global scenario of net governance.

Furthermore, documenting this process should also contribute to improving coordination initiatives both national and internationally on Internet governance issues. Once again, it is important to observe the Dutch Cyber Security Council's strategic recommendations in its second phase, which highlighted the importance of national and international coalitions to create international standards; permanent dialogue; regulation (self- or institutional); and knowledge.

Therefore, effective coordination and collaboration among stakeholders on Internet governance issues make fundamental democratic values possible, such as dialogue, openness, transparency, cooperation, and progressive construction of collaborative information and knowledge.

II
Interviews
Interviews by

Marilia de Aguiar Monteiro

Bachelor's degree at Getulio Vargas Foundation Law School in Rio de Janeiro, academic exchange at the Institut d'Etudes Politiques of Lille, France. Researcher at the Institute f or Technology and Society in Rio de Janeiro (ITS/RJ).

Carlos Affonso Pereira de Souza

Doctorate and Master degree in Civil Law at the State University of Rio de Janeiro (UERJ).Director of the Institute of Technology and Society of Rio de Janeiro (ITS/RJ). Professor in graduate and post-graduate courses at UERJ, PUC-Rio and IBMEC. Visiting Researcher to the Information Society Project of Yale Law School. Member of the Copyright Commission of the Brazilian Bar Association (Rio de Janeiro Section).Elected councilor at the GNSO/ICANN, representing the non-commercial Internet users (2008-2009), and an elected member of the NCUC's Executive Committee. Policy fellow of the NGO Access and a member of the Advisory Council of the NUPEF Institute.

1. Interview with Henrique Faulhaber

Rio de Janeiro, February 12, 2014

Carlos Afonso Pereira de Souza: From a historical perspective, could you explain the reasons why CT-Spam was created within the Brazilian Internet Steering Committee - CGI.br?

HF: The Brazilian Internet Steering Committee - CGI.br is an agency that deals with Internet governance in Brazil. Since the beginning, there have been concerns related to structural governance, that is, the governance of domain names and IP addresses.

After the World Summit on the Information Society[1], in 2004, I joined CGI.br, in 2005, for my first mandate. At the time there was a critical mass behind the idea that the Brazilian Internet Steering Committee - CGI.br should discuss other layers of In-

1 For more information on the World Summit on the Information Society please check the publication of CGI.br Booklets – Geneve and Tunis documents at: <http://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf>

ternet governance, and not only the structural layers.

In those circumstances, I proposed that we formed an anti-spam working group within CGI.br. Why? Because spam is a problem that afflicts Internet users; because then, in 2005, 90% of e-mail messages were unsolicited and still served as a significant vector for spreading viruses and malwares, or botnets, or software intended to steal passwords.

Spam was a significant means of infecting users' machines. But then again, on the one hand, there was discomfort and a strong desire to separate the wheat from the chaff, to see which of the incoming messages would be of interest, and whether it was not an advertisement carrying a virus. Spam was also a waste for the whole network value chain, especially for access providers, who had to spend a great deal of resources to filter out the spam for the users, nonetheless a large amount of spam would still reach them. The same happened to telecommunication businesses because, if 90% of e-mail traffic is spam, you are wasting resources, paying for a high level of broadband that could have been used for Internet navigation, and for other things. Spam had always been a problem for the Internet since its creation, but the problem was certainly increasing, and it was an issue that deserved CGI.br attention to concerns, discussions, and studies. That's how this group started: it was an initiative I took and my colleagues soon subscribed as well.

We began by holding seminars to discuss what Brazil could do to reduce spam volume; how do users behave whenever getting such undesired messages; whether some type of national legislation would fit, given that some countries (the European Union, the United States, and Canada) already had anti-spam legislation; to examine security aspects and find out to what extent we could improve internet security quality by fighting spam. We have studied international initiatives, the OECD (Organization for Economic Co-operation and Development), the ITU (International Telecommunication Union) itself, in order to draft what could become a national anti-spam program. Those initiatives were developed along independent tracks.

We held seminars and created an important web site around 2006, 2007, namely <antispam.br>, where users and net administrators could discuss problems, give tips on how users could defend themselves, and explain what was spam and what was not. We

elaborated a joint program with FGV's CTS (Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas Getúlio Vargas Foundation Center for Technology and Society), at that time, so we could work on researching spam international legislation in order to offer a bill draft that could assist Brazilian National Congress to include combat on spam into a national law that could parallel the most current, modern and pertinent anti-spam legislation of the time.

At the same time, we ordered a study by a university – in this case, the Federal University of Minas Gerais (UFMG) – to evaluate why Brazil was either on the first or the second place amongst countries from which most spam originated. Besides the inconvenience in our mail boxes, all Brazilian users received a huge amount of spam. It didn't happen only in Brazil, but everywhere in the world; even so, Brazil was dubbed "The King of Spam." According to international indicators, Brazil was amongst the countries where most spam originated from – as I said, either the first, the second or the third, but always on top. The study showed that, in fact, the Brazilian network sent a lot of spam to destinations abroad, but such spam was not sent by Brazilians. The Brazilian network functioned as a hub; that is, we had a lot of virus-infected machines; many Brazilian machines were part of "botnets". Then, international spammers used the Brazilian net to redirect spam to other countries. That's why there was such a huge amount of spam coming from Asian countries, written in Chinese, in Mandarin, that passed through Brazil and returned to Asia.

What we observed was indisputable. The SpamPots work demonstrated that we had been used; that spam was an important virus carrier and infected other machines; but also that Brazilian spam originated elsewhere in the world.

All that together – our studies, the experiences of other countries, discussions on law and this research – led us to conclude that we had to have a technical means to refrain the Brazilian network from sending out so much spam.

Blockage of port 25 was a recommendation that had already been adopted by other nations in order to prevent spam from leaving the net in its origin. That is, instead of fighting spam after it has reached a user's inbox by filtering, labeling and dumping it to trash, we turned to a method which had already been recommended by others, but never tested in Brazil, to prevent final

users' machines, even when contaminated, from sending e-mails directly by port 25. This is the so called blockage of port 25 or port 25 management: the idea we most invested in amongst the ideas discussed by the CGI.br anti-spam group and the one which gave us a very satisfactory final result, given that now, in 2013, we have left the black list top three and find ourselves in a much more comfortable position, ranking between the 25th and 30th place on the list of countries where most spam comes from.

CAF: How did you do it?

HF: As soon as we realized that such a technical measure could diminish both incoming and outgoing spam flow on the Brazilian network, we began to talk with the sectors involved in the Internet chain. This was because spam left users' homes by passing through the ISP, by telecommunication operators' communication channels, and they are all very different from one another, don't you agree? It could be fixed-line Internet, DSL, cable TV, mobile Internet, cellular telephony. Then we set up a working group, this was in 2008, to discuss how to implement such kind of blockage. This meant making e-mail users of Outlook, Thunderbird, and others migrate out from port 25, which was to be blocked. Services providers had to instruct their customers on how to make adjustments on their e-mail software from port 25 into another port, which turned out to be port 587. Communication operators from these various media – cable, cell phones, etc. –should prevent e-mails from being transmitted from any user's port 25. This only affects residential users; it doesn't affect the company. Whenever sending an e-mail, home users necessarily used an electronic messages provider such as Gmail, or others. They could not install a server on their machines to fire messages off to everyone. Actually, people didn't do this; mass mailing firing from home users was performed by software placed in the users' machines, without their awareness, by viruses. And the machine kept sending thousands of e-mails per day, without the awareness of users, degrading broadband service and placing Brazil on the top of spam lists. Such a measure mainly aimed to prevent contaminated machines to link to the Brazilian domestic network -- and they were many at that time, around one million -- from sending spam around the world using this malicious software.

Starting in 2008, we began talking with the various groups in-

volved in the problem: (i) ANATEL, because, as ANATEL regulates telecommunication companies, port 25 blockage would require its assistance, and history later proved it was indeed necessary; (ii) access providers; (iii) the telecommunication companies; and (iv) final users, through consumer's defense agencies. This led us to conclude that in order to organize so many players – we are talking about 2,000 providers, 40 telecommunication companies, and ANATEL– we would have to follow some formal procedures, some steps, what have you, to move forward. Therefore, in 2009, CGI.br issued a resolution indicating that users should no longer use port 25 when communicating by e-mails, but port 587 instead, through e-mail servers. Providers should assist users in their migration, and telecommunication companies would have to block port 25. All that based on what we had previously concluded as being best practices for diminishing spam transmitted from the Brazilian net.

We issued the resolution and began to meet more intensively, on a monthly basis; meetings attended by 15, 20 people representing these various sectors. We then noticed that, although providers were instructing users to move to port 587, communication providers and telecommunication services suppliers had not decided yet to follow them because this would depend on a regulation by ANATEL. As their sector was regulated by ANATEL, they feared being fined or otherwise sanctioned in case they did violate some regulation.

Demi and I went to ANATEL to see its president at that time. Though ANATEL was part of the Steering Committee, there had been some migration. Dr. Plinio Aguiar was leaving and Ambassador Sardenberg was about to take his place. We told Mr. Sardenberg that ANATEL, as well as CGI.br, should issue a resolution telling the telecoms that they must effectively block port 25 for the sake and safety of the Internet in Brazil.

This eventually happened. It took a long time, but protocols within the agency do take time; they pass through the Executive Council, through a whole branch of technical experts.

In 2010, however, ANATEL's Executive Council recommended that telecoms should also block port 25, as recommended by CGI.br. Things went well, and this was really a necessary step. As I said before, major access providers had already migrated their entire customer base. Neither Terra nor UOL, for example, was using port 25 any longer. They had done a great job, but it was not

enough that users stopped sending e-mails by port 25; providers themselves had many infected machines, and they were a lot. Several providers had made the change, but continued sending spam through port 25 because it had not yet been blocked.

The ANATEL resolution was a major step, but we tripped up in the next one. Lawyers representing telecommunication companies, in our meetings, would say: "Look, ANATEL told us to block it, but what worry us now are our contracts. What are consumers and consumer defense groups, the Procons, going to do about our blocking port 25? Contracts do not say that port 25 will be blocked, and port 25 has been open ever since." So we launched a campaign, targeting the Ministry of Justice and its Consumer Protection Department, where at that time Juliana Pereira was in charge of the National Consumer Office. We then worked to convince people that the measure would benefit consumers and net security. And some time later, in 2012 or so, the Consumer Protection Department issued a Technical Note declaring that port 25 blockage would benefit the Internet in Brazil. This statement provided lawyers with the reassurances they wanted, and that no consumers' rights NGOs appeared to object; not even the Ministry itself would be able to fine operators for blocking the port.

This led us to sign, in 2012, a Cooperation Agreement among CGI.br, ANATEL, operators and telecom providers, which was supported by the Ministry of Justice and the Department of Consumer Defense, according to which port 25 would be blocked within 12 months.

Then in March 2012, the year-long process began. We were a little worried because this would be a progressive project: city by city, data center by data center, simultaneously performed by different types of operator: fixed-line, mobile, cable TV, and so on. How would it affect final users? One day someone who had not been informed about migration to port 587 might find it impossible to send e-mails. So we organized a warlike operation to determine whether at that time problems were being encountered because the last thing we wanted was that the process should be halted in the middle. The agreement even provided for the interruption of the process in case reactions against it were extreme.

The truth is that, because we had previously started with our web site and publicity efforts, including press relations and seminars; specialized Internet teams and net managers with technical

knowledge were all very aware of the operation when the blockage itself was initiated. Still, there was always some concern that people who lived in remote areas, such as small cities in the country, would start complaining for not being able to send e-mails. However, anyone could find instructions on the web itself, and the call centers of providers and operators were not swamped when the key was turned. Actually, turning the key was far from traumatic. We got ready for a much more traumatic change than we ended up facing. It was a success because all operators managed to close port 25 within a year and we were able to watch, from one week to another, how Brazil fell in the spam rankings. We fell from third to fifteenth place and began to carefully monitor the amount of spam leaving the Brazilian network according to those lists.

CAF: Looking back on the very beginning of the port 25 management, where did the development of SpamPots come from? Did they derive from the partnership with the Federal University of Minas Gerais (UFMG)? Could you provide more detail about the development of this phase?

HF: We already had a project managed by CERT.br, within CGI.br, to deal with security incidents. This project involving fighting spam and port 25 was only possible because it was operationally managed by CERT.br. The team that most closely worked with technical issues was the information security team. They already had, in Brazil, a project called Honeypots that followed the same model from abroad.

And how do honeypots work? They are computers plugged into the network for the purpose of being attractive to attackers and to collect data about the attacks. This information is used to improve our defenses. So that is a honeypot. Based on this method, an international experiment already applied in Brazil, folks from CERT.br hired the department led by Professor Wagner Meira at the UFMG to perform the data debugging work that would later be known as SpamPots – these are, again, machines set up to be attacked, a kind of zombie spam machine that, as we found out later, was able to send spam all over the world.

A series of spampots was then installed throughout the country on various networks and machines set up only to collect data on the spammer behavior and on where the spam had been addressed. And starting with these databases and the variety of collected information by dedicated machines, it was concluded

that Brazilian computers machines were being used, in the international network, as mere messengers who would forward the spam to another location. This was the principle behind the SpamPots program, in which UFMG got involved in regards to ID data debugging algorithms for identification data: where did it come from, where does it go to, what is its language, and so on.

CAF: Would you say that CGI.br' multistakeholder characteristic was reflected in this process? If so, what are the advantages and challenges of this characteristic?

HF: Well, first of all, this Brazilian anti-spam experience, particularly regarding port 25 blockage, was a classic example of how a multistakeholder environment can function to promote or improve Internet governance. That is, this project typically shows how academia, the technical sector (since port 25 management is a technical process), end users, civil society and the Internet value chain; and access and communication services providers, along with the government, have to work together to attain a solution for a problem that affects them all.

Could the government have done it all alone? Actually, it could, but only as an arbitrary imposition, not by means of dialogue with all sectors, as we did. We actually got the government involved because of the necessity of considering regulation in the process. We needed ANATEL, we needed the Ministry of Justice, but at this point, the project was already in motion. Spam is a national problem. Brazil could not solve it by external means, but must develop a solution inside its own borders. And we effectively needed the cooperation of all: from academia, by studying the problem and recommending good practices; from providers and operators both doing their part. So I believe that is an example of how Internet governance can be carried out according to each service layer and why it makes good sense to have multistakeholder governance.

CAF: How do you relate port 25 management process to the debate on net neutrality?

HF: The issue of net neutrality in relation to the port 25 management emerged at the very beginning, even before the drafting of CGI.br resolution, and it was raised by ANATEL representative to CGI.br. ANATEL already worried about such debate for it was about to foster the blockage of something that has always been open, and that would come to be used as a criterion for the entire

network. Therefore, it could be seen as a violation of net neutrality. But the fact was that the conclusion, at that time – a time in which even the third sector was trying to understand whether there would be any neutrality violation or not – saw port 25 management as a technical measure that could be justified by the benefits it would bring to the net operation and security. So, it could be taken as an exception, once it touched net neutrality, but it would also be seen as a good practice because it was based on an agreement to which all parties committed.

In fact, neutrality violation is a dubious claim when you block port 25, since you examine the message header, but not the message itself; you don't investigate message contents. It's simply an address. Port 25 is an address field that must be verified by the routers in order to deliver the message.

Net neutrality violation is a controversial topic in itself. Some people don't even consider it a neutrality violation. Undoubtedly, if there had been a violation of neutrality just because the message headers were analyzed, but the issue was so broadly debated and negotiated and thoroughly thought of that no doubts would remain about that being a matter for the good of all. That is to say, it had nothing to do with filtering or prioritizing traffic in some nontransparent way in order to benefit a particular party.

So, then, what we defend in terms of net neutrality is the transparency of net management practices and that there be no differential treatment of packages or content. And that was not the case. Objectively, this issue was a false one. No neutrality violations were observed and this practice offended in no way the principles we advocate.

CAF: Some governments, regarding port 25 management, have opted for issuing an executive, administrative order that had to be followed by the private sector. It did not happened this way in Brazil, and we had this long process that had the advantage of being inclusive, while taking much longer than it certainly would have had it been implemented by a regular executive order. Do you believe that such a multistakeholder process, even if it takes longer, ends up achieving better results? Could you tell us a bit more about this issue involving the quality of multistakeholder procedures as applied to port 25 management?

HF: The example that comes to my mind when you talk of other countries which have undergone such measures through a dif-

ferent approach is that of Japan. Japan has effectively opted for a governmental decision. There, port 25 was blocked without exceptions. The Japanese came to Brazil, and we talked with them just as we were in the middle of our process to understand how we should block port 25. But Brazilian market culture and reality are very different from Japan's.

In Brazil, we have a multiplicity of players, both in terms of providing access and of providing communication services. To me, that makes it much more complicated to achieve the same goal through government intervention.

Both in Europe and in the US, where it hasn't been globally done, except through initiatives by certain operators, similar results were achieved without any efforts of any multistakeholder entity for Internet governance such as CGI.br. I guess that, for the developing world and for countries that continue to top the list of spam traffic, the multistakeholder approach is the best because it is quite complicated to do it from top down, with government enforcement, in a highly competitive environment in which you have different size players. In our case, it took a long time because we had to involve the government. Had there been a purely technical conviction about the reasons why it could have been done, everything might have been concluded a lot earlier. It took longer because we had to submit to all those governmental protocols, but I still believe it is a good pathway for countries that have not yet adopted it, and which have, currently, taken our place at the top of the spam lists.

