UNIVERSIDADE DE BRASÍLIA
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE
CENTRO DE ESTUDOS EM REGULAÇÃO DE MERCADOS
CENTRO DE INVESTIGAÇÃO EM ECONOMIA E FINANÇAS

SÉRGIO ANTÔNIO GARCIA ALVES JÚNIOR

POLÍTICAS NACIONAIS DE SEGURANÇA CIBERNÉTICA
O Regulador das Telecomunicações
– Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT) –

BRASÍLIA
2011

SÉRGIO ANTÔNIO GARCIA ALVES JÚNIOR

POLÍTICAS NACIONAIS DE SEGURANÇA CIBERNÉTICA
O Regulador das Telecomunicações
– Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT) –

Dissertação apresentada ao Programa de Pós-Graduação em Regulação e Gestão de Negócios (REGEN) da Faculdade de Economia, Administração e Contabilidade (FACE) da Universidade de Brasília (UnB), como requisito parcial à obtenção do grau de Mestre.

Área de Concentração: Regulação
Orientador: Prof. Dr. Paulo César Coutinho

BRASÍLIA
2011

O candidato foi considerado aprovado pela Banca Examinadora.

_____

Prof. Dr. Paulo César Coutinho (Departamento de Economia – ECO/UnB, orientador)

_____

Prof. Dr. Marcus Faro de Castro (Faculdade de Direito – FD/UnB)

_____

Profª. Drª. Claudia Canongia (Gabinete de Segurança Institucional – GSI/PR)

Brasília, junho de 2011

À família e a amizade.

À tolerância.

"O que foi tornará a ser, o que foi feito se fará novamente;
não há nada novo debaixo do sol.
Haverá algo de que se possa dizer: 'Veja! Isto é novo!'?
Não! Já existiu há muito tempo; bem antes da nossa época."

(Eclesiastes, 1:9-10)

RESUMO

Com a massificação do uso de tecnologias da informação e comunicação (TICs), em particular o acesso à Internet, a Sociedade da Informação passa a depender da segurança das infraestruturas críticas e da disponibilidade, integralidade e confiabilidade das informações que a sustentam. À medida que cresce essa dependência, ameaças ao ciberespaço se tornam ameaças à própria Sociedade da Informação. Nesse contexto, o mundo desperta para a "Segurança Cibernética". Parte-se da premissa que o regulador de telecomunicações teria papel destacado nesses esforços, vez que o setor disponibiliza grande parte da infraestrutura e serviços subjacentes à Internet. Este trabalho buscou identificar o papel da Agência Nacional de Telecomunicações (Anatel) em uma política brasileira de segurança cibernética, utilizando como modelos (i) melhores práticas divulgadas pela União Internacional de Telecomunicações (UIT, agência especializada da ONU) e (ii) projetos da *Federal Communications Commission* (FCC, regulador estadunidense). Seguindo as respectivas políticas gerais de segurança cibernética enunciadas (i) pela Cúpula Mundial sobre a Sociedade da Informação (CMSI) e Conferência de Plenipotenciários 2010 (PP-10), para a UIT, e (ii) pela Casa Branca, para os EUA, ambas as instituições promovem a atuação significativa do regulador. Na UIT, várias soluções encontradas por outros reguladores indicam margem para sua atuação, mormente como assessor técnico no desenvolvimento das políticas nacionais de segurança cibernética, com foco na qualidade dos serviços prestados ao consumidor e cooperação com o setor privado, que pode desenvolver e adotar padrões seguros; nos EUA, as respostas às consultas públicas da FCC sobre (i) resiliência das redes de banda larga, (ii) impacto de um regime de certificação voluntária de segurança cibernética e (iii) eventual plano (*roadmap*) de segurança cibernética para a FCC, sugerem cautela na atuação do regulador, que deve analisar o impacto regulatório, evitar duplicação de esforços e promover parcerias público-privadas. No Brasil, nota-se a ausência formal de Ministério das Comunicações e Anatel na formulação da Política Nacional de Segurança Cibernética nascente, considerando discurso do Presidente da República, que, em 2009, clamou pela intensificação de atividades de segurança cibernética na UIT (foro sob competência da Anatel, conforme Lei Geral de Telecomunicações). Com mandato mais claro, seja como protagonista na atividade regulatória direta (na proteção de infraestrutura crítica e imposição de padrões técnicos) ou como contribuinte eventual (no combate ao crime cibernético e na formulação da estratégia nacional de segurança cibernética), recomenda-se a atuação da Anatel e a coordenação/cooperação com outros *stakeholders* nacionais, em particular, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e o Grupo Técnico de Segurança Cibernética (GT SEG CIBER). Com isso, acredita-se que a Agência poderia promover o combate ao spam e *botnets*, proteção de infraestruturas críticas, resposta a incidentes de segurança, pesquisa e desenvolvimento, alinhamento de posições do País na UIT e demais foros internacionais de telecomunicações.

Palavras-chave: Sociedade da Informação; segurança cibernética; infraestruturas críticas; políticas nacionais; Anatel; UIT; FCC.

ABSTRACT

With the widespread use of information and communication technologies (ICTs), particularly Internet access, the Information Society becomes dependent on the security of critical infrastructure and the availability, integrity and reliability of information that support it. As this dependency grows, threats to cyberspace become threats against the Information Society. In this context, the world awakens to the theme "Cybersecurity". The text assumes that the telecommunications regulator would have a prominent role in these efforts, since the sector provides much of the infrastructure and services underlying the Internet. This study sought to identify the role of the National Telecommunications Agency (Anatel) in a Brazilian policy on cybersecurity, using as models (i) best practices published by the International Telecommunication Union (ITU, a specialized UN agency) and (ii) projects by the Federal Communications Commission (FCC, the United States' regulator). Following general policies for cybersecurity announced respectively by (i) the World Summit on the Information Society (WSIS) and the Plenipotentiary Conference 2010 (PP-10), to the ITU, and by (ii) the White House, to the USA, both institutions promote meaningful roles for the regulator. At ITU, a number of solutions found by other regulators indicate room for their attributions, particularly as technical advisors in the development of national cybersecurity policies, with focus on consumer-oriented quality of services and cooperation with the private sector, which can develop and adopt security standards; in the USA, responses to FCC's public consultations on (i) the resilience of broadband networks, (ii) the impact of a voluntary cybersecurity certification program and (iii) a cybersecurity roadmap, suggest caution to the regulator, who shall consider regulatory impact analysis, avoid duplication of efforts and promote public-private partnerships. In Brazil, it was noticed the formal absence of the Ministry of Communications and Anatel in the formulation of the emerging National Cybersecurity Policy, considering the President Lula's speech, in 2009, when he called for the intensification of ITU's cybersecurity activities (a forum under Anatel's competence, according to the General Telecommunications Law). With a clearer mandate, whether as a protagonist for direct regulatory activity (in protecting critical infrastructure and determining the adoption of technical standards) or as a sporadic contributor (in combating cybercrime and formulating the national strategy for cybersecurity), it is recommended Anatel's action and coordination/cooperation with other national stakeholders, in particular, the Institutional Security Office of the Presidency of the Republic (GSI/PR) and the Working Group on Cybersecurity (GT SEG CIBER). Thus, the Agency could facilitate the combat against spam and botnets, the protection of critical infrastructures, the handling of computer security incident response, the promotion of research and development initiatives, the alignment of Brazil's positioning before the ITU and other international telecommunications fora.

Keywords: Information Society; cybersecurity; critical infrastructures; national policies; Anatel; ITU; FCC.

SUMÁRIO

Lista de abreviaturas e siglas

AGU – Advocacia-Geral da União

Anatel – Agência Nacional de Telecomunicações

BM – Banco Mundial

CBC – Comissões Brasileiras de Comunicações

CGSI – Comitê Gestor da Segurança da Informação

CIA – *Central Intelligence Agency*

CMSI – Cúpula Mundial da Sociedade da Inforamação

CNCI – *Comprehensive National Cybersecurity Initiative*

CPI – Comissão Parlamentar de Inquérito

CREDEN – Câmara de Relações Exteriores e Defesa Nacional

DDoS – *distributed denial of service*

DHS – *Department of Homeland Security*

DNS – *Domain Name System*

DNSSEC – *Domain Name System Security Extensions*

DoD – *Department of Defense*

DoE – *Department of Energy*

DoJ – *Departament of Justice*

DoS – *Denial of service*

END – Estratégia Nacional de Defesa

ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

EUA – Estados Unidos da América

FCC – *Federal Communications Commission*

FIRST – *Forum of Incident Response and Security Teams*

FTC – *Federal Trade Commission*

Funttel – Fundo para o Desenvolvimento Tecnológico das Telecomunicações

GSI/PR – Gabinete de Segurança Institucional da Presidência da República

GSR – *Global Symposium for Regulators*

GT SEG CIBER – Grupo Técnico de Segurança Cibernética

GTSIC – Grupo Técnico de Segurança de Infraestruturas Críticas

GTSIC–Telecom – Grupo Técnico de Segurança de Infraestruturas Críticas de Telecomunicações

GTSICI – Grupo de Trabalho de Segurança de Infraestruturas Críticas da Informação

IANA – *Internet Assigned Numbers Authority*

ICANN – *Internet Corporation for Assigned Names and Numbers*

ICET-98 – Conferência Intergovernamental sobre Telecomunicações de Emergência

IEC – infraestrutura crítica

IEEE – *Institute of Electrical and Electronics Engineers*

IETF –*Internet Engineering Task Force*

IGCBP – *Internet Governance Capacity Building Program*

IGF – Fórum de Governança da Internet

ISO – *International Organization for Standardization*

ISP – Internet Service Provider

LGT – Lei Geral de Telecomunicações

MC – Ministério das Comunicações

MCT – Ministério da Ciência e Tecnologia

MDIC – Ministério do Desenvolvimento, Indústria e Comércio Exterior

MF – Ministério da Fazenda

MJ – Ministério da Justiça

MMA – Ministério do Meio Ambiente

MPOG – Ministério do Planejamento, Orçamento e Gestão

MPS – Ministério da Previdência Social

MRE – Ministério das Relações Exteriores

MS – Ministério da Saúde

NSA – *National Security Agency*

NSF – *National Science Foundation*

NSPD – *National Security Presidential Directive*

NSTC – *National Science and Technology Council*

NTIA – *National Telecommunications and Information Administration*

OCDE – Organização de Cooperação e Desenvolvimento Econômico

ONU – Organização das Nações Unidas

PGR – Plano Geral de Atualização da Regulamentação das Telecomunicações no Brasil