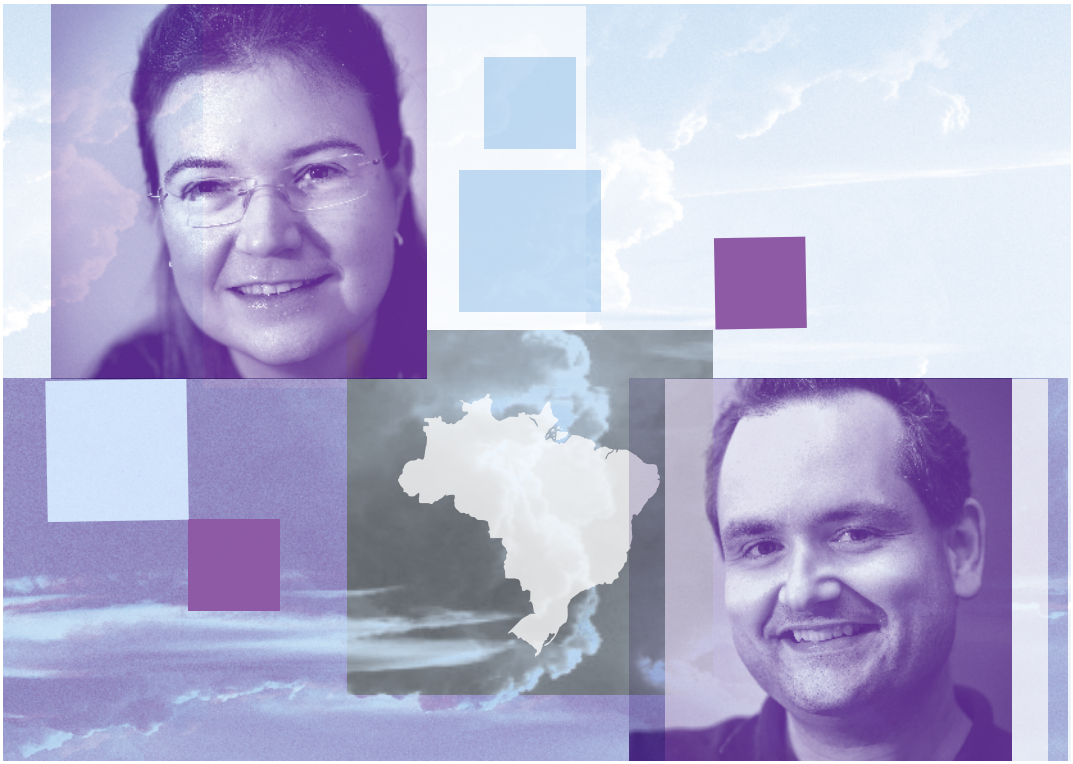
In conclusion, although port 25 management has proven to be a successful project, and it has been the most outstanding feature from all work by CGI.br working group, the anti-spam project, in fact, all aspects were summed up and each supported the other. In fact, an important initiative was born from our anti-spam project and it is still underway: email marketing self-regulation. Unsolicited commercial messages received by business users are inconvenient; on the other hand, email marketing teams need to sell their products. We have always defended that the marketing teams should not send the first e-mail before having previously established a commercial relationship with the addressee, or until users state they wish to receive those e-mails. However, e-mail marketing certainly is an important activity that supports a num-

ber of activities on the network. So, email marketing teams joined the discussions to establish whether there should or not be any regulation of the sector. One of our colleagues, who had helped us a lot during the process as a provider's representative, between 2009 and 2010, assumed the leadership of an internal process amongst email marketing providers to elaborate a code of conduct for electronic mail sending. Such code would define good practices; and bad advertisers, those who send unsolicited e-mails that would be characterized as spam, would be punished or warned by their own trade association. So that's a result I believe is still proving itself, but it was a good initiative. We have started to accept that e-mails be used for advertising, but we have set limits to individual privacy and preferences, which was considered a good result from the group's work.

Education was, to me, another fundamental issue. The <antispam.br> web site supported awareness regarding the spam problem.

We're not done with the spam problem. We no longer appear on the list ranking the major spammers, but it remains a problem. And a problem that affects other media: social networks, SMS. So this educational effort to raise awareness and alert users is a fundamental byproduct of what is still out there. We have campaigned to publicize the site, and we have noticed that because it had helped us greatly in implementing port 25 management it has become a reference.

So, to me, it was all quite positive, because we have reached our goals concerning spam. And the whole work left us with, so to say, an interesting melting pot for future issues, for us to know that it's possible to make things change through projects involving multiple sectors. When we started having spam problems, everyone said it would be too complicated a problem, one we could not handle. It is indeed complicated, as complicated as ever, but we have shown that we can do something about it, and that's my conclusion about the whole process.



2. Interview with Cristine Hoepers and Klaus Steding-Jessen

São Paulo, September 25, 2013

Marília de Aguiar Monteiro: Could you introduce yourselves and tell us about your work at CERT.br?

CH: My name is Cristine Hoepers, and I currently work as a director in CERT.br, where I started working as a security analyst. In the beginning, we used to deal only with incidents of a more technical nature, but as time went by, work here assumed a more political slant. I currently work with CGI.br advisors, training new professionals in the area, and in some projects targeting to raise awareness. At the time of the CT-Spam project, I worked more in the technical area, but I was also deeply involved in understanding the problem and convincing actors regarding the effectiveness of the proposed solution; and trying to explain to all actors what it was, mainly to those from different areas. I guess that was the greatest difficulty we had then.

KJ: My name is Klaus Steding-Jessen and I am a CERT.br technical manager. I started working here in 1999, when it was still

called NBSO, before it was known as CERT.br, so I have been here at CERT.br for quite some time now. As to my current work, I interact most with our incident response team, but most of the time I work on projects, on trend analyses, analyzing threats to the Internet in Brazil, deploying sensors such as spampots. We use other types of sensors as well. I am also involved in the training of new incident response teams, a project that began in 2004. I also advise various CGI.br groups.

In respect to port 25 management, my main task was to ensure that such an issue raises serious security matters. In the beginning, people would often say "What does spam have to do with safety?" To us, that has always been closely associated to infrastructure abuse, to net abuse. Independently of circulating spam content, it is, above all, an abuse of our infrastructure, our network. That's how we got involved with spamming, before it came to Henrique's attention. At that time, I was also attending my doctorate and some points raised then ended up benefiting the project. An early prototype of these spam capturing sensors was born there. In my discussions with CGI.br commissioners, by talking to Marcelo Fernandes, it became clear that we could develop such a project within CGI.br; we had a tiny sensor there that moved and detected what was happening regarding spam. That kept growing, and contributed, from the point of view of the whole project, by producing numbers. In the beginning, as Cristine said, no one was truly convinced that it really happened until we came up with shocking numbers. "Look, we have captured half a billion spam with only 10 tiny sensors installed in Brazilian networks". People's typical reaction at that time was to point that out as a merely theoretical problem. I guess our greatest contribution was precisely to transcend the theoretical level and showing that we were talking about real, palpable numbers.

CH: As a complement to the role of numbers, something we often heard before our investigation took place was that the available numbers were provided by anti-spam and anti-virus programs manufacturers. Thus, no matter how strongly we knew we had a problem, we needed some metric, some neutral data showing that it was real, that could help us leave the sphere of theoretical issues by demonstrating what was really happening to the Brazilian Internet. Such point came out in a conversation with Marcelo Fernandes. He said: "If it is possible for us to see that we have a problem, then we should carry out a project that illustrates its magnitude and how it came about." The project was launched in 2006.

KJ: In 2006 we began the SpamPots program.

MM: Speaking of which: I would like you to explain what damages spam causes and, mainly, what were the results of this initial project – the SpamPots project – that consequently led to the port 25 management program. And expanding the question for your further consideration, I would also like you to tell us what port 25 management is and why it was chosen as the main source for fighting spam.

KJ: From my point of view, the image that Brazil projects abroad has always concerned us. That has always been something we oriented our steps. Seeing Brazil at the top of various blacklists; that was something that motivated us to improve the way Brazil was perceived. We have always attended conferences on security, I guess since 1999, in which we would hear people saying: "Oh, but Brazil sends a lot of spam. What is happening? It appeared amongst some of the top..." Since 1999! And the same thing happened regarding security incidents: "Oh, but Brazil spreads a lot of security incidents." Year after year, due to our efforts to create a larger number of incident response groups, we noticed improvements regarding security incidents. That happened little by little, but we did not see the same improvement regarding spam. There was the same old litany about Brazil being the "The King of Spam". I don't know what you think, Cristine, but that was a great motivation to us: "how can we improve Brazil's image abroad?"

Another great motivation was that those were not even Brazilian spam. We were living in the worst of two worlds. It was already bad enough, and we also had foreign spammers abusing the Brazilian network.

CH: I guess this is the central point. We could not have said: "Oh, we're getting too many e-mails, we need better filters." That was not only about us wasting time, it was about us wasting bandwidth here in Brazil. We had to deal with the entire operational problem due to excess traffic in which all Brazilian IP addresses were becoming part of blacklists all over the world -- in some of them one could read "I wish to block any e-mails coming from Brazil". They didn't even bother to specify any particular network. Then, we had reached a position in which the whole world was acting against us by blocking incoming data from Brazil. That had a very deep impact on us and we needed to prove that all that spam was not created in Brazil, but was being sent to the whole world through Brazil by spammers who were abusing infected Brazilian machines. And there came

the greatest problem: how can you tell they are doing so? We, who work on a daily basis on the front line, can see this, but we lacked a number, a project that could convince people. And this meant a double challenge: convincing the technical teams, a task impaired by our not knowing what project decisions they had made and which could make our project implementation more expensive – we noticed that, but wasn't sure. It was something we could not explain why not to adopt, then, if you hadn't thought of net management, it could have an enormous impact.

In its impact, I guess what counted most was that: Brazil's image abroad. I guess that was the greatest political impact we suffered; the one that led to that Japanese delegation's visit. They came to ask us why we were not facing the problem. We were playing the role of "front men" for spammers on a global basis, and that's where network management came from.

KJ: It is necessary to clarify an important context in this story. CERT.br has this other project called Distributed Honeypots. It has existed since September, 2003, and aims to assess other things on the Internet in Brazil, such as attacks and infected machines, which escape spam detection. This project is still underway, it had been running for ten years in September 2013, and counts with more than 50 sensors spread all around the Brazilian network.

So, we already had developed some know-how with the honeypots. We knew how to set up a machine that would emulate certain operations without being manipulated by abusers, but which could allow abusers to perform some actions as trying to extract passwords, which we regard as a strong attack. SpamPots were, then, so to speak, a specialized variant of this project. Let's forget all other kinds of attacks and focus specifically on attacks by spammers: proxy misconfiguration or misconfiguration of e-mail servers.

In its first version, SpamPots were nothing but a modification of what we had set up for the previous project, which used such services as Honey, a software program and set of scripts that I wrote to emulate the targeted behavior.

Spammers would start scanning the whole Internet in a search for ports. They would run batteries of tests to see whether the machine could perform certain actions, such as forwarding net traffic and so on. And our system would reply to spammers as they said "Yes, it worked." It would basically instruct the computer, by these open proxy ports, to connect to the e-mail server to a particular destination and we would answer that "Yes, your command was

completed, what would you like to do now?"

Obviously, it never got connected to anywhere; it kept spammers trapped in a sort of loop. When they believed to have reached their destination, however, they would begin to inject spam messages. This was the first version, which started as a test and after a conversation with Marcelo Fernandes, it began to be installed in broadband machines. We really wanted to recreate this residential computing scenario which emulated the use of Windows on an infected broadband connection. And that was it. We chose five operators at that time and to each one of them, we used a different access modality – fixed IP, residence to residence, dynamic IP to another... and that's how we set things up for each of the five operators.

CH: We wanted to have six ones, but we never succeeded in activating connections with Oi, which was still Brasil Telecom at the time.

KJ: Right. And it was a hundred percent voluntary work. Then some CGI.br board members placed machines in their homes, such was the case of Carlos Afonso, even Henrique Faulhaber and Marcelo Fernandes. We had a little machine in which we installed Unix – OpenBSD -- and a volunteer would take this machine, plug it into his or her broadband connection and leave it running. And they still had to put up with my constant calling whenever the connection went down.

CH: Why did we choose to do it? The operators did not know that we were taking measurements. We wanted metrics without letting operator's devices know that. A second consideration is that we really wanted to simulate an actual situation: a real broadband, in a real users' home, where sometimes energy fails, or someone disconnects a cable; a real machine, but from which nobody was actually sending spam. We wanted to make the experiment offer the most experiences possible and that it did it through the most credible way.

At that time, service quality problems began to come into light. We still didn't have SIMET, the broadband project, but we had a few reports.

KJ: It was with Carlos Afonso, in Rio, with Velox, that it became clear. You could not navigate 15 minutes in a row with that thing. And it was the broadband that failed. You would call them and ask them to reset the modem and to do this or that. It was the beginning of the quality movement. Remember Mariana? What was it? AJato? The service never went down! It was more stable than many data centers, in fact.

CH: Thinking back on the project, what did we want to measure

there? A spammer-free machine. It is important to remember, once you mention proxies, that it is very difficult to explain which ports, which services we were emulating. A proxy service: you have your computer at home and want to share your broadband. A lot of magazines will give you tips on how to configure this, that or some other standard that opens to any Internet user to access your broadband. Today, most malicious code infects the machine itself, mainly the botnets, which exploit several services. One thing that they always do – they can rent one – is to open a proxy port dedicated to do this.

That's what we emulated. We did not emulate any technique for sending spam, but rather what techniques spammers used to remain unnoticed. Then we could state that the problem existed on a large scale, because the spam volume in those ten machines shocked everybody. I believe that today, after having completed our internal scripts, we have done so on a global scale.

KJ: No matter how big problems were; we had 10 machines collecting data for 15 months and 500,000,000 spam messages were captured.

CH: Incoming spam, mind you! They would have produced 10 times more spam messages, once each spam was loaded with 10 final destinations on average.

KJ: Sometimes it became a problem even for us. Spammers consumed so much of our bandwidth that our own server couldn't collect data. We had to develop a queue system in order to prioritize our goals over the spammers' ones, otherwise we could not collect the data.

CH: Another issue was often raised in our discussions on port 25: broadband is asymmetric. That is, you have a certain amount of download speed, and providers try not to tell you the upload rate, but, today, you won't have more than one mega. We saw that spammers would have it all; they would overload your upload rate because of the amount of messages leaving your machine. It ended up affecting the entire user experience. Users would not be able to keep a stable connection, could not manage to upload anything into a social network. Spammers were, then, completely flooding users' bandwidth.

Here comes something that was discussed as another effect, the bandwidth effect. Spammers were consuming more than just users' upload capacity. Then we have the study by UFMG. They worked on e-mails data-mining and also analyzed e-mails languages. We have not only seen that 99% of the IP connections came from abroad, but also that 90% of the messages had foreign destinations, and in the Chinese language. It became clear those

were people from abroad abusing our structure.

KJ: China and Taiwan.

CH: Nearly 70%. And what happens today? We can see a changing international process. We see that Brazil suffers from fewer abuses, but that spam flow keeps migrating. It is that same old story, a measure that will make spam more expensive from the moment all countries have adopted it. It became more costly for spammers to remain anonymous. And spammers aim is not to be identified; they are always looking for victims.

Everybody suffers in this chain of events: providers' IPs get blocked; users see their modem lights blinking without knowing what is going on with their bandwidth. It's a whole bunch of things. So, if we manage to make things harder for spammers to abuse, they will have to employ more costly techniques, which are not more costly in financial terms, but in terms of time, effectiveness, and in the amount of spam they will be able to send. They'll have to create passwords, or some easily detectable accounts.

KJ: Emphasizing something you said, something that was not only important to highlight the amount of abuse, but that became crystal clear, it was that the final destination was port 25; no matter which other port was being abused, spammers always wanted to get to port 25. They would come in by using a malware, by exploiting any misconfiguration on users' e-mailing sets, and would try everything, always towards the same destination: port 25. There they would find an e-mail server for spamming. That was something quite bombastic for us to demonstrate: that port 25 management would be devastating for spammers. It was something that did not only show that abuse existed, but also that they all share the same goal: reaching port 25.

At first, some operators said it would be better to block the incoming connections addressed to the proxy, and we discouraged them by saying: "look, I had 30 today!" It doesn't matter where malware was loaded, but its destination must be port 25, or else it cannot interact with an e-mail server via such port, which is the SMTP standard.

CH: In 2005, when CT-Spam began, while discussing it with Rubens Kuhl, we ended up publishing a technical document about what could be improved. At that time, we had already raised the issue, though we hadn't named it "Port 25 Management" yet because it was something that had just begun to be discussed among Internet Service Sroviders in the world, and here, in Brazil, we

were the first to recommend it in a document. Later, in 2005, a recommendation titled "Port 25 Management" was issued[2].

MM: Where did this recommendation come from?

CH: It was a MAAWG (Messaging Anti-Abuse Working Group) recommendation, but it all depends. Japan calls it OP25B (that is, Outgoing Port 25 Blocking). The first challenge was to define a topic that would not frighten managers. Blocking always does that. It is a matter of technical terms versus nontechnical terms. In the end, it relates more to management than to blocking. If you block it, you put an end to e-mailing. It was necessary to differentiate users from servers that transport and exchange messages.

MM: Could you explain the management itself?

KJ: We had that experience in all our meetings with journalists. It was incredibly hard to explain.

CH: One of the most difficult parts of the work was explaining port 25 management.

KJ: I would put it this way: in every e-mail system, there are basically two services we need to understand: submission, that relates to users sending an e-mail to a server; and a second service that relates to the transportation of e-mails, that is, servers talking to servers. Port 25 management makes such division of functions evident, and works as an enforcer that only allows the submission of e-mails by some networks, such as the residential ones. Then, basically, what port 25 management does is to prevent transportation of e-mails, because it makes no sense that we speak of transportation by a residential network, since there are no e-mail servers there. So, it serves to guarantee that submission will only happen on networks with a residential profile, 3G, Dynamic IP, and so on, and that transportation be made by other nets. It is basically designed to force it to happen only in that way.

Before port 25 management, on well-behaving networks, this would not happen; in bad-behaving networks, you would have machines there, which are actually performing transportation and trying to communicate to a server instead of trying to reach an intermediate in order to submit – and submission implies authentication. Separation and enforcement between quite distinct activities such as submission and transportation.

---

2 MAAWG, "MAAWG Recommendation": Managing Port 25 for Residential or Dynamical IP Space Benefits of Adoption and Risks of Inaction. Available at: <http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf>, accessed on 12.10.2013

CAF: I see why journalists got scared.

KJ: We spoke about ports and the guys would ask: "What is a port?"

CH: I guess we tried to improve the way we defined port 25 management over the years. Every time we had meetings with someone from a non-technical field and every time we had any change of representatives in our port 25 management group we had to explain it all again.

And there is something I am not sure whether to mention now or not, but that became the core of our working group. In 2005/2007, we recommended, we were still working. We were trying to take it to CGI.br and say that it ought to be implemented through a more political process, and they would keep saying it was a technical decision.

And meetings were indeed took place in 2009. I guess something important happened when they published the article "Brazil: The King of Spam", which had a huge impact. It was published in a lot of American newspapers, on the media, and that was when we realized the size of it all. Everybody was lay awake thinking, "But how can we do nothing about it?" I remember that CGI.br coordinator at the time telling me to write an article contesting the fact.

At the time, we were oriented to deny such information. And I wrote an article explaining that we did not have spammers, that it all was about net abuse, and I tried to link my arguments to the SpamPots program's results. That was the final push for an internal CGI.br meeting, restricted to board members. It was then decided that we promote a formal meeting to see what happened, once it had gone beyond control, we were amongst the top 10 and, suddenly, we reached the top position in all lists The article "Brazil: The King of Spam" was what provided an inflection point to general behavior. Technically, verification would be simple: to separate submission from transportation – technically simple for us. Separating submission from transportation never caused problems to anyone. Downloading e-mails from your provider needs one of two protocols: IMAP or POP. You use some other method to download incoming e-mails, but the submission process was what created most stress. But to create such division, and move users from port 25 for authentication to port 587, it could only be effective if those who provided connection could block traffic out from port 25. That gave us a lot of work because of that same old story: that you first had to migrate users, and then have specific companies implementing it, given that here in Brazil there is no such thing as one and the same company providing both connection and e-mail. We have seen that in some countries – in the USA, Comcast was the first to implement

it, in 2003, followed by AT&T –, they used to say "look, you are my client, do you wish to send e-mails from here? You can even continue to use port 25, but if you don't, the responsibility is yours."

Here in Brazil, it was a little more complicated because operators said that they could not provide e-mail, and that they had no means of blocking it. Telefônica users have n providers, Vivo and Oi clients, Internet via radio clients in the backcountry. So, it was necessary to promote such a necessary coordination so as not to upset Brazilian users, and no one could be prevented from sending e-mails. It was logical, in a way: first, to migrate providers and users to a new port, which basically meant opening up the e-mail client and changing the port, which is not a complex task. And, then: to effectively implement the blockage. And here comes what we only know because of the meetings – "Because I can't", "Because I won't"... Our regulatory model had this particular difficulty: different operators ought not to do it much before or later one another and so such coordination among actors was needed – between those who provided e-mail services and those who provided connections, no matter whether via radio, 3G, etc.

Additionally, while the process was being studied, we used to see in the media: "Then we are going to block port 25!", and we had to say: "No, pay attention, it keeps being used for transportation, it continues in use". And then some specialist, who didn't know very well what we had proposed, would show up and declare his opinion: "That is an absurd! The guys want to block services from port 25? That will put an end to e-mail service!" Yes, it will end up transportation, right?

Differences between submission and transportation were not clear to everyone. Knowing who did what regarding e-mail services access ... Our discussions made aware how difficult it was to understand numbers. Those who provided connectivity did not know how many e-mail providers existed out there. They used to think: "I don't know who's on the business, then, I won't be blocking if I'm not sure whether my users have alternatives for submission".

There were also doubts regarding web mail. We said, since the very beginning, that web mail would not be affected. Even to major providers, such as Terra, it was still not clear who used web mail and who used another service. In short, it was all about them saying that they wouldn't do it, wouldn't turn the key, unless their competitors did it too and all users had already been migrated.

CH: And that's when it began: if telecom providers will not do it, we will not migrate users.

KJ: Each was waiting for the other to move, and nothing happened.

MM: The next question is about the coordination of actors. Initially, it involved the Internet connection providers and telecommunication companies; they were the first to be contacted after CT-Spam implementation. So, in the beginning, was it thought to be a coordination of actors from different sectors or just a collaboration of technical sectors?

CH: Good question. I guess we hoped not to make it so bureaucratic. That was a technical measure, a complex action taken as a whole; today they implement several filters in their structures; we have already attended several meetings.

KJ: Our general view is that there are several good net practices to be adopted, and we guessed that really meant implementing a good practice: to prevent residential users' machines from being infected in order to send spam. We imagined that half a dozen meetings with people from a more technical staff would do, that they would be enough to ensure how much spamming represented a waste of net traffic and bandwidth, and that it was bad for them. We believed it would make them join the initiative, and turn the key. But the opposite happened, even when we talked to people from a technical background.

CH: I guess that, now, you are about to mention the problems we faced regarding the beginning of our relationship with different actors. Actually, before CT-Spam was set, we had held a meeting with the operators' technical staff and they said, "You have convinced me, but we need to consult with our attorneys and our commercial team" or else: "Will I have to add costs to my budget for equipment replacement?" There were many difficulties and the project didn't move forward.

Many said they would only do it if Telefônica or NET also did it. Suchaposition progressively prevented us from moving further, even in meeting that were 100%technical. After meetings with Henrique Faulhaber's participation, however, the technical staff changed places with the companies' managers.

KJ: Just to link such difficulties to port 25 definition, I sincerely believe that many people who attended these meetings, even from the technical staff, found it difficult to comply. I guess that many of them did neither understand how e-mails work, nor did they understand parts of what we were saying. Many left the meetings in distrust: "These people are crazy! They want us to block a backbone port?" Even in the technical meetings, it took a long time for them to understand that it was not in the backbone, but only on the net, on residential nets, and only for outgoing connections.

CH: That was when they started demanding the presence of legal and regulatory representatives. When regulatory, commercial and legal sectors' representatives joined in, the discussions started to overlap with debates over the Marco Civil. So we reached a point where all discussions ground to a halt in the face of several obstacles. We got used to hearing "We are only going to do it if our attorneys say it is okay". And finally, the attorneys said it was ok.

We began to hear such remarks as: "We could only do it if the major content providers, and the Procons get involved too." Telefônica said it would have to involve all the country's 600 Procons, but once its representatives stood alone in the matter, we suggested that we invited only Sao Paulo's Procon.

At this point, some representatives said that we should, then, also bring IDEC – Brazilian Institute for Consumer Protection (Instituto Brasileiro de Defesa do Consumidor) and Proteste – Brazilian Association for Consumer Protection (Associação Brasileira de Defesa do Consumidor) in, and someone mentioned the State's Attorney Office (MPF). It has never been too clear for us whether such claims, to bring everyone in, were true, or were nothing but procrastination. And at a certain point, meetings always had someone around the table who claimed to be regulated by ANATEL.

A cooperation agreement was signed by ANATEL; first regarding telecommunication operators, and later involving other participants.

However, we kept facing claims which advocated that, if you stand for net neutrality, you cannot manage port 25. No one will benefit from it, the rule will be the same to all, no service will be impaired – there won't be any detrimental consequences for anyone. And even after the agreement was signed, its implementation took still a while.

Port 25 management was being implemented in Europe and North America by a large ISPs working group called MAAWG. I spent a long-time talking with MAAWG's chairman and could ask him if there existed any case studies that showed the benefits of its implementation, the economic benefits for providers, and he said there wasn't because such measure was so obviously beneficial for providers.

In the meantime, here in Brazil, people could only see problems, such as: "This will cost us to implement, don't you have any studies?" Financial issues were never much spoken of, and in order to produce metrics, it was necessary that operators themselves generate figures, and didn't want to do that either. We spent almost a year talking about metrics and numbers, but no one wanted to share any information.

CAF: Cristine, why do you link this moment to the Marco Civil?

CH: Actually, what we observed had a more retrospective nature, having to do with timing. When was MCI (Marco Civil da Internet) presented to Congress?

CAF: It was opened to public comment in 2009 and forwarded to the Congress in 2011.

CH: 2011? At that time, we were facing the same debates we face today: ANATEL wanted to regulate the Internet. We saw operators wielding a great deal of influence by saying they would only do something if it was regulated by ANATEL. Even in the end, after the cooperation agreement was signed, many said they would do nothing without being regulated by ANATEL. It reflected their desire to have ANATEL regulate the Internet.

KJ: At that point, many of those representing operators were responsible for the regulatory sector. They feared that users' complaints would make ANATEL take a position against them.

CH: I don't know if it was due to MCI or not, but in 2010, after public debate of the measure, this need for regulation by ANATEL became much clearer. One could view this as a means of political leverage to force ANATEL into regulating the Internet. But why regulating it? Legal departments said that if users complained to operators, they would have to formally register their complaint with ANATEL.

Several stages followed – ranging from people saying that a letter from the president of ANATEL would suffice to others claiming for regulation. Mr. Sardenberg issued the letter, but for some, it wasn't enough. As always, the representatives who claimed regulation by ANATEL came either from SindiTelebrasil or some specific operator and these were the ones who wanted ANATEL to regulate it well.

MM: But this spam study involves analyzing telecommunication networks, doesn't it?

CH: It is a matter of TCP/IP. It will pass through the router, but some operators implemented port 25 blockage of outgoing traffic in the CPE – Consumer Premises Equipment, in the modem of home users; others did it in their concentrators. I don't know whether some implemented it in a router, but in any case, it is a TCP/IP filter that is not foundation to the Internet; that would be telecommunication.

KJ: During discussions, there was a well delineated distinction between telecommunication, and at this point, ANATEL is involved in addition to the Internet part, TCP/IP and other protocols which do not involve telecommunication. . I am not sure

I understood your question properly, whether you really believe this is related to telecoms or ...

MM: Whether that was why companies were pushing for ANATEL's approval ...

KJ: Technically speaking, we are referring to TCP/IP, ports, Layer 3.

CH: It makes no difference whether it comes by cell phone or smoke signals.

KJ: That is the Internet. I agree with Cristine: it does not matter the media it is implemented in. I, too, believe the debate had to do with networking, TCP/IP, and nothing to do with ANATEL. ANATEL's prerogative in the whole story is another discussion entirely.

CH: There are users having problems on the net and some would call ANATEL. Even at CERT.br, we receive e-mails that read "I've e-mailed ANATEL, my broadband is suffering several attacks and they told me to talk to you." We don't really know what ANATEL does with the complaints about the Internet they receive.

Yes, there could be users with problems that would indeed call ANATEL, their telecom provider, or even Procon. A serious matter of concern was the involvement of actors.

In 2009, we came to a point in which we advocated the involvement of a more politically oriented team. At that point, however, they began to insist on economic issues, on high costs, as a reason not to implement it. And while a lot was being said about damages to users, we started to hold meetings to explain the technical aspects. A key moment was when DPDC – Department for Consumer Protection and Defense (Departamento de Proteção e Defesa do Consumidor) joined us; it was when things started to move again.

KJ: To us, Marilia, it sounded more like a stalling measure. When we were getting closer, there would arise an obstacle such as our having to reach a certain percentage of migrated users. It seemed this would never happen until UOL reported it had migrated 100% of its users. Then, someone would say: "No, we have to have the letter from ANATEL." So for us, it always sounded like a delaying measure, although we think it would be unfair to generalize.

CH: Even when we brought consumer defense into the debate, they said we needed DPDC; we brought DPDC in and they said a technical note would be required. And it was never like: "You have this whole bunch of things to solve". They would always bring a new issue in every time you presented a solution.

KJ: It also looked as though they were not being well advised. Not everyone from the technical staff was convinced that the problem

would be solved, though they didn't talk about it.

CH: We got to a point in which all the obstacles had been placed and we only lacked the Cooperation Agreement to be signed. Then operators sat down with us and said they wanted ANATEL to regulate it. This happened when Levy joined CGI.br, embraced the cause and pushed it to a conclusion in late 2010.

We attended a SindiTelebrasil meeting with all the operators' regulatory Vice Presidents to hear memorable statements such as: "No, port 25 management is like an herbal tonic: it won't do you harm, but could do you some good." And then one operator's Vice President said: "But it seems to be really good, why haven't you implemented it yet?" To me, that was the peak .

KJ: This was very frustrating for us. We wrote that document in 2005, proposing good practices...

CH: Brazil was the first country to formally propose it...

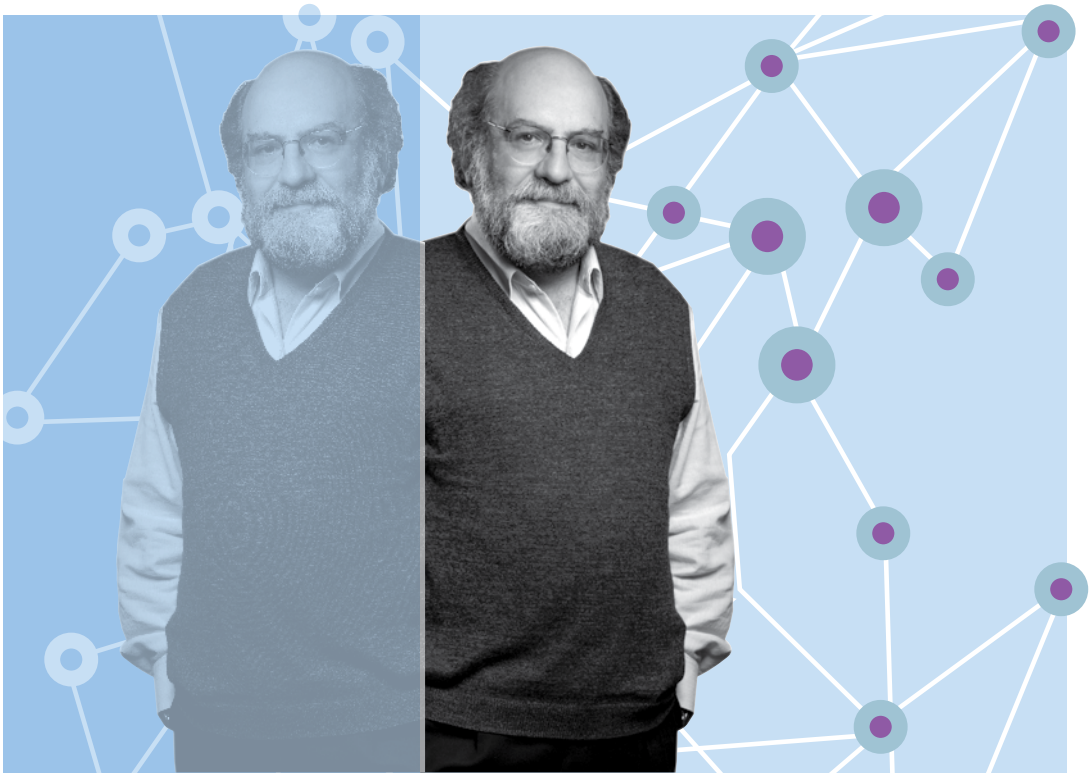
KJ: And then listening to Japan asking us why haven't we already implemented it five years after having written the paper? It took Japan six months to implement it. We know that the Internet was instituted in a different way in Brazil, the Comcast case was much simpler: if you provide both the technical means and the service, it is a much simpler decision to make.

CH: It is interesting to see how it works in Norway. We do some research within our group for CERTs around the world and they said they had already heard about that. They recalled receiving a statement from operators announcing that they would implement it because spamming was too high.

Essentially, that's what we so naively expected: it is so technically simple, so cheap to implement, and brings enormous benefits. For example, one of the operators said, during a break in one of our meetings, that it had set up an entire international management area to establish cooperation and to remove their servers from blacklists. They asked us for tips on how to be taken off such lists.

And they had been there for two years! We showed them some of issues and metrics, and got no response. And they were spending money, creating new costs by establishing an international management area.

The only clear exception is Sercomtel, which in 2006, after our recommendations in 2005, implemented it and also to present a report on why they did so.



3• Interview with Demi Getschko

São Paulo, Brazil, September 25, 2013

DG: My name is Demi Getschko, I am an electrical engineer, a graduate of São Paulo's Polytechnic School in 1975. It was there that I received my master's degree and doctorate as well. I have been involved in networks since the mid-1980s, and especially at Fapesp – (The São Paulo Research Foundation) (Fundação de Amparo à Pesquisa do Estado de São Paulo), where we made the first Internet connections, and since then I remain involved with networking. Port 25 management was brought about when we felt embarrassed at the notoriety Brazil had gained on spam blacklists. So, we decided to dive in the problem, to understand its motives and to see how we could avoid it.

Carlos Afonso Pereira de Souza: Could you explain what port 25 is?

DG: Port 25 is a port used by the protocol known as SMTP, or Simple Mail Transport Protocol – a simple protocol for e-mail transmission. Like everything else on the Internet, it is simple and in some

ways, it emulates the collaboration process we see on the Internet.

Then, what is port 25? Through port 25, any machine can access others by using this port. The machine will send a "hello" and ask the other to send an e-mail for you, that is, you will be asking the other machine to forward an e-mail to someone. Then, it was perfectly acceptable on the Internet – that you depended on help, in the middle of the way, to send an e-mail to someone. And this is the basis of SMTP. Only that is, of course, an open port, an invitation for abuse. We did not know whether there would be abuses or not; we did some research on what was happening with Brazilian spam. This has probably been relayed by more than one person: we found out that Brazilian spam was not in Portuguese. Then, through the use of honeypots, machines designed to attract spammers, we observed how much spam there was. One could then see that machines were being used to forward large amount of e-mails coming from some place in the far East and returning there. Such e-mail hit the machine and was sent to as many destinations as could be found in the users list, and returned to Asia.

We saw clearly that those e-mails were not national – they didn't have a Brazilian origin or destination. We functioned as a reflector, and the easiest thing to do was to swap out this port for another one with password authentication. You can also ask a password-authenticated port to send e-mails and so on, but if you don't know the password, let's say that abusers will try to find another machine that does not require a password and you become a harder target, you no longer are amongst abusers' first choices, once your machine doesn't leave its port 25 open. Then, you are no longer a target, and this made us fall below the 20th position on spam blacklists, which is proportionally even better, because Brazil had regularly been rated either in the 8th or 9th position. We were above the average predicted by our size and our major participation on the Internet. That, in brief, is a description of our process.

By doing so, you suggest something that could be considered a restriction on things that were expected to be open on the Internet. From a more negative point of view, you would be violating net neutrality, which contains, since its origins, in several RFCs (Requests for Comments), the possibility of being violated. And the answer is simple: we are actually suggesting an exception to network neutrality, because it does not in fact refer to neutrality, but rather to an abuse. By closing port 25, we don't eliminate any Internet charac-

teristics. On the contrary, e-mails keep being sent collaboratively, we are just making it more difficult for those who intend to abuse port 25 to send unsolicited messages. This represents a beneficial exception to the neutrality principle, and is fairly well justified. Such reasoning can be used in eventual discussions on neutrality, the Marco Civil and related topics, to demonstrate that rules are more justifiable by their exceptions than by their formulations.