PIB – Produto Interno Bruto

PICT – Proteção de Infraestruturas Críticas de Telecomunicações

PNBL – Plano Nacional de Banda Larga

POSIC – Política de Segurança da Informação

PP-10 – Conferência de Plenipotenciários 2010

PPP – parceria público-privada

SAE – Secretaria de Assuntos Estratégicos

SC – Segurança Cibernética

SINDEC – Sistema Nacional de Defesa Civil

SVA – serviço de valor adicionado

TCU – Tribunal de Contas da União

TIC – Tecnologias da Informação e Comunicação

UIT – União Internacional de Telecomunicações

UIT-D – Setor de Desenvolvimento da UIT

UIT-R – Setor de Radiocomunicações da UIT

UIT-T – Setor de Normalização da UIT

USA Patriot Act – *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*

UNODC –Escritório das Nações Unidas sobre Drogas e Crime

WTSID – *World Telecommunications and Information Society Day*

INTRODUÇÃO

Com base no modelo proposto pelo curso "*Internet Governance Capacity Building Program (IGCBP)*" da organização DiploFoundation[1], optou-se por proceder a uma pesquisa política que integre o conhecimento acadêmico e teórico a aplicações práticas.

Por meio de pesquisa bibliográfica e documental, sobretudo baseada em documentos públicos disponíveis na Internet, abordou-se a temática em suas características qualitativas, com foco exploratório e reflexivo da questão. Dessa maneira, acredita-se que esta dissertação apresente resultados tangíveis úteis aos órgãos e atores interessados no tema.

Originalmente, pretendeu-se averiguar como países e organizações internacionais estão desenvolvendo e atuando em suas políticas de segurança cibernética, em particular, os reguladores do setor de telecomunicações. O objetivo seria responder à pergunta: caso haja, qual o eventual papel da Anatel em uma política nacional de segurança cibernética e em sua correspondente governança?

No entanto, na fase de pesquisa, percebeu-se que a carência de fontes e entrevistas formais sobre diversos países impossibilitaria o aprofundamento pretendido. Algumas hipóteses podem explicar a ausência de informações: (i) o tópico é afeto à segurança nacional, e, como tal, tratado em nível restrito, (ii) as barreiras linguísticas impediram encontrar informações consistentes sobre estratégias e políticas públicas e/ou (iii) os Estados simplesmente não estão atuando no tema com foco em regulação.

A solução encontrada foi restringir o registro da pesquisa a Brasil, Estados Unidos da América (EUA) e União Internacional de Telecomunicações (UIT), pelas seguintes razões:

---

[1] "IGCBP aims to assist individuals involved in Internet Governance issues from countries with limited financial and human resources to develop the skills and knowledge required to participate meaningfully in this global debate." http://www.diplomacy.edu/ig/default.asp

a) UIT: como uma Organização Internacional do Sistema das Nações Unidas (ONU) integralmente conduzida por seus Estados Membros e Membros do Setor (setor privado, institutos de pesquisa, academia), seus trabalhos refletem idealmente o consenso resultante de processo negocial. Ao analisar o histórico de atuação de seus membros, encontra-se um subterfúgio para esboçar a tendência de posicionamento de grupos cujas políticas não foram identificadas. Ademais, a UIT (seus membros e consultores contratados) tem desenvolvido diversos trabalhos técnicos e divulgado melhores práticas de segurança cibernética úteis a órgãos formuladores de políticas e reguladores de telecomunicações, consubstanciados por grandes conferências políticas internacionais;

b) EUA: é possivelmente o país que aborda tema de maneira mais transparente e incisiva, com esforços recentes de democratização da participação pública na constituição de uma estratégia nacional de segurança cibernética que geram uma miríade de apoios e críticas (também contrários a sua divulgação pública). Por meio de pesquisas na Internet, encontra-se farto material recente, incluindo as reações a projetos de lei e consultas públicas levadas a cabo pelo governo. Entre reguladores de comunicações de diversos países, a pesquisa identificou que as propostas do órgão americano (*Federal Communications Commission*/FCC) são as mais objetivas (e ousadas) de segurança cibernética como política pública para o setor de comunicações;

c) Brasil: demanda referências que facilitem o desenvolvimento de sua estratégia nacional de segurança cibernética, atividade em curso capitaneada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR). A Agência Nacional de Telecomunicações (Anatel), órgão regulador do setor, tem sido frequentemente chamada a se pronunciar no plano internacional (particularmente à UIT) e poderia ser um ator relevante no esforço de segurança cibernética também na estratégia brasileira. Maior sinergia entre a Agência e outros órgãos da Administração Pública Federal facilitaria, por exemplo, a execução de meta de curto prazo (vencido ao final de 2010) estabelecida pelo Plano Geral de Atualização da Regulamentação das Telecomunicações no Brasil (PGR), de 30 de outubro de 2008: “Realização de estudos e adoção de medidas

para a proteção da infraestrutura nacional de telecomunicações contra falhas e ataques de guerra cibernética."