CAF: Some respondents say this is no neutrality violation because content itself is not accessed; what we have here is just an analysis of addresses.

DG: If you close the VoIP port, for example, you don't investigate content of messages, but you prevent the guy from doing so. Just as when you close Telnet or TCP ports. In short, these are neutrality violations because you are eliminating access to a standard port... well, not eliminating. You are just requesting that a certain Internet standard port not be accessed for some reason. So this is no neutrality violation in the sense that you went there and vetoed the contents of some messages. This because, when you combat spam, we believe that fighting spam should never be done by defining its contents. If we try to fight spam by the content of messages, we would be walking into a dangerous pool of quicksand. We define spam by the behavior of the message and not by its content. At that point, in my view, we had some neutrality violation because we asked that a certain Internet standard port not be used anymore for the general benefit of users.

MM: Then, not analyzing content is a question of privacy?

DG: Not analyzing content is an issue that establishes that content should never be analyzed in intermediate instances. The only party allowed to access content is the recipient. For example, as a recipient, I have the right not to receive adult-themed messages and I install a filter. No intermediate party has the right to say, "Oh, this message is not good for you!" Only I can do it, being the final addressee –it could be a man or woman responsible for his/her family who could prevent children from watching this at home. But this is up to the final user, who could be a family or the responsible for a family. And this guy is the one that can filter unwanted messages: "I don't want biased e-mail, or adult content, or I don't want to receive jokes", In short, these are users' decision, and no intermediary can engage in this kind of filtering unless authorized by end users to do so.

MM: So privacy issues were not addressed in discussions on fighting spam or on port 25 management?

DG: No, privacy never came up. We never defined spam in terms of whether it was commercial in nature or not. We think of spam as something you receive without having solicited, something you are not interested in. There might be something that interests you. In early Internet days, we used to say "This spam thing, it's so cool, because I never receive anything and suddenly, I get something funny, sometimes some attractive bargain." So, in the beginning of the Internet, when the net was slow and you received no e-mail from anyone, at that time one could find someone saying that wouldn't mind getting some trash, because sometimes I might get interested in something. Obviously, as time passed, it became a large amount of trash, something you didn't like anymore. But we define spam as something unsolicited, no matter if the message itself is great or not.

MM: Isn't port 25 blockage imposing limitations on commercial freedom?

DG: You might say it imposes a limit on such a right, but in fact, if you think well about it, using port 587 will cost nothing, once it is as open and cost free as port 25, it only requires a password. Therefore, there won't be any business limitations. I guess, for example, that e-mail campaigns that lack the "opt-in" feature, that do not offer users the right not to receive them, constitute spam. You should never be able to advertise to anyone without their previous consent. You may well characterize a commercial activity as spam; it belongs to a grayish zone in respect to whether or not you should stimulate it. Users are more entitled not to be harassed by spam than I am to sending them. Obviously, I have the right to send e-mail to whomever I wish, but the person has the right to refuse delivery.

MM: Were such measure implementation costs somehow viewed as a barrier for implementing combat on spam?

DG: No. In general, people do not feel we all save money by doing so. Operators surely waste a lot of bandwidth sending spam here and there, so, bandwidth is unjustifiably costly. The first issue is economic. End users also save when companies don't absorb costs. Over the last mile, the end user also calls for savings that the provider refuses to assume. Danger lies, of course, in your closing a port like this without previously informing users who use down-

load and upload e-mail, use e-map interfaces and so on. Users must be warned to change ports in their definitions, otherwise there is a risk that users stop receiving e-mails for a while and complain. For this reason, we managed the process very carefully and held awareness-raising campaigns. Users were informed by providers. We also called in people from Procon and the Ministry of Justice, because providers wanted to be sure that they would not be sued by suggesting users to change ports – and some e-mail got lost in the process. They feared the risk of being blamed for it, but the opposite happened: they were actually complimented for that. I believe that was an unjustifiable fear, but one is supposed to prepare for risks.

MM: What about the delay in implementation? What can it be attributed to?

DG: First of all, this is not something that can be rapidly implemented. Let's say you have 200,000 users and 50,000 of them use e-map or some other form of messaging. You will have them all, one by one, reconfigure their port before you close the old one. Configuration is a time-consuming task.

Later, we had a legal phase in which providers began to worry about liability, whether they might be liable in all of this. A consumer could tell Procon, "They ordered me to it, but I don't know how..." So we consolidated our communication with the Ministry of Justice, the Procons, and so on. There was a rhythm, it could have been carried out faster, but it also required focused caution. First, we observed the results of those who had already implemented it and used them to stimulate others to do so as well. Some operators started earlier as Brazilian e-mailing operators, Internet content operators; they started earlier. It became evident that this was not complicated, and from then on, people moved faster and faster. It became a flow. We hope that the same will happen with IPv6 as well but I don't believe it will.

CAF: And how is it going, this IPv6 relocation? What to expect?

DG: Regarding IPv6 implementation process, we have, in our favor, the fact that we are not the first place in the world where IPv4 has come to an end. There is no more stock in the Asian domain registry, the APNIC. In Europe, I gather that RAIP announced the end of the final block this April (2013). So, the Asians and the Europeans moved before us in this process. The next region due to run out of addresses is in fact Latin America along with North America. It is difficult to know who will run out of them first be-

cause North America is a major consumer, besides exhibiting a powerful legacy. Africa, in that it has a large reserve and little consumption, will be the last.

We are constantly mindful that such things are not interoperable. IPv4 and IPv6 are different. You will have IPv4 here to reach the IPv4 world, and IPv6 to reach the IPv6 world. The truth is that you won't have to have an IPv6 domain, you will automatically receive an IPv6 when IPv4 addresses are done. So, the next wave of users will come using Ipv6. If they don't find a world that can communicate in their language, which is IPv6, their Internet experience will be bad, broken, truncated.

Let me give you an example: everyone pays income tax in March or April by using <receitafazenda.gov.br>; you use the system and it works. If you are a fresh user who will access it in January or February though PNBL – the National Broadband Program – or whatever the case it may be, and you receive an IPv6 address because there no longer is IPv4, if you get to <receitafazenda.gov.br>, will you be able to access it? Not today. It means that few Brazilian sites work with IPv6. To give you an example, today we have the Federal University of the State of Santa Catarina; another is UNESP, that works well with IPv6; I guess the State of Ceará has an e-government site that works well. We have a program called "Validator" that enables you to write sites' names to see whether they already respond to IPv6 or not.

Major portals already respond to IPv6. If you are a UOL user, they respond; so does Terra and, of course, all of international services such as Google, Facebook, because those people are not asleep.

We have a very important problem to be addressed. It concerns the sites that offer services to citizens, governmental sites from all instances which, in general, are not paying attention to it. CGI.br has just issued a resolution aiming to stimulate people to pay attention to it: sand is flowing in the hourglass and IPv4 time is coming to an end.

CAF: So is there a parallel between port 26 management and IPv6 regarding communication, education and partnerships?

DG: I really don't see a parallel between them. After all, you have to convince people who don't see. I mean, at this point, the processes are equal. The impression is "We are doing fine; why do we need this?" I hope, in this case, that international paradigms be even more important than our pressing. If you keep insisting

that is important, they will adopt it slowly, but once they perceive things are changing abroad, it will be different.

MM: Do you believe the same happened to port 25 management, whose blockage CERT.br has been suggesting since 2005 as a good practice, but was never speeded till 2010, after a Japanese group stated that Brazil needed to implement it?

DG: What we actually showed the Japanese government, when they came here, was the differences in our closing port 25. They had not come to tell us Brazil had to do it, they came to tell us how they had done it. And we used it to tell people here: "Look, they have had good results over there." That was very interesting for us: the first thing operators used to say was "we cannot do anything unless it is regulated by ANATEL; we are telecom operators and have to answer to ANATEL." We drafted a document, signed by ANATEL coordinator, Mr. Sardenberg, and by CGI.br coordinator, Mr. Gadelha, that emphasized the problem. Soon arrived Levy, a representative of the telecoms who picked up the fight by saying: "If telecoms don't sign this individually, I will sign in the name of Sindi Telecom, SindiTelebrasil and so on"... It was then signed and all arguments against it were defeated because it became clear that it would not expose them to risks, but rather to praise. Everybody was happy in this stage became history.

Now we hear arguments such as: "You see? If we had the Marco Civil then, nothing could have been done because it violates neutrality." It has nothing to do with anything, but an argument is an argument.

CAF: What about "We'll remove control over port 25 if the Marco Civil is approved."?

DG: Exactly. They will open port 25 supported by the Marco Civil and they say nothing will happen. If you open port 25, spam will gradually return. It won't happen immediately because you have to change the port in your PC to port 587. If they threaten to do so, they may do it, no problem. But we, of course, don't want them to do it.

As to IPv6, we are rooting for signs of progress. It's not trivial. What happens on the Internet, and this is both a good and a bad thing, is that it always defends itself so as to guarantee its own survival. IPv4 was supposed to have ended in 2001. Why hasn't that happened? Because someone came up with something call NAT, which is that thing you use on the router free networks. For

example, net 10. Everybody uses net 10 in all local nets. Net 10 was eliminated from manual routing for an IETF RFC. So what does this mean? You walk away with 8 million repetitive e-mail addresses, leaving only 3 or 4 in the port. You have save a lot of addresses. Instead of needing 8 million addresses, you use only 8, because you have hidden millions in each one of them. Such a tactic added 12 years to IPv4 lifespan.

And now we face another maneuver, known as the double NAT. There, instead of gathering an ocean of unique addresses, you get these unique addresses and create several ports amongst them for the same translation. You get a simple IPv4 and, besides hiding an entire IPv4 net behind it, you can still map it for IPv6 by using different ports. It is not very good, it's called Double NAT. But it's a way of stretching it a bit, of giving some more lifespan to it. It would have been ideal if we had created the IPv4/IPv6 double approach while there still was IPv4 enough. That would have been painless and trivial. Now we lack enough IPv4 addresses and have to use the Double NAT. But this is a technical approach that we don't have to use; there are various alternatives...

CAF: This publication would like to emphasize the participation of various sectors, actors and agencies. Among the governmental representatives in port 25 management, do you recall any entity, any governmental representative that has played a significant role?

DG: ANATEL is not exactly a governmental department; it's a regulatory agency. But ANATEL immediately supported the CGI.br initiative. Sardenberg signed that agreement with Gadelha and told everyone that he recommended operators to work on port 25 management.

CAF: Any other governmental department?

DG: Not that I remember, no. I don't recall any involvement of the Ministry of Communications, especially because only operators were there. The active partners were, basically, access and information providers, major portals, such as UOL and Terra, and people who provided e-mail, and who had to teach users, and telecoms, because, in general, the last broadband mile is always in their hands.

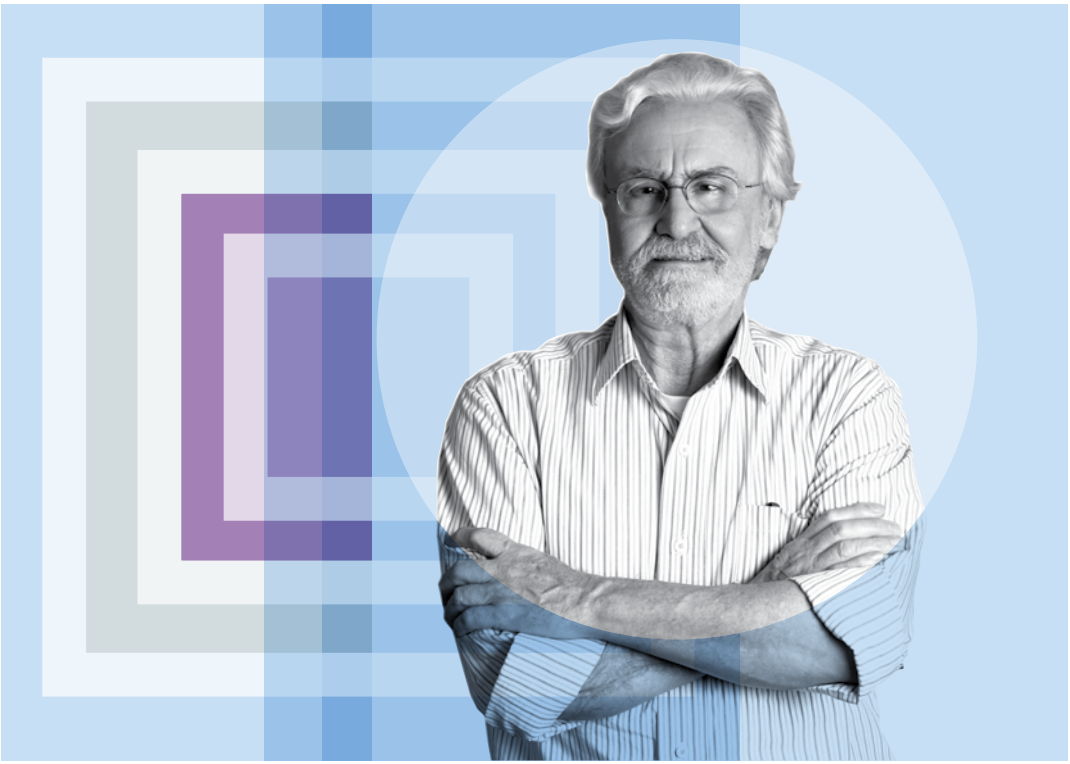
CAF: Besides commercial freedom, do you remember any debate over freedom of expression? The two are very different debates.

DG: Debates on freedom of expression only came up along with discussions on spam definition. A little of that also came out in

Dubai, because, in Dubai, we came across a somewhat awkward definition of spam, which was later withdrawn, but was counterattacked, and I don't know where things stand now. There is always the risk of us having a spam definition that leads someone to read e-mails in order to see whether they are spam or not. Then, you may open up a window that might never be closed again. "I will read it to see whether it is spam or not." And you will be violating privacy in a totally inappropriate manner. So I guess this is the only moment when such discussion came up, because much damage could be caused then.

MM: Do you think that any other organization, if not CGI.br, would have been capable of implementing port 25 management?

DG: The problem is that we spend our days discussing Internet matters. No other staff is so exclusively dedicated. Telecommunication agencies discuss spectrum; ANATEL discusses allocation of frequencies; each organization has its own focus. And there is CERT.br, our team – who, perhaps, should discuss a little more the honeypots program they have there, which captures not just spam, but malicious software and new viruses as well. So, we already had a tradition in this area of discussing figures or performing qualitative research on tracking attacks, that is, what the new virus was. For instance, there is a discussion on spam and service denial, both following the same line. That is, machines especially designed to function as zombies during an attack that impairs service. Spam is not so bad, because there is a port for service delivery, but it's the same thing: you look for weaknesses in the users' machines and seek to exploit them according to your interests, and that was the solution we have found in the management of port 25.



4. Interview with Carlos Afonso

São Paulo, January 24, 2014

Carlos Affonso Pereira de Souza: Could you explain to us in detail what port 25 is and why was it important for CGI.br to coordinate its management process?

CA: Port 25 is the standard port used by e-mail servers. This is the port where messages are sent from by SMTP – Simple Mail Transport Protocol. E-mail servers use this standard to communicate amongst themselves. It can be changed if everyone agrees, but that is the standard – just as FTP uses port 21 to copy files, etc. Users of services that send e-mails through an e-mailing program, such as Thunderbird or Outlook, cannot use any predefined port for connection with their e-mail service provider. Nothing makes it easier or harder for e-mailing. And it has nothing to do with incoming e-mails, only with outgoing traffic.

What is so problematic about leaving port 25 open to any final user? The problem is that, since the intelligence of the Internet

resides in the endpoints, any machine connected to the Internet can, in theory, run an e-mail server in any machine and spammers use it as follows: they contract a broadband connection, connect a laptop to it with one e-mail server software installed. A small Windows or Linux machine, whatever, sits there automatically sending messages through port 25 as though it were a genuine e-mail service provider. It is, then acknowledged by the e-mail services community as just another e-mail server.

And therein lays our problem, because this practice facilitates spam on a vast scale. If you want to send out spam and need to use your own, properly managed e-mail provider, things get harder because there are operating rules, agreements, and even ethical codes amongst providers seeking to minimize this entire issue. But if you have your own residential Internet service, your PC can operate the server from a location not subject to control by anyone else. The idea is to move the logical address of the port so that the endpoint user can send e-mail through an e-mail service provider. As a matter of convention, this port already existed, and as a matter of standards it is always an encrypted connection, using the starttls standard, which resides on port 587, a port set aside for this exclusive purpose: to send a message to its server through the user's own e-mail account. For end users, nothing changes. For spammers, there are significant changes, because he can no longer pose as an e-mail server on a network endpoint. This, then, is the importance of migrating to this port. For end users, instead of using port 25, port 587 is used. If you are a company or any organization with a broadband connection, you may request that port 25 be reopened, because you want to handle your own mail.

There is no ban involved here. This was a collaborative proposal for minimizing spam, which is based on the installation of a server on an endpoint that sits there sending out as much spam as it can. This has had a very positive effect. There has been a noticeable reduction in spam mails. For the first time in Brazil, all known e-mail service providers follow standard rules in order to avoid spam. Clearly, they need to do so, considering that broadband is extremely costly in Brazil. Providers have, let us say, a 100Mbs connection, and there are small providers whose owners do not want 30% or 40% of their bandwidth to be used by spammers. So, they save on bandwidth, which is an advantage for them.

It is interesting here to remember Principle 6 of the CGI.br Decalogue for Internet Governance. When, after years of discussions, we approved the net neutrality principle, we took the precaution to add "except for reasons of a technical nature." All the rest is, as I used to say and still do: "all data packets are equal before the net."

This, then, is an issue of a technical nature: It involves changing a port number. You know that there are thousands of ports that can be used for all kinds of services. If two parties came to an agreement to use a specific port, they could use any port they configure for such service. For example, files are not sent over port 21; but over port 2221. You have to coordinate it with the other guy. If you both agreed to it, things will work the same way.

The problem is to follow standards so that the whole network can recognize what you are sending as an e-mail, or a file transfer. These are the standard protocols.

CAF: I would also like to hear your comments on multistakeholder participation (and the role of CGI.br) and on the net neutrality issue. Let us continue with the neutrality issue. Blockage of port 25 would count as a technical justification for analyzing and investigating the headers of messages and, based on such analysis, not to forward the message. The question is: can we say that port 25 management is an exception to the Internet neutrality principle as provided by CGI.br regulations, or wouldn't it have anything at all to do with debates on neutrality as it doesn't refer to any privilege for one packet over another?

CAF: This is a discussion that frequently emerges in the interviews we have conducted to date.

CA: It forms part of the discussion, but only as an exception to the rule. Look, let me tell you something: all message headers of all packets are automatically analyzed. Why? Because the router has a switch that decides where to send a given packet, and the switch needs this data; the metadata of the packet to determine its port number; to know where to send it to; to determine whether it is FTP, SMTP, etc. All information in that message header is automatically read, otherwise the packets won't travel. The router needs to know it in order to route. This is not a violation of net neutrality. On the contrary, it is a fundamental principle of the Internet that the least possible effort be used in order to send the packet to the other side. So this is not a problem of reading message headers; on the contrary, it is being constantly, automatically read.

It is different from either reading the headers in order to extract other kind of information or to attempt to gather data for profiling, or to prevent the packet from being delivered as it should be as defined by the port at the IP address. That would be different; you would be interfering with where the router automatically decides to send this packet to. Very different!

CAF: In this whole process, CGI.br played an important role in coordinating various actors. Can you explain CGI.br coordination role?

CA: Again, this was extremely important, not only because it reinforced the principles we established, but because of all the work CGI.br does as a facilitator of network security responses. Let me sum it up as follows: We have no formal authority, but we do have the credibility to propose measures for maximizing net performance. Along these same lines, we had previously undertaken an effort to unbundle the network at the loop end so that more than one broadband provider could use the same physical infrastructure, but we failed to succeed regarding ANATEL, just because the operators said no. But this is part of our work: issuing recommendations, like this suggested unbundling, as it is known, which gives you more broadband options at the endpoint, more options for your equivalent fixed-line telephone service.

Our work on port 25 is the same thing: we identified a problem that was not ours alone. It is a global problem and we proposed discussing it with the main broadband operators in search of a decision to block this port, but making it clear that users could request that it be unblocked. In this case, users face responsibility, right? It does not mean that using port 25 is forbidden. The operator will block the port– and operators are not always blocking it, we have tested and it is not always blocked – but let us assume they all did. It is not mandatory, there is no rule against that, it was a collaborative agreement. And we acted as technical facilitators familiar with the problem. We have an entire security sector here that analyzes such problems and is well qualified to say: "If this port is blocked at final users' endpoint, there will be a significant reduction in spam and also in net traffic." And that is how it turned out. This was why it took so long! It took a long time. We spent years fighting this battle. So the point is this: CGI.br has a very specific role to play and has no regulatory or legislative attributes in regard to these matters. It has only a few very specific responsibilities concerning IP addresses

and domain names, distribution of domain names and distribution of ".br" domain names, and nothing more.

CAF: Port 25 process is seen as a multistakeholder process and as an experiment that could be carried out with the general public. Here we have the task of translating highly technical aspects for the general public, together with current debates on Internet governance, and it is important that multistakeholder practices like this one come to light.

CA: This is interesting in the scope of, let us say, those who define the rules for the very definition of the network. There is an open international organization called IETF – Internet Engineering Task Force – which since the beginning of the Internet, has worked based on recommendations known as "requests for comments (RFC)." Based on these RFCs, they recommend standards for the functioning of all network's aspects. IETF is what you might call a pluralist, multistakeholder organization. Anyone can join, anyone can go there to debate, anyone can offer RFCs for discussion by IETF. Depending on the circumstances, your RFC may become part of an archive of RFCs that number in the thousands. It is there that you will find the RFCs that define these standard ports, that define services and how they function as routers, how you can tell traffic from a page from e-mail traffic even when the logical port is changed. You can consult a web portal on port 8085 instead of port 80, for example, the latter of which is the Internet standard.

And so all these functional characteristics of the network are defined in a pluralistic manner by IETF (Internet Engineering Task Force) and from a technical point of view. Technical! From the point of view of routers and switches. This is an example of collaborative agreement. This is not the ITU – International Telecommunication Union issuing some regulation. This is a characteristic, so to say, it's an Internet characteristic. IETF follows the Internet standard of collaborative work. Here we do the same thing.

And in this work on port 25, we are a pluralist organization by nature: CGI.br is a committee whose nongovernmental members are elected by their communities. So we have representation. If we fail to represent our communities, that is another problem, but we do have representation. When we are working with a telephone provider or an Internet access provider, we bring such representation into the discussion. The same goes for informing

the community of this decision which fosters the blockage of a port, or encourages unbundling. This, I guess, is an important experiment that is followed in other governance models for the Internet such as those maintained by IETF.

CAF: Is the Internet in Brazil better off after having closed port 25?

CA: No doubt it is better off! Just look at the statistics produced by CERT.br on countries that send most spam. We have definitely made a huge difference, and as soon as blockage was adopted by major operators, decrease was significant. It's like an ant. The Internet is highly complex and this is one of its wonders. You cannot exterminate ants, but you can at least minimize them. And so if some guy is going to send spam from Russia or Arabia, fine, but here in Brazil, we have reached a tacit agreement that it will not pass through our territory.

CAF: Any other thoughts?

CA: Regarding this whole story of port 25, I would say: "No big deal." Some operators lobbyists are used to saying, "this is a violation of net neutrality that you are defending!" But how so? Where is the contradiction? I think I have already explained that such arguments make no sense. On the contrary, we are improving net performance with it.

5• Interview with Marcelo Bechara

São Paulo, January 24, 2014

Carlos Afonso Pereira de Souza: Could you comment on your participation in port 25 management?

MB: Although I had been a member of the Brazilian Internet Steering Committee (CGI.br) for six or seven years, I would say that my role had much more to do with my work as an ANATEL agent than as a CGI.br member. I say this because the committee was attempting, with specific groups – in which I played no part – to foster a technical debate on port 25 management. Actually, it really bothered us being in second place in spam international rankings.

I participated in the necessary dialogue between CGI.br and ANATELAt the time, I had just joined ANATEL and was still the representative of the Ministry of Communications on the steering committee. It was an interesting process: it had to be forwarded to the agency's board of directors; after that, the agency director would sign a document produced by CGI.br with companies

and, unless I am mistaken, with the state's attorney. It was in fact quite an important document, one that involved divergent actors. And so it had to be submitted to the presidency of ANATEL, and I wound up as the voice of the project inside ANATEL. This was really quite crucial and at the end of the day, it produced a fine example of collaborative work.

CAF: Talking about ANATEL, CGI.br and their competencies, could you briefly describe, in layman's terms, what were ANATEL's competencies to regulate connection providers and Norm 4? Just a brief aside before we get into the discussion of port 25.

MB: Norm 4 actually predates the founding of ANATEL itself. ANATEL was founded in 1997, the auction process took place in 1998; in 1995 we had an Ordinance that instituted Norm 4, which dealt with the relation amongst connection providers and "companies" – we still called telecoms that way then – the state-owned public telecommunication and infrastructure companies. They were called public for a very simple reason: these were state-owned companies, privatization had not yet begun and the Internet access model was all provided by dial-up modems. I would say that till a little later than 2006, 2007, there was still more dial-up than broadband in Brazil. This only changed with mobile broadband, and obviously dial-up connections, as I remember the numbers, went down to only 10% of the total, and with a downward trend, which we hope will continue.

What, then, was ANATEL's role? ANATEL's role, when it took charge of regulating the telecommunication sector, was to be responsible for telecommunication infrastructure, where the Internet resides. It was also assigned to deal with network functioning. They have a program there that says, "value-added service, or what some call value-aggregated, is not a telecommunication service," which means to say: "That is ANATEL, don't mess with that."

However, the item that defines value-added service reads that the relation between value-added services providers and telecommunication services providers must be managed by ANATEL. And so the regulatory environment is not very clear, and it is understandable that it not very clear, because the modification of the regulatory environment from 1995 to the present has been considerable, especially when it concerns the limits of ANATEL's powers.

With respect to this type of issue, there was a specific regulation

– "Regulation of Multimedia Communication Service" – that providers, the established mainstream connectivity providers, ended up following. The result was that even today they are defined as both value-added services providers and telecommunication services providers. Sometimes one same company within a single corporate structure. There are more than 4,000 providers today.

The very issue of net neutrality is already covered by the multimedia communication service regulation as an unspecific value. And why unspecific? Because it is expected that the legislature will deal with the issue and that there will be no conflict between ANATEL regulation and the decision of the legislature, with which ANATEL will have to comply.

CAF: Let us leave net neutrality for a little later on. Returning to the telecommunication companies' role, could you speak about the relationship between telecoms and CERT.br? How did this relationship between telecoms and security incident reports develop?

MB: I don't know, but if there is going to be communication, it may not be due to an ANATEL initiative, but rather by CERT.br itself or the companies. What was ANATEL's role in this whole process? Was it for administering and managing port 25? If telecommunication services providers' participation was not needed, and they were both owners of the infrastructure and responsible for data communication, ANATEL would not be part of this agreement. So, why is ANATEL there?

For one simple reason: the telecoms are regulated by us, are administered by us, and this is quite clear, including in the agreement. That is to say, when ANATEL and the telecoms sign, this is what happens in the universe of these two actors: "If you fail to comply, I, the regulator, can take administrative action to compel you to comply, up to and including fines." And so this is an idea that not only further legitimates the proposal but that also enforces an obligation to comply, a duty to perform on the part of the telecoms. This I believe was the role of ANATEL.

In issues related more to the field of security, the very usability of the Internet, ANATEL remains quite timid in relation to its own actions because it harbors certain doubts. The Marco Civil casts doubt on ANATEL's role, for example. I often say that there is no power vacuum. Port 25 is an example, a positive one, of the absence of a power vacuum. Why? We had a real problem because of the ac-

tions of foreigners, because our machines were being considered as zombie machines. That is, most Brazilian users did not know they were being used as instruments for disseminating and proliferating spam traffic. But Brazil was in an extremely uncomfortable position. This had been proved. There were damages on navigability, on the economy and most people disliked living with this; the adoption of software, this not efficient. Port 25 proved to be extremely effective. CGI.br realized that in order to make it happen, it had to appeal to the federal Public Prosecutor's Office and to the very users; consumers and final users should have a more sophisticated vision of consumer's rights on the Internet. They should know that their rights were being denied every time they received any unsolicited message or advertisement that kept repeating to exhaustion even without any authorization on their part.

How do you articulate this model? And who is in charge? No one is in charge. Not a single person. Generally, when nobody takes responsibility, the Public Prosecutor's Office (MP) acts. But the actions of this body use tools that require a slower process: they pass through the courts, for example. So how could we solve it all? We gathered a bit of each and then it worked, it started to be effective. Since its adoption two or three years ago, we have plummeted in the blacklist of spammers, and thank God we are no longer in a position which left Brazil with such a terrible image in the international community.

CAF: As to the process itself, what do you think made it last so long? Because this is a frequent criticism to this initiative.

MB: Nothing did. Even routine processes with preexisting implementation standards may be extremely slow. That's the bureaucratic machine. In ANATEL's case, I can tell you that we have a public consultation mechanism which passes through our legal counsel and follows normal legal channels. Things are also slow in the Brazilian Internet Steering Committee (CGI.br). I am part of that process, and I can tell you this: It's slow! But why? I think that port 25 was the first time that CGI.br acted more like a steering committee and less like an information center (NIC.br), which has a life of its own taking care of IP addresses and domain names; things that CGI.br does not get involved in. It has a hierarchical relation with CGI.br, but in operational terms, NIC.br has a life of its own from the point of view of its processes.

The Steering Committee, on the other hand, focuses more on

debates than on management. In this case, it acted as a steering committee, but this is not something that is part of its routine, as in my opinion it should be.

This has happened very gradually. Till some time ago, CGI.br resolutions were not published, not even online. Port 25 is a typical "we have to do something" case. As it might have been traumatic, due to the question of unanimity, we began like this. Thus, in itself, it would be a slow process to internally convince the steering committee how to do this, how to adopt this and still involve other actors. How to make the same case after having involved other actors? Can you imagine it? We would have to face ANATEL's legal department, then face the legal departments of CGI.br and NIC.br, then invite the Public Prosecutor's Office and Consumer Defense ... and reach a final draft. Look, I know how difficult it was to reach that final draft. Telecommunication companies were extremely exacting and wary, living up to their usual standards, and so I really believe there could have been no other way to do it and it was highly unlikely to happen quickly. What you can't lose sight of is the learning experience; that once one deals with it in a more systematic basis, one tends to find out mechanisms that will make processes move more quickly and faster.

CAF: Let us look at the telecommunication companies' role in the port 25 process. There was a heavy demand for the presence of ANATEL. Can you explain what those demands were? Why ANATEL's participation was so required? And in your evaluation, what was the importance of ANATEL's participation?

MB: Telecommunication companies are already accustomed to dealing with regulatory agencies, and so despite our open conflicts with these companies, they preferred dealing with a party whose workings they already understood. That is, they know how they could be fined, they know how it works, they know what ANATEL and its related regulatory bodies are. They preferred dealing with ANATEL to dealing with consumer protection organs, with whom they are in eternal and constant conflict. It is only natural. Those are users andservice providers. ANATEL functions more as an intermediary on behalf of users, but we are not part of the Brazilian consumer protection system, we are not a Procon. We deal with markets comprising economic agents; consumers and companies are both economic agents, and we try to promote equilibrium in this market.

In an environment in which you are dealing with consumer defense, the Public Prosecutor´s Office and CGI.br, and then, all of a sudden, companies are urged to take part, they imagine "How are we going to take responsibility for network management issues when the agency that regulates us – including our network functionality – is ANATEL?" So I guess that ANATEL enters the process as a facilitator to make it viable, as a bridge, and to legitimate the telecommunication providers and even the final users' participation. Not that final users needed it. They never need it because they already have legitimacy and their own representation, but with the Public Prosecutor´s Office's at their side, it was more guaranteed. But I believe that, even for users, ANATEL's presence also added legitimacy because they counted with the presence of an institution formed, inclusively, by a superintendence dedicated to users, with its own specific processes and the power to sanction or to do whatever else might be necessary.

CAF: Once port 25 was implemented, did you hear of any feedback from ANATEL or from the telecoms regarding improvements in broadband quality?

MB: I believe so. Obviously, we have a group that deals exclusively with broadband, both mobile and fixed. Various elements are taken into consideration by this group; not least that it is a group formed by the agency itself, together with companies and experts. Tools were developed for gauging quality of service. I have no doubt that elements such as spam interfere greatly, because they end up overloading the network, with serious effects. And so I believe that yes, we must have some level of information. I don't know if relating specifically to the port itself or perhaps as information on the system as a whole.

CAF: During the port 25 management process, some companies alleged that the process would be costly. How was this issue solved? How could this question be approached in the debate, and how was it decided that it was important to do so even facing some costs?

MB: Companies' arguments about costs are the same they use in every case. That is, they oppose to each and every measure to improve service quality, whether it impacts investments or not, because sometimes you do not really need all those investments. Sometimes you can take steps that have a much greater effect on the quality of service than on the issue of investments needed to accomplish such steps.

Sincerely, I don't know whether they really needed to invest so much. I think they do not, but they always use costs as arguments.

ANATEL has done a very good thing – one that did not exist at that time because its internal regulation was not the one in force today – by ensuring that wide-ranging measures be presented with analyses of regulatory impact. I don't know if that would be the case, because it was not a regulation, but rather an agreement, but even if a Regulatory Impact Assessment RIA – (AIR – Análise de Impacto Regulatório) could be performed, what would it prove?

What is an RIA? It is a regulatory cost-benefit analysis. I believe that in this case you don't need to be an economist to verify that the benefit was truly extraordinary. Then, even if costs and investments had been required, I think it is part of their and our business to wish things to function properly. To me, it has been treated naturally and normally, once we are used to dealing with it.

CAF: And how do you connect debates on port 25 to the ones on net neutrality?

MB: I have my own peculiar point of view on the net neutrality issue. Quite peculiar, in fact. I see the importance of neutrality, how everyone favors it. You will not find a single person who would say, "I am against net neutrality." Net neutrality is a principle, a value, and I think there has never been any questioning about it, any support for non-neutrality.

Now, defining what neutrality means is what makes debates more interesting. This is a concept that has evolved. These days, I believe that some are defining as matters of net neutrality things that have nothing to do with it. For example: to me, packages' speed and capacity do not refer to net neutrality. If I have a package for which I pay more for increased capacity, this is a matter of my profile as a consumer, not net neutrality. In my view, net neutrality presupposes network management, regardless of my speed or capacity. I may have the best broadband in the world, with unlimited capacity, if such a thing existed. Yet, I could find my network being degraded so that I can't have access to a certain type of information. To me, this is net neutrality.

I guess that port 25 management makes perfect sense within the context of net neutrality. Why? For good or ill, you are creating mechanisms to block or impair access to undesirable content, but it's still content. At this point we have to bring up the concept of

spam content quality. But this is out of the question, otherwise I will be able to say that some contents have priority over others.

I think port 25 is a fine example of the fact that not all content is equal and that not all content should necessarily receive the same treatment. The Internet does it by itself. You have some applications that are deterministic, some that require a greater effort. For example, two seconds, three seconds make a difference to a Skype conversation, whereas a delay of three or four seconds in the arrival of an e-mail doesn't have the same impact – if it has any impact at all.

Then again, my fear regarding net neutrality is that the Marco Civil, rather than focusing on preservation of net neutrality, might try to advance into the area of technological concepts. Technology, you see, has a dynamic all its own, let alone the Internet. We are entering an era that I no longer call the "Internet of things" but rather "The Internet of everything." What is the Internet of everything? My refrigerator will be connected to the Internet, but will it be required to show the same respect for neutrality than telemedicine? I sincerely don't know! But my refrigerator is still there, a machine connected to another machine, and I only interact with it by programming the fridge; I am not navigating. And we are heading toward this Internet of things, or the Internet of everything.

So, as to the discussions on net neutrality, I am afraid the question is: If the Marco Civil had been issued before our port 25 agreement, would it had been possible for us to make such agreement? This question needs to be answered. Honestly? I don't know whether we would have made it, because it would depend, there still is a vacuum, a vacuum remains. It is better to assign either CGI.br, or ANATEL, or the Presidency of the Republic, it doesn't matter who would be in charge, because someone has to be in charge of the issue, or else we will have to face a gap like the ones we've already faced before. And perhaps we will not be capable of reproducing the same solution, no matter how slowly, next time.