Nessas linhas, optou-se pela seguinte estrutura de texto:

I. No capítulo de abertura, apresenta-se a questão e sugere-se balizar o trabalho pelos conceitos de "segurança cibernética" cunhados por GSI e UIT, citando a relevância do tema nos EUA e a proximidade entre as atividades de Anatel, FCC e UIT.

II. No capítulo seguinte, adotaram-se como modelos os casos (i) da UIT (baseado no artigo "*Cybersecurity: The Role and Responsibilities of an Effective Regulator*"[2], sobre melhores práticas e recomendações para atuação de reguladores de comunicações em segurança cibernética) e (ii) dos EUA (FCC, conforme seu Plano Nacional de Banda Larga). Procurou-se contextualizar ambas as propostas em meio às respectivas políticas gerais de segurança cibernética, conforme propagadas (i) pela Cúpula Mundial sobre a Sociedade da Informação (CMSI) e Conferência de Plenipotenciários 2010 (PP-10), para a UIT e (ii) pela Casa Branca, para os EUA.

No caso da UIT, citam-se as várias soluções encontradas por outros reguladores e sugeridas pelos autores do *paper*; no dos EUA, identificam-se as respostas às consultas públicas da FCC sobre (i) a resiliência das redes de banda larga, (ii) o impacto de um regime de certificação voluntária de segurança cibernética e (iii) um eventual plano estratégico de segurança cibernética;.

III. No capítulo final, apresentam-se, em linhas gerais, os esforços preliminares de formulação de uma política brasileira de segurança cibernética, particularmente sua governança, para, em seguida, comentá-la com base nos modelos e foco na identificação de papéis a serem desempenhados pela Anatel. Ao cabo, recomendações sobre a atuação da Agência, tanto internamente (atividades que podem ser empreendidas na instituição, no bojo da missão da Agência) quanto externamente (execução da política nacional).

---

[2] UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). *Cybersecurity: The Role and Responsibilities of an Effective Regulator*. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf

1. NOÇÕES INICIAIS SOBRE SEGURANÇA CIBERNÉTICA

1.1. Interconexão, dependência e sustentabilidade

Nos últimos quinze anos, computadores e telefones celulares móveis com conexão à Internet se tornaram bens de consumo por excelência. Devido à redução nos custos dos produtos, a criação de plataformas amigáveis, a conexão em rede, a convergência tecnológica, a rápida disseminação das tecnologias da informação e comunicação (TIC[3]), eleva-se a experiência social a um novo estágio, onde distância e identidade são cada vez menos percebidas pelo contato direto.

São cerca de dois bilhões de usuários de Internet em todo o mundo, altamente concentrados nos países desenvolvidos e centros urbanos[4] que, de maneira cada vez mais intensa, passam parcelas significativas de suas vidas online, batendo papo, trocando e-mails, realizando pesquisas, lendo notícias, escutando músicas, assistindo vídeos, interagindo em redes sociais, fazendo compras, pagando contas, procurando emprego, acessando serviços do governo, buscando pornografia, ou apenas vagando sem rumo pela web.

Tudo. Todos. Ao mesmo tempo. Em todos os lugares.

Em 2009, um estudo divulgado pelo Banco Mundial (BM) afirmou que, em países em desenvolvimento, cada 10% de incremento em penetração de banda larga acelera o crescimento do Produto Interno Bruto (PIB) em 1,38%[5]. Como este, outros indicativos de ganho de bem-estar socioeconômico decorrente do emprego massivo de TICs impõem a elaboração e execução de planos

---

[3] Para fins deste trabalho, as telecomunicações serão consideradas subconjunto das tecnologias da informação e comunicação (TICs).

[4] UIT. *Key Global Telecom Indicators for the World Telecommunication Service Sector*.Disponível em: http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html. Acesso em: 2.12.2010

[5] KIM, Yongsoo; KELLY, Tim; RAJA, Siddhartha. *Building Broadband: strategies and policies for the developing world*. http://go.worldbank.org/7EP6QCMY40.

0nacionais de banda larga como instrumento estratégico de desenvolvimento das nações.[6]

Aparentemente, as sociedades que não se integrarem à grande rede ficarão a reboque. Não parece absurdo afirmar que o mundo caminha para ser interconectado. Interconectado e dependente.

Para a subsistência do ecossistema da Internet[7], que envolve as redes de telecomunicações, os serviços, os aplicativos, os usuários, e para o sucesso dos programas de disseminação do acesso à banda larga, torna-se primordial que as infraestruturas que sustentam essa sociedade sejam seguras e que as informações necessárias estejam disponíveis, íntegras e confiáveis.[8]

À medida que cresce essa dependência, ameaças ao ciberespaço[9] se tornam ameaças à própria Sociedade da Informação:

> As ameaças reais e potenciais na esfera da segurança da informação estão entre os desafios mais sérios do século XXI. Essas ameaças podem causar danos substanciais às economias e à segurança nacional e internacional. As ameaças provêm de uma ampla gama de fontes e se manifestam em atividades disruptivas dirigidas tanto a indivíduos, empresas, infraestruturas nacionais e governos. Seus efeitos trazem risco

[6] "O Governo Federal do Brasil tem discutido com representantes de vários setores o chamado Plano (ou Programa) Nacional de Banda Larga (PNBL), em vias de ser formalmente aprovado como programa prioritário de governo. Iniciativas similares têm sido discutidas ou adotadas por diversos governos (África do Sul, Austrália, Canadá, Coréia do Sul, Espanha, Estados Unidos, Finlândia e outros). Em praticamente todos os casos, as ações contemplam forte presença do Estado como agente catalisador e até mesmo operador (como é o caso da Austrália) de componentes estratégicos dos sistemas participantes." *Cf.* AFONSO, Carlos A. FONSO, Carlos A. "Que banda larga queremos?" In: CGI.br (Comitê Gestor da Internet no Brasil). *Pesquisa sobre o uso das tecnologias da informação e da comunicação 2009*. São Paulo, 2010, pp. 65-72. http://www.cgi.br/publicacoes/artigos/artigo67.htm

[7] KIM; KELLY. *op cit.*

[8] "Multinational corporations who are seeking to do business in such countries, either by outsourcing tens of millions of dollars of work or investing hundreds of millions of dollars to build a plant locally, have to be certain that ICT-based capabilities they develop are going to be accessible and secure. This means that countries who want investment must have a rational approach to cyber security—it is becoming part of the package corporations must and will consider." IN: BRUCE, Robert *et alli*. *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues.* http://www.ists.dartmouth.edu/library/158.pdf

[9] Apesar das vicissitudes em torno do termo "ciberespaço", optou-se empregá-lo em seu sentido dicionarizado: "1. Dimensão ou domínio virtual da realidade, constituído por entidades e ações puramente informacionais; meio, conceitualmente análogo a um espaço físico, em que seres humanos, máquinas e programas computacionais interagem. 2. Restr. A Internet". Aurélio. Para análise detalhada do termo, vide FRAGOSO, S. "Espaço, ciberespaço, hiperespaço". *Textos de educação e cultura*, n. 42. UFBA, 2000. http://www.scribd.com/doc/33757586/Espaco-ciberespaco-hiperespaco

> significativo para a segurança pública, a segurança das nações e a estabilidade da comunidade internacional interconectada.[10]

Notícias frequentes veiculadas na mídia sobre episódios que ameaçariam a estabilidade do ciberespaço evidenciam o interesse público e de especialistas: mais recentemente, sobre possíveis ataque do vírus Stuxnet a infraestruturas de enriquecimento de urânio do Irã[11], vazamento de informações de inteligência pelo site Wikileaks[12], desvio de tráfego mundial da Internet pela China Telecom[13], bloqueios dos governos indiano e estadunidense às compras de

---

[10] Trecho do relatório do Grupo de Especialistas de Governo sobre os avanços no campo da informação e das telecomunicações no contexto da segurança internacional, constituído no âmbito da Assembleia-Geral da Organização das Nações Unidas (AGNU). O grupo foi estabelecido em 2009, por determinação da Resolução da AGNU 60/45, com especialistas de 15 Estados: África do Sul, Alemanha, Bielorrússia, Brasil, China, Coreia do Sul, Estados Unidos da América, Estônia, França, Índia, Israel, Itália, Qatar, Reino Unido e Irlanda do Norte, Rússia. AGNU A/65/201. O tema "avanços no campo da informação e das telecomunicações no contexto da segurança internacional" entrou na pauta da AGNU em 1998 (A/RES/53/70), após uma carta do então Primeiro-Ministro russo, Igor Ivanov, ao Secretário-Geral da ONU, Kofi Annan, em que aquele afirmava que os efeitos de armas de informação "podem ser comparáveis aos das armas de destruição em massa".

http://www.un.org/es/comun/docs/index.asp?symbol=A/65/201&referer=http://www.un.org/es/ga/documents/symbol.shtml&Lang=S. (Tradução livre)

[11] *Stuxnet worm 'targeted high-value Iranian assets'* http://www.bbc.co.uk/news/technology-11388018; *Was Stuxnet Built to Attack Iran's Nuclear Program?* http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html; *'Stuxnet virus set back Iran's nuclear program by 2 years'* http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475; *Stuxnet pode ser parte de problemas atômicos do Irã* http://exame.abril.com.br/tecnologia/noticias/stuxnet-pode-ser-parte-de-problemas-atomicos-do-ira;

[12] *WikiLeaks Releases Secret List of Critical Infrastructure Sites* http://www.wired.com/threatlevel/2010/12/critical-infrastructures-cable/; *Veja lista traduzida dos locais "vitais" para segurança dos EUA revelada pelo WikiLeaks* http://www1.folha.uol.com.br/mundo/841676-veja-lista-traduzida-dos-locais-vitais-para-seguranca-dos-eua-revelada-pelo-wikileaks.shtml; *WikiLeaks divulga locais "vitais" para segurança dos EUA; Brasil está incluso* http://www1.folha.uol.com.br/mundo/841393-wikileaks-divulga-locais-vitais-para-seguranca-dos-eua-brasil-esta-incluso.shtml; *WikiLeaks backlash: The first global cyber war has begun, claim hackers* http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war; *Sabotagem e alta espionagem são os maiores temores do mundo digital em 2011* http://veja.abril.com.br/noticia/vida-digital/sabotagem-e-alta-espionagem-sao-os-maiores-temores-do-mundo-digital-em-2011

[13] *China redirecionou tráfego da web para seus servidores, dizem EUA* http://www1.folha.uol.com.br/mundo/832324-china-redirecionou-trafego-da-web-para-seus-servidores-dizem-eua.shtml; *US accuses China Telecom of internet hijack* http://www.computerweekly.com/Articles/2010/11/18/243984/US-accuses-China-Telecom-of-internet-hijack.htm; *China Telecom Denies Hijack of Web Traffic After U.S. Report* http://www.bloomberg.com/news/2010-11-18/china-telecom-denies-hijack-of-web-traffic-after-u-s-government-report.html.

equipamentos de infraestrutura de telecomunicações das chinesas Huawei e ZTE[14], preferência nas compras da Telebrás por equipamentos nacionais[15].