So I think this debate really matters and that other important measures like this one should be taken up; and that CGI.br should work more as a manager of the Internet, especially in regards to whatever the net mostly needs.

CAF: Any final thoughts on technical or political aspects of this process?

MB: On political aspects – particularly because I would not dare to talk about technical aspects after you have interviewed so many

renowned experts. I think that from the political point of view, it is obvious to say that we learned a lot, surely, but we learned that it is politically possible. This learning process proved to us that there is a way to make it possible: a task force, of multistakeholder in nature or not; it doesn't matter.

A task force may sometimes have a multistakeholder character, and, depending on its objectives, it might not. But it is not impossible to find a way to make decisions that lead to workable solutions. And it has to be done. Speaking for ANATEL, which I represent, it is no accident that ANATEL has a seat in CGI.br, a representative there. This makes sense, a perfect sense: you need to have an interaction that is not confined to debates, but that also considers the operational point of view in order to effectively do things. Because this is politics – and politics is dialogue; it presupposes dialogue in an environment in which competence is only vaguely defined. I hope we can use this model as a way of maturing a political debate that has assumed, in my opinion, the status of a silent revolution. We were not out banging our drums during the port 25 negotiations. Once the agreement was signed, it was openly and broadly divulged. I think this was the best example of how to proceed: to work in silence – not without transparency, but in silence – which is a different way of making things happen, particularly because the topic was highly technical and some 99% of Brazilian Internet users wouldn't have any idea about what port 25 is or does. But there is no doubt that it is making a difference in everyone's lives when they use the Internet.

6. Interview with Eduardo Parajo

São Paulo, January 24, 2014

Carlos Affonso Pereira de Souza: Can you explain what port 25 is?

EP: I'll try to explain it in simple terms. Port 25 is the port that would be used, without management, by your e-mail client to send a message to another person on the Internet. The problem is that clients' software and e-mail servers would both use this port to send mail. Clients' machines started, then, to be abused by spammers that transformed such computers into mini-servers, very often without the users' knowledge. We ended up drowning by spam being sent from Brazilian computers to the rest of the world.

CAF: What was the effect of this infestation on Brazilian machines?

EP: That had devastating effects on the Internet in Brazil. Firstly, spammers' capture of users' machines worked the machines' processing capacity and bandwidth capacity to exhaustion because it kept sending e-mails over and over again. Users might have noticed how extremely slow their access to the Internet had been.

Sometimes they would blame either the machine, or the software, or his connection provider. At the end of the day, someone else was using all their resources in their place. So this was the primary effect that I would say was devastating to users.

The second effect, which is quite delicate, was that the Brazil's global reputation for Internet quality and security was severely damaged. Brazil appeared on a list of major global spammers; then, many Brazilian IP addresses began to appear on these blacklists, with severe consequences; and finally, from the moment these IPs or series of IP addresses began to appear on spammers blacklists, various e-mail servers from all over the world started blocking messages coming from Brazil. There were other even more radical reactions: there was a time, for example, that Europe blocked all incoming e-mail from Brazil to any European server. That was when work began on setting up the port 25 management project.

CAF: Can you explain this process?

EP: Confronted with all these facts and the abuse of end users' machines in Brazil, CGI.br initiated a working group to look for a way to minimize these issues.

From the start, there was a highly technical issue to address: how to modify the way users sent e-mail, the port users sent messages from. This was not a Brazilian invention; there had been a Request for Comments (RFC) proposing the creation of a port called 587, which is heavily used. The group created by CGI.br was joined by various protagonists of the national Internet, ranging from access providers, major backbone operators, and major e-mail service providers, who began to meet in order to raise general awareness about the need to change some configuration in the servers and in the clients' e-mail software.

So it was a long, time-consuming process, but its final objective was the following: to prevent users from having their machines captured by spammers to be transformed into e-mail servers to send spam on the Internet.

CAF: What agents were invited to join the port 25 management project?

EP: Basically the access providers and the telecoms operators that host users. Why them? A joint effort along three axes was needed. The first concerned the major e-mail servers, which needed to alter the RFC in order to send and receive e-mail through port 587 and not port 25. A second aspect involving these same

providers was to inform the new configuration to users, and that e-mails should be sent by the new configuration. You also have another characteristic of access providers, which provide Internet connection to users. They were the ones who generally interacted with users, and therefore were supposed to tell their clients: "Look, we are proceeding to a security adjustment, an important modification that you will have to make to your e-mail client." And finally, there were telecom operators who provided users with a connection and had to migrate the majority of them to the new port, to physically block this port for the specific benefit of the residential endpoint class of customers. I mean to say, even though malware had infested the machine and continued sending to port 25, there would be a physical blockage of ort 25 to prevent this mail from being forwarded.

And so you had this gathering of players representing providers, telecoms, and e-mail servers that was fundamental for notifying and educating users. Obviously, we also involved ANATEL in the process because telecom operators were afraid of carrying out the blockage of port 25. We also involved consumer defense groups in the project. The completion of this project involved a great deal of effort on the part of all these players.

CAF: This project took some time to be implemented. What do you attribute this delay in concluding the process to?

EP: I truly think there were several factors. We had, for example, telecom operators blocking the port, and users who were not prepared for that, so that call centers' traffic volume increased. The same can be said regarding the e-mail and Internet connection providers. It took a lot of time, I would say, for this group, and for the operators especially, to raise awareness about the importance of the change. Among providers, both ISPs and e-mail providers, awareness had already been raised and work was underway. But you have to remember you were dealing with millions of e-mail users. I will give you an example: one of the players has more than 10 million e-mail accounts. How would it communicate with all of them? You would find yourself quoting the old saying: "Which came first: the chicken or the egg?" Who would act first? And so, when the major e-mail and connection providers began to take their first steps, the operators began to move as well. I think an important consideration for operators was the fact of us having

agreed on a communication channel linking this group and their representatives, including here at CGI.br. It was at this point that the process began to flow.

CAF: To what extent do you believe it was important for this process to have a multistakeholder characteristic? Could it have been successfully implemented otherwise?

EP: No way. I think the Internet as a whole is a multistakeholder process. It does not depend on one single segment, and no single segment will solve all its problems. Each segment may have an idea, but it won't be put to practice without the help of others. And so this multistakeholder process is highly necessary.

The Internet is a collaborative environment. There is a basic structure provided by telecom operators, but its functioning presupposes interaction and things don't move forward without interaction. From users to major operators, major e-mail and connection providers, to the commercial departments: without an effective interaction, the process cannot succeed.

CAF: One of the content-related issues raised by port 25 is how this process relates to net neutrality. Can you comment briefly on the closing of port 25 and net neutrality?

EP: I think the one has nothing to do with the other. My position is very clear and the group had always taken great care since the beginning to explain that such a process would not interfere with net neutrality.

The truth is that our group's work was a technical recommendation regarding an issue of security on the Internet in Brazil. We have never spoken about discriminating e-mails from one person, because they are slower, or from another person, because they are faster. Then, there was no interference with the neutrality process. I know that some say there is. Perhaps the focus of your question is whether blocking port 25 would be effectively influenced by debates on neutrality. If you pick up a copy of the CGI.br Decalogue, you'll see that port 25 management has contradicted none of them at any time, because the Decalogue states that it is not recommended to block, filter, or monitor the net traffic for commercial, cultural, religious, or any other reasons. Port 25 management has not violated the Decalogue in any way. On the contrary! Furthermore, it was a decision that emerged from a participative process, involving all society in the discussion. The very

cornerstone of the Internet is the principle of collaboration, not the individualism of a single sector alone.

CAF: Considering the Marco Civil and the closing of port 25, would the latter be suitable for an eventual net neutrality clause?

EP: Let us separate the Marco Civil from net neutrality. The issue of neutrality in particular is that no one wants any discrimination or prioritization of data traffic. I think this is one of the basic principles we defend regarding neutrality: that there be no filters, blockages, or prioritization related to business, political or religious interests. We have to do away with them to preserve the neutrality process. I guess it also applies to the Marco Civil. No matter what text is approved, I think it ought to be inspired by the CGI.br Decalogue rather than create a new nomenclature for what is now called network neutrality. I think the steering committee chose its Decalogue's words very wisely, including the way it defined net neutrality. I think that the Marco Civil or any bill project ought to extract this text and enshrine this principle in the law's text.

CAF: And speaking of the port 25 process, what lessons can be learned from its multistakeholder model that could be applied to future initiatives?

EP: It is a process beset by deadline issues. It's a kind of process we begin without ever knowing when it would be over. This is one lesson we learned from this process. It took five, six years to implement. And I can give you another example of something happening right now: the three years it has taken to implement IPv6. In Brazil, things tend to happen in the last second before time is up. We should learn this lesson so next time it might not go this way again. The players involved in this process pushed back hard; it was not a simple process.

For example, the port 25 group thought long and hard about the communication process between users and providers, which really is a complicated matter, because some users understand what you are doing, but some others have no clue about anything. So I think that port 25 management has taught us not to spend so much time on similar processes yet to come.

I think we'll have an enormous amount of work next April or May, after we run out of IPv4 new connections, a process currently underway. I think we cannot be extremely radical, not to allow things to happen without supervision. But we must also not let the process be continually postponed. I think this is the

essential lesson, that we must first unite the parties and then try to complete the process as quickly as possible.

CAF: So were the results of port 25 management positive?

EP: I remember the last time Ilooked, we were ranked thirtieth on a well-known international list of spammers. I believe this experience was extremely positive for the quality of the Brazilian Internet. You can imagine millions and millions of users infected, using 100% of their capacity, at the same time, to forward spam to addresses outside Brazil. This is an absurd cost for users to bear, a cost that Internet-related companies must carry on their books.

Unfortunately, we cannot measure such cost in monetary terms, which would make it easier to apply an objective, parallel measure to economic impact. Some companies, for example – mainly the major operators – had all of their IP blocks blacklisted. Now imagine the damages to those users who could not send e-mail to various locations. It would be an interesting study, perhaps, to try to measure the financial cost or quantity of resources abused in this manner.

7 • Interview with Rubens Kuhl

São Paulo, January 24, 2014

Carlos Affonso Pereira de Souza: Could you explain what port 25 is?

RK: Port 25 is used for communication between Internet e-mail servers. When a user submits an e-mail to the Internet, he doesn't necessarily need to use port 25. After this message is submitted, the server which the message was submitted to uses port 25 to deliver the message to its destination.

CAF: And what is the importance of blocking port 25?

RK: Port 25 had been abused by people seeking to deliver undesired e-mails. Those people then would make the users' machines, without their knowledge, deliver unsolicited e-mails in a way that the actual responsible for such a nefarious attitude could not be identified .

CAF: How can a machine's vulnerability be exploited?

RK: This vulnerability is exploited by sending an e-mail message from that machine that is to be delivered to the e-mail server it normally uses to forward mail to other addresses.

CAF: What were the effects of port 25 blockage?

RK: Brazil, once ranked amongst the countries which the largest volume of unsolicited e-mail was generated from, fell several positions in the blacklist figures: dozens of positions onto a much more comfortable one; a more compatible position, let us say, with our internal processes.

CAF: What was your participation in the port 25 process?

RK: Cristine Hoepers, Klaus Steding-Jensen, and I were the first to propose this. They were working at CERT.br and I had recently left a job at a major e-mail provider. And we all noticed how difficult it had become to send e-mail because Brazil had a reputation as a leading transmitter of spam.

CAF: How do you connect debates on net neutrality and port 25?

RK: Port 25 is linked to net neutrality because, from a technical point of view, port 25 is a violation of neutrality. According to some regulatory drafts, not yet approved, there are good reasons for violating technical neutrality of the net. One objective that interests all parties, here in Brazil, is to earn the confidence of the global Internet.

CAF: Returning to the port 25 process itself, how do you see the role played by CGI.br in the whole process?

RK: CGI.br played a fundamental role in the port 25 management project because CGI.br was the only environment in which all interested parties – users, telecoms and access and e-mail providers – could meet, debate and come to conclusions as to whether or not to implement port 25 management. Any attitude taken by the executive branch of government would have been viewed as an intrusion by the public administration on the prerogatives of the market and its players. And so this decision was taken within the context of a multistakeholder environment in which all involved actors were represented enabling a much more spontaneous and effective alignment with the initiative.

CAF: Was closing port 25 the best solution?

RK: Closing port 25 was the best solution for the problem of our declining credibility. It had already been adopted by major networks in other countries. Unfortunately, we took a long time to adopt it, but it was the best, and possibly the only, practice for combating spam. Other issues, such as network reliability, we still have to address, but for the reliability of e-mail delivery it was the only way out.

CAF: How do you compare the Brazilian experience with the experience of other countries?

RK: The Brazilian experiment wound up repeating the experience of the major North American networks, such as Comcast, which managed to remarkably diminish the volume of customers' complaints and improve e-mail delivery reliability after having implemented this reconfiguration. In the Brazilian case, however, you had a more serious problem: Brazil was classified as a nation, and as a result, blocks of address lists from Brazilian ISPs began to appear on the blacklists. The U.S. did not face this kind of disruption. No one was going around blocking all e-mail servers in the country. But Brazil was facing that risk. As a result, this type of initiative was beneficial not only to the networks that implemented it, but to Brazilian networks in general.

CAF: Any further thoughts on this project, in its technical or political aspects?

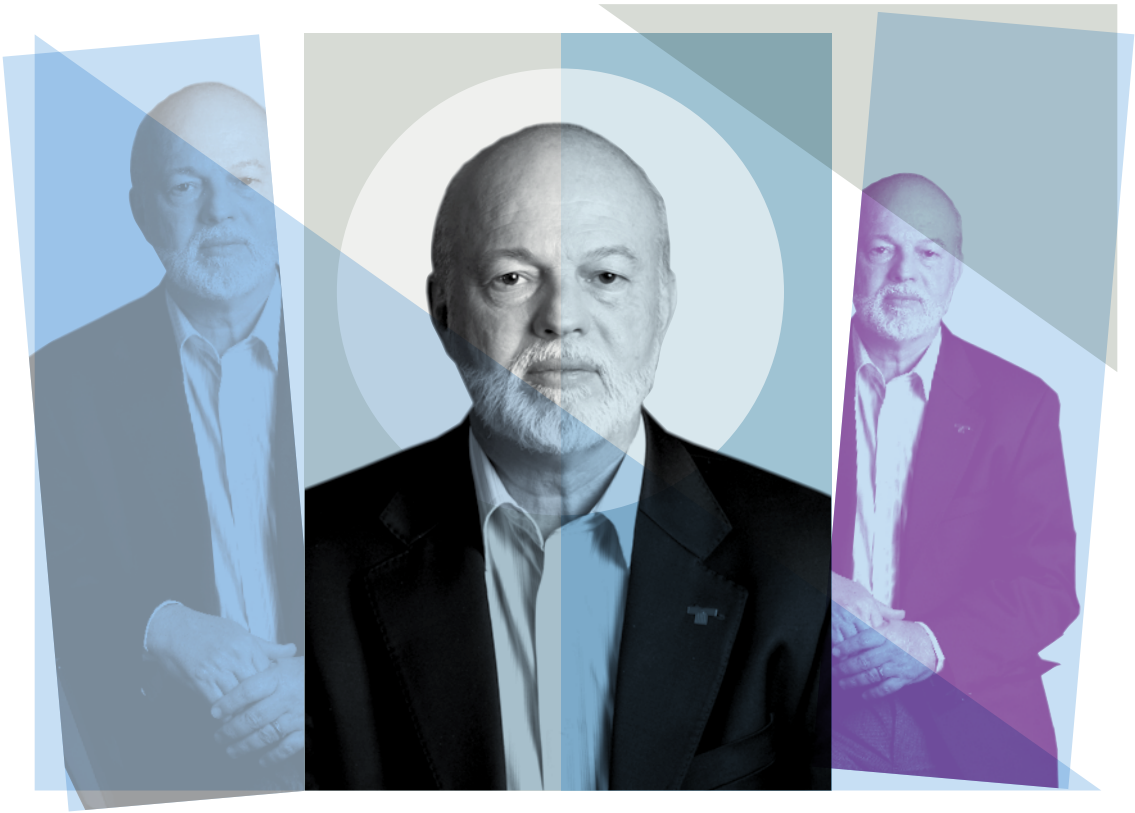
RK: Port 25 management implementation was effective, but it took much longer than it might have taken. I think it was a lesson, for the parties involved, that it is possible at times to expedite certain initiatives, so long as their objectives are clear. Even so, certain players kept postponing its technical implementation. So this project stands as a lesson for the next time we have to implement political processes.

CAF: But is this not inherent in a multistakeholder approach?

RK: It is inherent to the multistakeholder process that it takes a bit more time. What we need is to speed up the process. It will continue as a process that involves extensive debates, but such processes could take less time than this one did.

CAF: If you were to balance the duration of a multistakeholder process that seems to take too long and the achievement of expected results, are the results of a multistakeholder process necessarily better?

RK: The results of a multistakeholder process will always be perceived as superior, because it is backed by the participation of all the players involved. And so regardless of whether it is better or worse, it will always be looked on more positively. This is an advantage from a political viewpoint: that is, this port 25 project constituted a learning process in which participants learned that defending merely one specific point or insisting on an adjustment according to their own needs will only slow the process – an indicator of our political maturity in making such a decision.



8. Interview with Eduardo Levy

São Paulo, January 24, 2014

Carlos Affonso Pereira de Souza: How do your duties at CGI.br relate to the process of port 25/TCP management?

EL: I think it is important to begin with a summary of my history at CGI.br. Not just my own, but the history of the telecommunications sector. The process of electing members to CGI.br had never drawn much interest from the telecom sector, so much so that the sector never had representation on the Committee. The lack of representation was a loose thread, in that this work was already being performed in brilliant fashion by Henrique Faulhaber, whom I did not know. Actually, I only knew Professor Glaser from past association, and I only became aware of the brilliant work he was doing when, following the election in which the telecom sector selected a representative for the first time at CGI.br. I participated in a meeting at which, as I remember very clearly, we received a presentation by Henrique in which he reported the progress

made in the port 25 project, saying that of all the issues, perhaps the most important was to make a strong effort to involve the telecom sector in a general way.