Embora, por vezes, os textos soem apocalípticos ou sensacionalistas, isso não desautoriza a necessidade de esclarecimentos e pesquisa. Ao contrário, um dos desafios é identificar uma linguagem comum.

Spams[16], malwares[17], phishing[18], bots[19] e botnets[20], vírus[21], ataques de negação de serviço (DoS)[22] e ataques de negação de serviço distribuídos

---

[14] *Report: Sprint Rejected Huawei, ZTE for Security Concerns* http://www.pcworld.com/businesscenter/article/209963/report_sprint_rejected_huawei_zte_for_security_concerns.html; *India Said to Block Orders for ZTE, Huawei Technologies Telecom Equipment* http://www.bloomberg.com/news/2010-04-30/india-said-to-block-china-s-huawei-zte-from-selling-phone-network-gear.html; *Huawei, ZTE Growth to Slow on U.S., India Fears, ISuppli Says* http://www.businessweek.com/news/2010-08-24/huawei-zte-growth-to-slow-on-u-s-india-fears-isuppli-says.html; *Huawei opens UK Cyber Security Centre* http://www.mobilenewscwp.co.uk/2010/12/huawei-opens-uk-cyber-security-centre/

[15] *Telebrás decide comprar apenas equipamento local e irrita múltis* http://www.outroladodanoticia.com.br/component/content/article/2-noticias/1134-telebras-decide-comprar-apenas-equipamento-local-e-irrita-multis-.html; *Com foco na segurança nacional, Telebrás quer acesso aos códigos-fontes* http://www.teletime.com.br/30/09/2010/com-foco-na-seguranca-nacional-telebras-quer-acesso-aos-codigos-fontes/tt/200579/news.aspx; *Telebrás: Acesso aos códigos-fonte é procedimento de segurança* http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=23908&sid=10

[16] "Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do Inglês *Unsolicited Commercial E-mail*)" Cf. CERT.br. *Cartilha de Segurança para Internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2006. http://cartilha.cert.br/glossario/#s

[17] "Do Inglês *Malicious software* (*software* malicioso). Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, *rootkits*, etc." http://cartilha.cert.br/glossario/#s

[18] "Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros." http://cartilha.cert.br/glossario/#s

[19] "Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares*instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc." http://cartilha.cert.br/glossario/#s

[20] "Redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc." http://cartilha.cert.br/glossario/#s

[21] "Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e

(DDoS)[23], crimes cibernéticos, defesa cibernética, infraestruturas críticas (IEC); é nesse contexto que governos, organizações internacionais, empresas, sociedade civil, academia despertam para um tópico candente da Governança da Internet: "Segurança Cibernética".

1.2. Segurança e proteção – Conceitos

Como tema emergente, os conceitos e contornos da segurança cibernética estão ainda sendo delineados, e os registros na literatura acadêmica são vagos. No entanto, algumas observações já se afiguram sistematizadas em materiais produzidos por organizações internacionais, pesquisadores e agentes de governo.

Em 2008, a União Internacional de Telecomunicações (UIT), agência especializada do Sistema das Nações Unidas (ONU), adotou um conceito possível para a segurança cibernética, elaborado por representantes de Estados e setor privado:

> Segurança Cibernética é a coletânea de ferramentas, políticas, conceitos de segurança, medidas de segurança, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que pode ser usada para proteger o ambiente virtual e os ativos da organização e do usuário. Ativos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações, bem como a totalidade da informação transmitida e / ou armazenada no ambiente cibernético. A Segurança Cibernética se esforça para garantir a realização e manutenção das propriedades de segurança dos ativos da organização e do usuário contra riscos de segurança relevantes no ambiente cibernético. Os objetivos gerais de segurança incluem o seguinte:
> • Disponibilidade

---

arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção." http://cartilha.cert.br/glossario/#s

[22] "Atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet." http://cartilha.cert.br/glossario/#s

[23] "Do Inglês *Distributed Denial of Service*. Ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet." http://cartilha.cert.br/glossario/#s

> • Integridade, que podem incluir a autenticidade e não repúdio
> • Confidencialidade[24]

No plano nacional, o Gabinete de Segurança Institucional (GSI) da Presidência da República é o órgão que coordena as atividades de inteligência federal e de segurança da informação. Para fins deste trabalho, destacam-se suas ações de coordenação relacionadas à segurança para as infraestruturas críticas, segurança da informação e comunicações e segurança cibernética.

O GSI, por meio de sua Portaria nº 45, de 8 de setembro de 2009, apresenta a seguinte conceituação oficial para o Estado:

> Art. 2º Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas.
> § 1º São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
> § 2º São Infraestruturas Críticas as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

Ademais, a Portaria nº 34, de 6 de agosto de 2009, define também "Infraestruturas Críticas da Informação" como "o subconjunto de ativos da informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade". [25]

---

[24] "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality"

Cf. Recomendação X.1205 da UIT-T, §3.2.5, em decorrência dos trabalhos da Comissão de Estudos 17 da UIT-T. (Tradução Livre)

[25] "As Infraestruturas Críticas de Informação possuem a peculiar característica de poderem fazer parte, com relações de interdependências horizontais, de várias Infraestruturas Críticas, ou seja, a informação gerada por determinada área prioritária das Infraestruturas Críticas pode ser insumo

Contrapondo-se as duas definições de “segurança cibernética”[26], percebe-se que são congruentes, sendo a UIT mais detalhista em seu caráter técnico e o GSI a uma estratégia nacional de segurança cibernética, porém nenhum faz menção aos atores e seus papéis a desempenhar.

Nota-se também que, ao passo que a UIT faz referência explícita aos objetivos-atributos [27] da segurança e à informação transmitida e/ ou

---

para outra, evidenciando, desta forma, o alto grau de acoplamento e interdependência existente entre elas. [...]

Além disso, as dependências dos sistemas e serviços, as tendências e evoluções tecnológicas da computação distribuída, as interconexões de redes públicas e privadas e o compartilhamento de recursos expõem as organizações às diversas ameaças, entre elas: fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo, inundação, blackouts, códigos maliciosos, hackers, ataques de DDoS, entre outras.” Cf. CANONGIA, Claudia; MANDARINO Jr., Raphael (org.). *Guia de referência para a segurança das infraestruturas críticas da informação*”. Brasília: GSIPR/SE/DSIC, 2010. pp. 28-29

[26] O professor Johnnatan Zittrain comenta a imprecisão conceitual e o emprego inadequado do termo “cibernético”: “A note on definitions: the danger of network attack is both accentuated and obscured by the term "cyber." It depicts a realm greater than the sum of its parts -- hence cyberwar or cybersecurity sounding much more grave than "Internet war" or "Internet security." The cyber- prefix -- these days also used as a standalone noun -- can mean too many things at once. So let's break it out. First are attacks on the network itself: What could make the Internet go down? Second are attacks on devices attached to the Internet. What could make a Web site -- a bank, or Amazon, or theatlantic.com - become inoperative? Could my own PC suddenly stop working after getting some bad bits over the network? Third is spying: what data might be compromised from afar, whether letters and spreadsheets on your PC, a raft of credit card numbers and prescription data from an online pharmacy, or plans for a missile defense system stowed on the server of a government contractor. Finally there are attacks on physical infrastructure that's intertwined with the Internet, such as an electric grid or air traffic control.” Cf. *Cyber War: Johnnatan Zitrain weighs in*. http://www.theatlantic.com/technology/archive/2011/02/cyber-war-jonathan-zittrain-weighs-in/71027

[27] A) Para a UIT:

- availability: The property of being accessible and useable upon demand by an authorized entity. X.800

- integrity: The property that data has not been altered or destroyed in an unauthorized manner. X.800

- non-repudiation: The ability to prevent a sender from denying later that he or she sent a message or performed an action. J.170

- authenticity: The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information. J.170

- confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Cf. ITU. *ITU-T approved security definitions*. http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0003ZIPE.zip

B) Para o GSI:

- disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

- integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

armazenada, a definição brasileira cita e conceitua as infraestruturas críticas (cujas áreas prioritárias no Brasil são, atualmente, energia, transporte, água, finanças e comunicações), conforme comparação abaixo.

	UIT	GSI
O que é	a coletânea de ferramentas, políticas, conceitos de segurança, medidas de segurança, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que pode ser usada para	a arte de
Objetivo	proteger o ambiente virtual e os ativos da organização e do usuário geral: disponibilidade, integridade, confidencialidade	assegurar a existência e a continuidade da Sociedade da Informação de uma Nação
Por meio de / como	garantir a realização e manutenção das propriedades de segurança dos ativos da organização e do usuário contra riscos de segurança relevantes no ambiente cibernético	garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas
Ativos	Ativos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações, bem como a totalidade da informação transmissão e / ou armazenada no ambiente cibernético.	São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
SC e IEC, conceitos próximos	[IEC são usualmente consideradas sistemas, serviços e funções vitais cuja interrupção ou destruição teria um impacto debilitante na saúde e segurança pública, comércio, e segurança nacional, ou qualquer combinação dessas questões.][28]	São Infraestruturas Críticas as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

Tabela 1: Comparação entre definições de "Segurança Cibernética" para UIT e GSI

- confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

- autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. (Instrução Normativa GSI/PR nº 1/2008)

[28] A Recomendação X.1205 da UIT-T não define IEC. Citou-se extrato do documento *ITU-D Question 22/1: Securing information and communication networks: best practices for a developing country*. Vide nota 29.