I was not familiar with the process. My life was not the telecom sector; it did not involve port 25 and questions like that. I listened, reflected and concluded, "I might not have understood it correctly, because this project seems so obviously necessary." As a fresh member, however, I decided to study the issue better in order to define a position for the next meeting. That was the time when this process began for the telecom sector, and perhaps this was a demonstration that this sector should have permanent representation on the committee, given its importance not just regarding port 25, but for the Internet issues in general.

I talked again with people who were more familiar with the situation and heard how they were going to bait a hook with to address net neutrality as well. The questions were "Why?" and "What were the major reactions to this initiative?" One logical reaction regarding what we had agreed to do with ANATEL and what we had agreed to do with the Procons was: "You will take away specific clients' freedom to use a port they already have on their own computers? Procons may field complaints, saying you are limiting some freedom. And if you are taking freedom away, the Procons can complain and sue companies and ANATEL. ANATEL, on the other hand, may also find that we are acting in an unauthorized manner and we could be fined for interfering with a civil liberty."

This argument was somewhat logical, but there existed a broader understanding that was much easier for us to bear. We could stop, reflect and then say: "Any means offered to serve society must serve the public, and not be served by the public. Since port 25 management undeniably benefits society as a whole, we must work towards it and eliminate obstacles."

As to my role, I am not going to say that it was the easiest job, because the greatest efforts were made by participants in the group coordinated by Faulhaber. It was left up to me, however, to convince the companies, a work which resulted in the signing of a formal document amongst them all. We held an ample meeting to which I brought more lawyers than technical people because the lawyers wanted to be sure, not about the technical process, which was not their specialty, but that their clients would not be

sued tomorrow for having allowed the sector to sign a document that could give way to numerous future fines. So this was complicated. From the point of view of democracy, and observing the various forces working together, it was a beautiful sight, especially because society benefited the most. Nothing was strong enough to prevent society for benefiting from such process. So, I guess that, to me as a person, as well as to the whole telecom sector, we felt greatly proud to be a part of such process, to be capable of spreading it the way we did it, and to be able to see Brazil removed from all the global spam blacklists.

To me, there would have been no way to reach this agreement, not because of the persons involved, but because the telecom sector was not represented in such meetings.

I think that the issue of net neutrality follows the same logic: it is society that should benefit from the resources placed at its disposal. And so, when we speak of net neutrality, it is like saying you root for the most popular team of all: no one disagrees (laughter). Are you for or against net neutrality? I can't imagine anyone in the whole world who could advocate being against neutrality in the sense that the network cannot be allowed to interfere with anything I want to do online. But it is also a resource placed at society's disposal. And closing port 25 took away from a set of users their ability to use a resource they had the right to use. At that moment, as I see it, the net was not neutral, but something existed above that, which was the benefit to society. Traffic passing through that port had to be removed, or prevented from entering, because in principle it is not a real user that is making use of it. So let's start from the principle that your machine is running and you have no idea that at that moment it is consuming bandwidth and generating spam. This is probably because your machine has been inoculated with a virus that is consuming bandwidth. For this reason we entered into agreement with the Ministry of Justice and ANATEL, even though in theory we were taking away some freedom. The fact is that it is not the person who is doing this; it is a third party who is acting in bad faith, using bandwidth for purposes other than those intended. And so, by blocking this activity, you are acting in the benefit of society.

Still, this is a good example of how similar cases – or cases that might arise in the future, demanding an intervention in the network – can be developed in a way that benefits society as a whole.

This explains the telecommunication sector concerns about the existence of a rigid law. We appreciate the CGI.br Decalogue very much, but we often perceive that there can be a dichotomy between what we preach about the net being as simple and as free for every user, while creating a law that could have consequences that undermined such freedom.

I understand perfectly that the group that most actively deals with the Internet objects to excessive regulation. I do too, and the telecom sector is tightly regulated by ANATEL. Because society is meant to benefit, companies cannot be allowed to act without regulation. But the Internet possesses a much greater degree of freedom. Diminishing this degree of freedom by means of Congress legislation may work against what is preached about Internet freedom.

I can also understand perfectly well that just as the telecom sector is regulated, we must prevent abuses by parties with a great deal of economic power. For this purposes, however, we have CADE – Administrative Council for Economic Defense, the competition regulator, and ANATEL's regulations that apply to us. From this point of view, I believe freedom would be better served if we simply adhered to the Decalogue in force today on the Internet in Brazil, which serves as an example to the world.

CAF: I would like to know your opinion about the importance of the Steering Committee in this process. How do you see CGI.br role in the port 25 management and how will this affect future actions, given that despite the extensive discussion of multistakeholder governance, there are few practices and positive evidence that can be presented to international forums?

EL: I have my criticisms as well. I think CGI.br role was fundamental from the multistakeholder point of view and the participation of all interested parties. But if some branches had been missing, we would have probably gotten nowhere. The telecoms sector was absent from the debates. Its participation could have been more or less important; depending on the moment, it could have had a greater or a lesser importance. Discussions at CGI.br are enormously rich, due to the characteristics of the market segments involved. The only problem I see concerns a certain lack of balance between investors and consumers. CGI.br comprises a large majority of broadband consumers, but it possesses only one representative of investors. In a sector that depends so deeply on massive investments, it is important to bear in mind who is going

to pay for lunch. In this case, lunch cannot be paid for by those who lead and dominate the discussion, but they should be an active and important voice, because they are, after all, paying for lunch. Do they receive something in return? They do. But there must be some balance. Just as it happens in the case of our regulations – and we have a lot of experience with ANATEL, which always takes into account the economic balance of those running the business.

When ANATEL issues regulation, mainly for concessions of services, it takes into account the social advantages, but also the situation of the party that will have to invest in it and to profit enough to live on. You cannot operate with deficits, because there is no way for you to exist; but you cannot exploit society by posting fantastically large earnings. Therefore, the agency focuses on balance.

From where I stand, based on my three years of attending the monthly meetings, I never took part in a single discussion in which someone might have remembered: "Who is going to pay for it? Who is going to invest in it?" or "Who is earning too many profits? Is the citizen being exploited?" Balance: this is one of the things that I lack in debates here because it involves extraordinary investments in the Brazilian network.

9. Interview with Danilo Doneda

Brasília, September 27, 2013

Marília de Aguiar Monteiro: Could you describe your current duties at Senacon – Brazilian National Consumer Protection Secretariat and how they relate to the port 25 management activities?

DD: I am the general coordinator to studies and market monitoring at the Brazilian National Consumer Protection Secretariat, Senacon. In my work I deal with topics related to e-commerce, communications and the Internet. We produce research, regulatory analyses, and impact analysis, and from time to time, we contribute to public policies related to the defense of the consumer in those areas.

During the CT-Spam anti-spam project, I kept parallel track of the project and participated specifically in the agreement that was to lead to the implementation of port 25 management with the involvement of consumer advocates. Some agreement signatories, such as telecom companies and their trade associations, insisted that a major obstacle might be consumers' complaints about port 25 management in case they were affected.

Given that this problem had not been technically evaluated in the beginning, and especially because it was a problem of a legal nature, CT-Spam sought out the consumer defense agencies and we were called on to give recommendation on whether the port 25 project was viable or not, and to verify potential impacts on consumers; to check on whether or not there actually was something to fear. It was at that moment that we got acquainted with all the work being done by CT-Spam, all the technical issues and related engineering aspects of implementing the port 25 management.

This was in 2010, I think. It was before I started here at Senacon. There was, to be honest, a problem of mutual technical incomprehension about what it was all about. It was a completely new universe for all of us. Consumer defense has a chronic problem precisely because it covers all markets, all consumption-related situations. Here, however, it faced certain technical data the meaning of which was not entirely obvious even to specialists in the area; there was a significant learning curve to be navigated from the very start. I know this because I heard stories about when this issue first arrived at Senacon, before I started here.

In August 2011, when I came to work here, the question was resumed and we were invited to a Committee meeting, or more specifically to a CT-Spam meeting, which as I recall counted on the presence of various government agents: ANATEL, MDIC – Ministry of Development, Industry and Foreign Trade and CGI.br itself, along with telecom companies. It was at this meeting that we learned the technical details of the problem and what response we were being asked to provide, that is, whether port 25 management could be a problem for consumers or not.

CT-Spam and CERT.br placed themselves entirely at the board's disposal for answering any questions of this nature. An important meeting was held here at Senacon, which was still a department at the time. If I am not mistaken, it was in 2011 that Henrique Faulhaber, Cristine and Klaus, from CERT.br, were working to provide a technical explanation about port 25 management and its implementation. At the same time, senior officials of the national department of consumer defense participated.

This question was to be technically examined by the general coordination, which was competent to assess the matter and to

verify whether the process would benefit consumers even though it might bring some minor problems – about which information was needed. If that was verified according to CT-Spam's report, we would inform the National Consumer Defense System, formed by Procons, that they would register customers' complaints in the event that consumers had difficulties with this process.

It was decided that we would analyze the issue and inform the consumer defense departments of our results. In the following months, we studied it and prepared a Technical Note on the subject. The Technical Note explained the nature of spam, a problem that afflicts consumers in terms either of discomfort, loss of time or loss of privacy. So much so that the consumer is induced to pay, with time or money, to use services that would be simpler and cheaper, and less vulnerable to spam attacks from the network. We found that there would be a sound benefit for users if Brazil could significantly reduce spam traffic on its Internet.

Coming to this conclusion was made considerably easier by the fact that I had participated personally in a study commissioned by CGI.br and the Getúlio Vargas Foundation Center for Technology and Society (CTS-FGV) in Rio de Janeiro. The study directly addressed combating spam, its perspectives, and a provisional draft for a piece of legislation. I remember that my part in such study led me to a clear conclusion, which I would later publish as a single-author paper, about the existing legal instruments being incapable of significantly reducing spam for several reasons. It was not only that the agents directly involved with spam fail to respect the line defining civility or legitimacy, or even the rule of law. Spamming, because of its peculiar low-cost cost structure, is not something that could be inhibited by legal, formal enforcement: it would need a legal approach to be complemented by a technical approach and even by an economic one.

Based on our accumulated experience and our verification of port 25 management results, we decided to issue a Technical Note reflecting our conclusion that also encompassed the possibility of some users, some consumers having problems: especially those using older equipment, non-classical terminals as computers or tablets for medical use, private equipment with obsolete standards for Internet connection that might still be in use. Those could be affected in some cases by our port 25 management.

Thus, the Technical Note sought to inform Procons around Brazil that there might be complaints along these lines, and that they should check whether the Internet connection problem would have something to do with port 25 management. If that was the case, they should turn to the agents, at CERT.br or other agents I don't recall at the moment, who participated in preparing the Note, and who would help solving the problem or even contact the operator, the access provider. If there was a legitimate reason for those consumers to keep using port 25, it should be reopened for them.

Today, based on the information we have had since port 25 management and the issuing of our Technical Note, absolutely no complaints have come to our attention at Senacon. From time to time, problems arose on a retail scale and were reported to the Procons. I have heard of such cases, but I cannot tell you whether they were claims or complaints. There are no figures on this and, as far as I know, no problems have become specific complaints or any disputes involving consumers and providers over the blockage of port 25.

In that sense, we assess our actions throughout the entire process in the hope that it was useful in dispelling concerns that this measure would have an opposite effect, harmful to consumers, and capable of blocking or impeding an implementation which, in our view, has offered consumers countless benefits.

MM: Prior to port 25 management implementation, had any complaints about spam been received by the National Consumer Defense System?

DD: It is not natural for users to complain of Internet spam to a Procon office. This is a problem we had been monitoring. We had and continue to have a different vision, that it is harmful to the development of the Internet or to Internet consumers. But this is the type of problem that appears in a systemic analysis, rather than in any data analysis from Procon. People go to Procons because they have a problem that affects them directly, that prevents them from buying something, that deprives them of the use and enjoyment of services; in short, because of something that directly affects their wallets in a sound and incisive way.

The spam problem is a chronic misery that affects many people but it's not the sort of problem that makes people leave the comfort of their homes to visit a Procon. Thus, our analysis was not influenced by any complaints about spam Procon had received.

We developed our market analysis using other indicators in order to analyze the market more specifically, to study aspects of its functioning that would have authorized Senacon to intervene even if the consumer was not directly affected.

MM: During the preparation of the Technical Note, did you identify and disregard any harm to consumers?

DD: Disregard? Well, any identified potential risks were considered in the light of those using out-of-date e-mail technology, as well as people who would use systems connected to the Internet which were not computers per se and which might use port 25 to communicate. At this point, these consumers could encounter problems. On the other hand, a market analysis also reveals that the number of such consumers is entirely marginal in relation to the mass of consumers who do not use this port. What are we to say about this? That the number of consumers who could have problems was considerably smaller than the global mass of users that would, indeed, benefit by the measure. Furthermore, the few harmed consumers would be those who, after being alerted to the problem, would have time to remedy the situation with their ISP, or by contacting a consumer defense agency. Our Technical Note tried to clarify doubts on the matter, so that consumers could be informed in a timely manner that possible problems due to port 25 management were not connection problems nor caused by any problems in service quality or continuity, but rather a specific incident, "artificially created by a new Internet architecture," that could be solved as it effectively was. We maintain contact with CGI.br and through it we receive news of operators who have opened port 25 for consumers who complained, establishing that the numbers of such requests were practically insignificant regarding the number of cases reported. Since the beginning of the blockage, we, here at Senacon, have received no direct complaints about the switch. We've just heard of complaints from operators who have identified the problem and corrected it for the consumer.

MM: What about possible violations of consumer rights? Have you identified any potential risks?

DD: Now look, the Consumer Defense Code (CDC) contains an article that is often left behind or brushed aside, which sets forth that consumer defense has to adapt and to keep up with techno-

logical development. It was precisely this article that provided the foundation for our Technical Note in the sense that it permitted us to execute this technical change, the management of port 25. Even though it might affect a small number of consumers, it was essential for the creation of a more favorable environment for all users. Possible damages to users, who would, in fact, not be harmed at all because they would be able to reverse the situation, were, to be honest with you, a problem easily offset by the benefits that blockage of port 25 would offer to consumers in general.

MM: Were the educational and awareness-raising activities carried out by CT-Spam effective? Were they noticed by the consumer defense agencies or not?

DD: The only indicator I would have to assess that would be if we had received some complaints or a comment about our educational material. There were none. And since our first contact with CT-Spam, one of the things we stressed hardest and insisted on as a fundamental principle was the need for someone to support our educational efforts, someone to clarify our doubts, in case some problem arose, because we had made it clear that, given the broad scope of our activity, it would be impossible for us to know any details concerning the specific functioning of the network. And from the beginning, CT-Spam proved itself available and, I dare to say, even happy to contribute to a project that was so close to us, in our DNA: the raising of awareness, the production of educational materials, and so on. Such material came to our knowledge, and we sent it to some Procons. Perhaps the most responsive Procon may well have been São Paulo's branch, which would certainly concentrate the largest number of people, of Internet users, maybe of dedicated, specialized services users, and who might have faced some kind of problem as well. As far as I know, that was how it happened and, as I said, the only metric we would have would be the good faith of consumer complaints. And so, in our point of view, CT-Spam's support was a complete success.

MM: The process of port 25 management implementation was considered long and slow. Can it be said that the involvement of other government agencies, such as the Ministry of Justice, ANATEL and, as you mentioned, others parties, could have postponed the process?

DD: In the final analysis, it is not for us to say. What it looked like

to us was as follows: in many cases, people speak on the consumer's behalf inappropriately. I noticed that in our meeting with CT-Spam. In any case, our analysis was that consumers' specific problems were purely marginal, and reality clearly showed this. To date, we have heard of no major complaint or problem that was not easily remedied. Our actions, I hope, and I will be very happy if it proves to be true, were successful in helping exorcize some witches, some ghosts, who whisper that some consumers should be protected in a way that could prevent the achievement of major gains for all consumers.

Maybe one of the first actions I witnessed here, at Senacon, which could exhibit some maturity in the sense of facing problems not only as issues demanding to be addressed, but as matters for assessments regarding the benefits they would offer. In this sense, we are doing nothing more than performing a risk analysis that is fully compatible with the Consumer Defense Code (CDC).

CAF: Was the port 25 experiment a violation of net neutrality? How do you evaluate this issue?

DD: Well, net neutrality is not an absolute value in the sense that it should serve some ontological purpose. Net neutrality is, in our view, to privilege the Internet and communications, without posing any interference to freedom of expression, to the free flow of information and consent. Because technical management measures proven to magnify freedom of expression, access to knowledge and free communication, cannot really be characterized as a way of violating net neutrality, but rather as exceptions to it, carefully implemented and studied: exceptions that reinforce the character of the core of net neutrality. In this regard, the Marco Civil is fully consistent with other legal defenses of neutrality throughout the world – in the sense that it does not mistake neutrality as a term to be viewed in absolute terms, leaving aside the technical management necessary for the entire Internet to do its work. In sum: the function it was created for, a free and open means of communication for all participants.

MM: And what about privacy?

DD: Do you mean privacy related to port 25 management? Senacon has not identified any privacy-related problem directly linked to the management of port 25. Any problem would be a devel-

opment occurring in a different spectrum, and Senacon has not identified any such cases.

CAF: One of the reasons for this project is to understand port 25 management as a multistakeholder experiment here in Brazil. How do you, as an invited member of the government, view port 25 as a multistakeholder initiative? How do you assess the participation of the other actors in this process?

DD: Personally, I could have arrived at the formula myself, but institutionally, Senacon had very little experience with multistakeholder governance. Nevertheless, as I told Marilia, Senacon faced it since before I started here, even before I joined the Ministry. Senacon first viewed it as an invitation from a public agency without considering it as having a sophisticated nature, out of a belief that the very agency in charge of its implementation already contained all divergent poles. Everyone was represented. Then, within this pot of multistakeholder representation, we attended our first meeting with CT-Spam, and it became clearly visible that there was a divergence of opinion that could be channeled through the positions taken by one or more of us.

We verified that our position in the Technical Note, which was extremely technical by the normal standards of Senacon, was that of a Technical Note that, as we saw it – and were happy to see it that way – could help orient any possible conclusions by CT-Spam.

In parentheses, I would add that down to the present day, my speech is regarded as incomprehensible by the staff of some of the Procons. It all began on the day I lectured to 150 Procons and the consumer defense office on port 25 management. Some representatives would not have looked more stunned if a Martian had come down to Earth than to listening to my speech on SMTP and port 25, consumers' rights, and so on. But significantly, no one complained, Procon teams got the gist of my message and still consider it a satisfactory protocol.

CAF: Considering the consumer who is technically less prepared in these relations, how do you view the role of Senacon as a mediator in such technical issues?

DD: Generally speaking, when the consumer relation exhibits such a technical complexity, involving decisions on what choice to make, the best option to buy, we enter the scene as regulators, to perform

our role as a "substitute consumer." That is, we act as an entity that will technically translate the terms of the problem bearing in mind the interests of the consumer by offering decision-making support. In this sense, as I said before, port 25 management is a little more modern once it includes deep-rooted regulatory principles. In the process of us acting as a "substitute consumer," we try to anticipate the risks in a situation in which the consumers themselves wouldn't have the technical knowledge to keep up with the learning curve. So what have we done? We have functioned as a final user, not only for the sake of the real final user, but also in the coordination of customer defense agencies, who face the noble task of engaging with consumers over the counter on a daily basis and who, for this very reason, find it enormously difficult to do research on themes as nearly esoteric as this one.

10. Interview with Jaime Wagner

By telephone, March 11, 2014

Carlos Affonso Pereira de Souza: What are your recollections about port 25 management at CT-Spam?

JW: The Regulatory Code of Practice for email Marketing emerged as a by-product of the work developed by the CGI.br Anti-spam Committee. During my time on the Steering Committee, CT-Spam developed two important activities: the management of port 25 and the drafting of an email marketing self-regulation code.

Regarding port 25 management, it is important to emphasize that it all began with the so-called hdoneypots initiative, developed by the CERT.br staff. It was the conclusions based on data collected by honeypots that led to the development of a technical basis for subsequent activities. To date, these activities concerned eminently technical issues involving dialogue amongst technical experts.

When I started at CGI.br in 2008, the CERT.br team was ready to "abandon ship" with respect to port 25. Why was that? It

seemed clear to me that some of the telephone operators opposed moving ahead with the project. In the meetings we held, we were under the impression that the initiative would not move forward.

Then I suggested to Henrique Faulhaber, the CT-Spam coordinator, a strategy of inviting the executives of the telecoms into the meetings, instead of just inviting technical experts, as well as trying to attract the industrial associations rather than individual companies. The strategy to date had been to maintain an open dialogue amongst technicians, but the process was bogged down in arguments such as that port 25 management was going to take a lot of work and, because of that, it would be better not to go on with it.

Checkmate was achieved at the moment the corporate executives began to attend the meetings and to understand the issues beyond their technical aspects. In the end, what Henrique and I decided to do was to attend the meetings, where I spoke my mind freely while Henrique would take a more conciliatory tone. It ended up working.

I used to say that I didn't want to talk to the technical representatives, but to the executives. I said I wanted to talk to people who would decide, and not to people who were idle in their work. My argument was: "Are you incapable of seeing that the costs this will generate for the companies is nothing compared to the loss of bandwidth the current situation is causing?" In the end, the companies were augmenting their capacity, but some of the bandwidth was being thrown away. "Just show it to the shareholders" – I would say. As a matter of fact, I am a Telefônica shareholder, for example. My point was that this work would enable revenue growth.

In addition to this change in debating tactics, we also tried to bring in representative entities. Here we ran into a problem, however, namely the degree of representation that the industry associations found in their representatives to CGI.br. At this point, telecoms had no direct representative to CGI.br. This seat was occupied by someone more related to the pay TV market.

Things only began to really move forward when we succeeded in overcoming the technical barrier and the representative of the paid TV sector at CGI.br was removed, his seat taken by Eduardo Levy. When I left CGI.br, as I remember it, Levy embraced the process and brought it to a satisfactory conclusion. Without him we would never have achieved our goal.

At first, Eduardo also showed some resistance, but he later realized that the management of port 25 was the best measure to take. He saw that the situation, at that time, generated nothing but "poor savings". From the companies' point of view, adhering to the technicians' arguments led to "poor savings" ...

There were in fact two obstacles in our talks with telecoms. The first came from the technicians and the second from the lawyers. You know how lawyers are, right? Always saying we cannot do this or that. And it was the lawyers who were attending the meetings and contributing to the impasse. When Levy took charge of the board, he solved the situation.

We had managed to make a good deal of progress, but from the political point of view, without Levy's participation, it would have been complicated, or at least would not have been implemented with the same speed.

CAF: What about the email marketing self-regulation?

JW: Elaborating the code was the second most important task that CT-Spam developed during my time at CGI.br, and it involved mobilizing companies to work for a common cause.

I always say that there are various kinds of spam. One of them I call "bandit spam," the type of spam we were combating with the ort 25 management. The other is a "naive spam," which dresses itself up as marketing. It consists of the person who buys a database and sends e-mails to everyone in the world, with the best of intentions and with the goal of increasing sales. This is the case with various small business owners who view this as a cheap form of marketing. The merchant has a legitimate interest, but he winds up as a spammer.

In the final analysis, the naive spammer is shooting himself in the foot because the reputation of his company suffers. He winds up with a positive return of one percent and the rest is negative. This is the profile of the naive spammer.

What is it we sought to accomplish? We brought in companies engaged in serious email marketing to discuss a Code of Self-Regulation. At the time, there were a number of anti-spam bills being debated in the national congress, some of which proposed making spamming a crime. CGI.br itself was involved in the debate and was working on a draft bill that took care of the spam problem by legislative means. Some of these bills were extremely odd, and CGI.br was working to explain to the congressmen what the tech-

nical implications of adopting one or another definition would be. Even so, there was no consensus, because CGI.br had not yet consulted with the community affected by this regulation, which was the entire body of companies sending this type of communication. The number of companies making a living from this service was growing, back in 2008 and 2009. It was a promising sector, one that might die out at the hands of bad legislation, which would make life difficult for newborn companies of the type that make up this market, this generation of youth coming together.

So what happened next? I was reading an e-mail addressed to CGI.br from someone who criticized our work at CT-Spam. I called him and his colleagues in to talk and we were able to come up with a solution that didn't require legal enforcement. All it would take would be a consensus among all the actors involved in this line of business.

Rather than seeking to define spam, as the bills in Congress do, we have opted to define what legitimate email marketing is, and then discard everything that does not match those criteria and subject it to an eventual anti-spamming law. For one thing, defining spam is a very difficult and challenging task.

And so we worked on the rules of this self-regulatory code for about a year before obtaining the approval of everyone involved. We were represented in the conversations of user rights groups, mail forwarders, providers, even the Association of Brazilian Internet Providers - Abranet. When we got to the point of writing down the code, we saw that much more than a mere code was needed, because the code had to be effective.

If the code were not effective, it would be dead-letter law, with no agency to promote it. To succeed, self-regulation needs to be monitored, and prove that it is working. We created a new agency along the lines of the National Council of Advertisement Self-Regulation – Conar (Conselho Nacional de Autorregulamentação Publicitária), which took its name from the Code itself. This was the origin of the Regulating Code of Practice for email Marketing – Capem (Código de Autorregulamentação do e-mail Marketing), whose by-laws contained a series of rules that effectively drove the application of the Code.

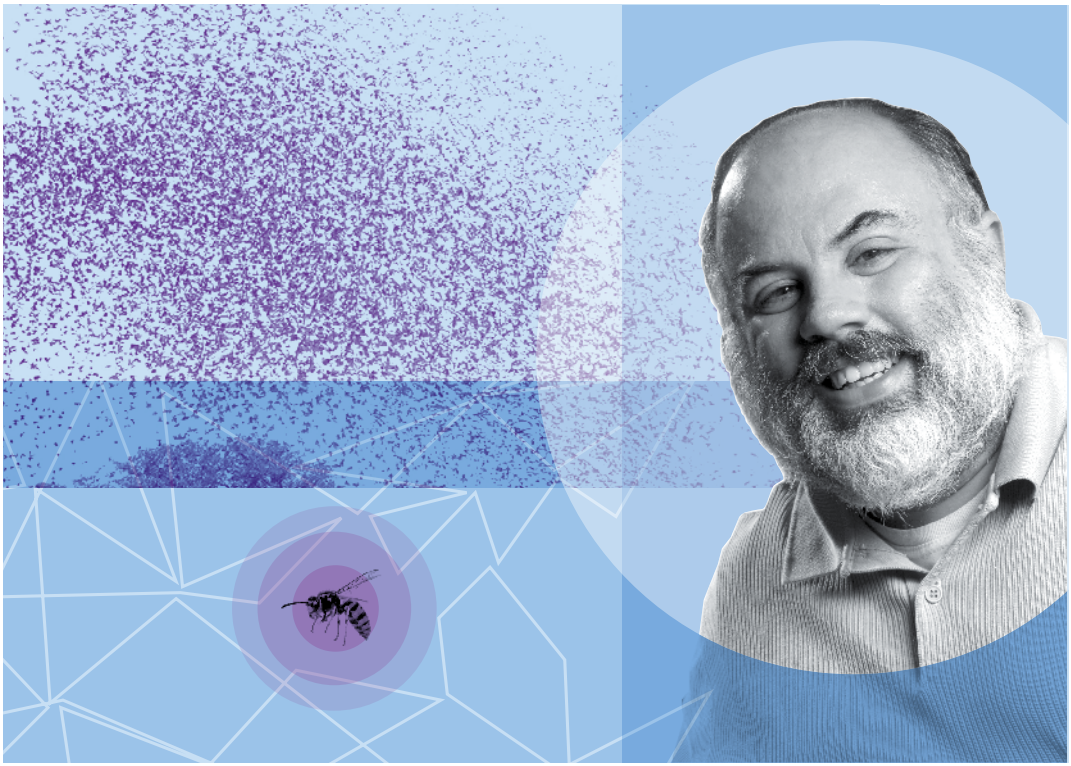
Capem was a simpler version of Conar, with fewer layers of appeals and an automated process that distributed the cases and supported the judge's ruling. We worked on this for one more year,

and when I left CGI.br, the organization was already in place. Because I was not re-elected, I wound up backing away from the project knowing that it was not mine to develop, but belonged to whoever represented the sector in CGI.br.

When I left, the major question was how the entity would be financed and maintained. At that point, we had a code of conduct and a legal identity. My idea at that point was to organize the mess stemming from the spam debate; I even created a Brazilian blacklist whose process was more closely regulated than other blacklists around the world. As you know, these private blacklists have technical criteria for including a name or address, but the removal of a name from the list is an eminently political matter: it's a matter of who knows who can be called on to remove the name from the list, as though you were working in a notary office.

Around this time, I wrote an article about the various types of spam, and this helped us in our work and in our efforts to define exactly what professional email marketing was. A major communication group, for example, took part in Capem meetings and based on our discussions refrained from selling its database. It then began proposing that it could send its messages to its clients, but would not sell the database as a whole.

These were some of the interesting effects of what CT-Spam was doing, as I observed from my point of view as a CGI.br member. Most interesting of all was the port 25 management process and email marketing self-regulation.



11. Interview with Marcelo Fernandes

Via telephone, February 1, 2014

Carlos Affonso Pereira de Souza: Could you describe how you became involved in the port 25 management project?

MF: In 2005 Henrique Falhauber , Klaus Steding-Jessen and I attended an Organisation for Economic Co-operation and Development - OCDE meeting in Geneva that dealt with the problem of spam. We were representing CGI.br and our mission was to present Brazil's position on combating spam. When we arrived, we were approached by a representative of SpamHauss who told us he would "love to kill the Brazilians, and especially you, who are producing all this trash on the Internet." In the course of our conversation it became clear that spam was more than just a national problem for Brazil, but also affected other nations and parties, who were feeling the effects of messages originating from Brazil. Oddly, in the same meeting, we noticed that even though we were inside OCDE and connected to an official network, we were unable to send e-mails.

Klaus quickly discovered that the reason for this was that they were using port 587 to send mail, so that we could not send messages with our current configuration. This trivial incident had the effect of awakening our desire to advance the debate on spam in Brazil and increase the involvement of CGI.br in this area. The first step we took was to create the Anti-Spam Task Force (CT-Spam).

At first, however, no one wanted to stick their hand in this wasp's nest. It took a lot of convincing and research to understand what would be the best measure to adopt and then organize the activities needed to reverse the situation of Brazilian machines as slaves to mass spammers. It was a debate in which it took us five or six years before positive results could be felt, enabling us to reach the level attained some time ago by the U.S. and Europe, in which residential connections were no longer allowed to send e-mails via port 25.

The focus of activity at the outset was to identify what was really going on: were we serving as "mules" or were we simply serving as a launch point for spam e-mails? It was at this point that the port 25 management project began to take shape.

My role in this story begins with the meeting in Geneva and with my attendance as an aide to the CERT.br team in an initiative that, in my opinion, has been one of the most victorious examples of network management in Brazil: the SpamPots project. This project played a crucial role in that it showed clearly that the measures being taken for fighting spam were not as effective as we would like them to be, and it pointed us in a different direction leading us to the issue of port 25 management. The SpamPots initiative led to academic studies on the impact of this research and how important it was for us to see what had to be done. It was clear that if we did not involve ourselves immediately in the port 25 management with support from operators, we would be fried. Google was already using port 587 and Brazil was not.

At this stage my contribution was to gather data to identify our problem, indicate routes that could be taken, and based on these activities, implement the application selected, in this case, port 25 management. It was at that point that meetings with the operators, conversations with the Ministry of Justice and the Procons, and the confusion you already know about, all began.

CAF: Were you at the meetings that took place after the decision to implement port 25?

MF: It was only in the first two or three meetings with third parties that we acted as agents of port 25 management implementation, because at this point I was dedicating myself more to the SpamPots. Negotiating with the operators was assigned to Henrique Faulhaber, and soon after Jaime Wagner joined the debate over the proposed self-regulatory body for e-mail marketing.

CAF: Could you describe in a bit more detail how this SpamPots project came about?

MF: When we got back from Geneva, we were all preoccupied with these allegations against Brazil, such as the conversation we had with the guy from SpamHauss, along with this confusion over blacklists and graylists and the like. This had to end. To accomplish this, however, you had to understand who was sending such spam, where from and where to. We had a few ideas, some clues, but I can honestly say that at that point we were still in a speculative phase, lacking as we did hard data that would support our suspicions that Brazilian machines were being abused by machines sending messages whose final destination was not Brazil.

In a conversation with the folks at CERT.br, we came to the conclusion that the time had come to prove that the impression the world was forming about Brazil was unfounded and untrue. Next, we developed a prototype server and installed instances of it on various network endpoints in Brazil, including both corporate and residential connections. Next, we sat down to listen. This service announced itself on the network as a server with all of its logical ports open to whomever came along. We very rapidly began to see, from the very first day, that these servers began receiving traffic on their ports, in a test to see which of them were working. The software we had developed had a peculiarity, however: it told potential spammers that their message was being delivered in the normal way, but this was not true. And so, based on this confirmation issued to the party seeking to exploit the server, we began to see heavy volume. In two or three months we had to upgrade our storage, so vast was the volume of data involved. The volume was so absurd that even though it consisted of plain text, it overflowed our storage capacity.

And so the question that remained for us in evaluating this test was: How do we show this to the world? It was then that we contracted a team of data mining experts from the Federal Universi-

ty of Minas Gerais, based on our contacts with Rogério Santana. CERT.br prepared a list of everything we wanted to know about these e-mails: "Where did they come from?", "What was their language?", "Who was sending them?" We selected all these topics, and others, such as whether they were "phishing," and then data mining commenced. We downloaded terabytes upon terabytes showing that the Brazilian network, because it was open to port 25, was attractive to the global network of spammers. Spammers were talented at avoiding obstacles to the sending of its messages. The Brazilian net was a perfect foil: its users were not accustomed to security updates and upgrades, antivirus was not in general use, and reasonably sufficient bandwidth was available to these endpoints. But all of this blew up as a result of our intense exploration of the national network. The spampots showed this clearly.

CAF: And how did you communicate this finding?

MF: I think my first presentation on the topic showed how we were suffering attacks from users located outside Brazil and that the management of port 25 could be the solution; this was presented to OCDE. It was interesting to see how this discovery by Brazil ended up generating interest from other countries. Klaus, for example, went to Qatar and installed spam pots there. Other countries that were learning from us had exactly the same problem and were being abused by the same networks of spammers. We then began to design a strategy based on this information. Our work received international exposure and we wound up signing a dozen agreements or so with other countries and telecom corporations for use of the technology. It was interesting to see that some of these parties were precisely the same that had accused Brazil of being one of the major sources of spam, worldwide.

With the initiatives taken following our presentation, involving government and other agents, along with civil society, the Procons and the diverse actors of the private sector, the result was that Brazil was removed from the blacklists of countries sending out the most spam. We fell ten or fifteen places because we had begun to make the lives of spammers more difficult. Some of the data from the spam-bots are public and can be consulted by anyone. Today, we no longer have any sensors deployed, but UFMG deserves the laurels for its close collaboration with CGI.br as a whole. I am very proud of that initiative.

CAF: Do you recall any resistance to the port 25 management initiative?

MF: The decision that it would be the best path to take had already been made. Telecoms put up some resistance in that they didn't want to implement it right away, because they feared lawsuits from consumers alleging that their contracts had been violated. This debate would hold the project back five years. ANATEL, although it supported the initiative, wound up not issuing a regulation because it viewed this as an Internet-related matter and had nothing to do with the telecoms. Looking back, it is clear that this was one of the most complex problems, in terms of the coordination of multiple parties that CGI.br had ever undertaken.

CAF: What lessons can you derive from this project?

MF: We can learn a number of lessons from the port 25 management initiative. The first is to understand that once a problem is detected, it is more important to produce data that may show you the best way to proceed: time is too important to waste speculating or referring to the international indices. With the results we now have, it can no longer be said that Brazil is a country that floods the world with spam. Secondly, it is important to determine as quickly as possible what the responsibilities of team members will be, and who will take charge of them. You have to abandon a scenario full of glamour and romance in order to understand that only education could resolve the issue. The user will understand, but only if those who manage a critical public resource assume their respective duties within the framework of the project. Third, I believe that carrying out internal planning makes all the difference, with goals and objectives, taking into account that, as vital as the initiative is, it will not last forever. That is why we cannot sit idly by waiting for something to happen. And finally, the time it took to implement the management of port 25 was not exactly what was hoped for and expected, if only because, as you have heard from the other respondents, facilitating collaboration amongst all parties, with their specific interests, is far from a simple task.

nic.br