Para a UIT, a correlação entre os termos “segurança cibernética” e “proteção de infraestrutura crítica” é natural; apesar de não serem sinônimos, são frequentemente intercambiáveis[29]. A proteção de infraestruturas de informação (críticas e não críticas) seria subconjunto da segurança cibernética[30], conforme a seguinte matriz:

[29] “While definitions may vary slightly, critical infrastructures (CI) are generally considered as the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of those matters. CI are composed of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data). What constitutes “critical” may vary from country to country, but typically might include elements of the information and communications (including telecommunications) technology (ICT), energy, banking, transportation, public health, agriculture and food, water, chemical, shipping, and essential government services sectors. Countries at all stages of development need to plan for and develop policies to protect what they determine to be their CI (in other words, Critical Infrastructure Protection, including both physical and virtual protection) in order to provide reasonable assurance of resilience and security to support national missions and economic stability.

Each of these economic sectors has its own physical assets, such as bank buildings, power plants, trains, hospitals and government offices. However, these critical sectors of a nation’s economy all depend upon information and communication technologies. Across the board, these sectors and their physical assets today depend upon the reliable functioning of this critical information infrastructure (CII) to deliver their services and to conduct business. Consequently, significant disruption to the CII could have an immediate and debilitating impact that reaches far beyond the ICT sector and affects the ability of a nation to perform its essential missions in multiple sectors. A critical information infrastructure protection (CIIP) program protects the virtual component of the CII.” *Cf.* ITU. *ITU-D Question 22/1: Securing information and communication networks: best practices for a developing country*. http://www.itu.int/publ/D-STG-SG01.22-2010/en pp 1-2

[30] “... CIIP is a subset of both CIP and of cybersecurity. Cybersecurity protects against all forms of cyber incidents by strengthening the safety of the critical information infrastructure on which the critical sectors depend and securing the networks and services which serve the day-to-day needs of users. Cyber incidents may affect the critical and non-critical information infrastructures alike and may take many forms of malicious activity such as use of botnets to conduct denial of service attacks and distribute spam and malware (e.g. viruses and worms) which affect the ability of the networks to operate. In addition, cyber incidents may include illicit activities such as phishing and pharming, as well as identity theft. The cyber threat continues to increase as the tools and methodologies used become more and more widely available, and the technical capability and sophistication of cyber criminals expand. Countries at all stages of development have experienced these cyber incidents.” ITU-D 22/1 Report. http://www.itu.int/publ/D-STG-SG01.22-2010/en p. 2

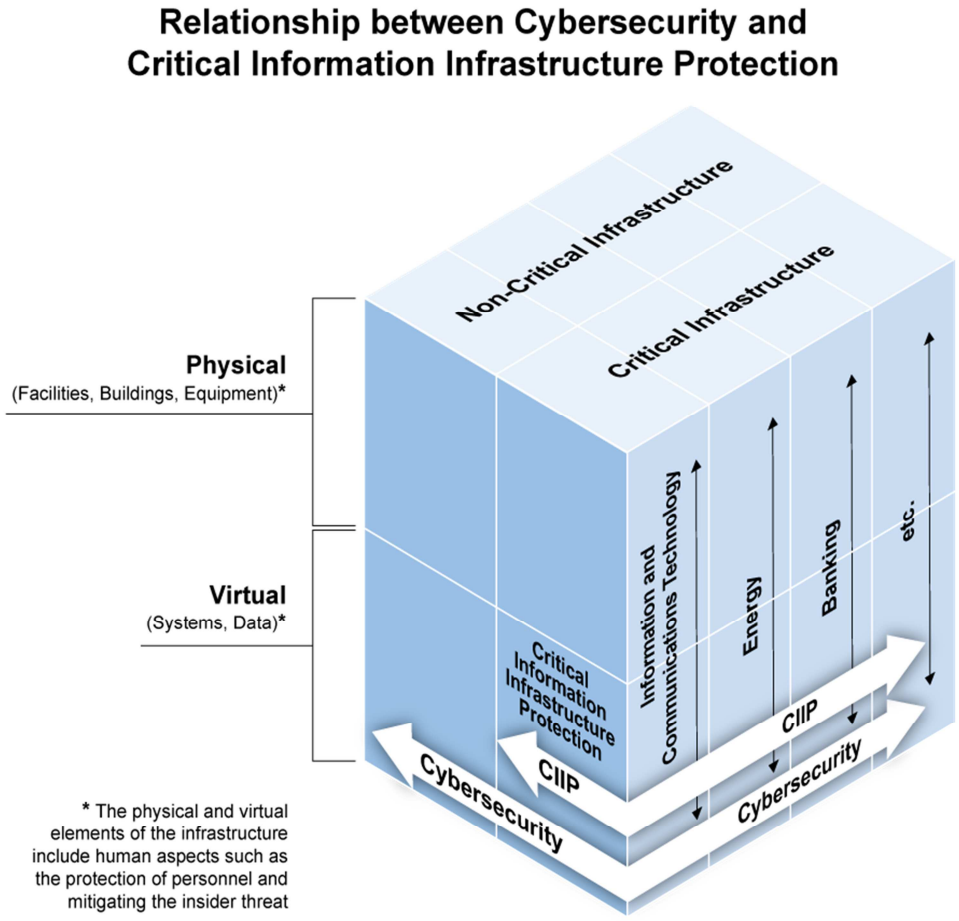


Figura 1: Relação entre Segurança Cibernética e Proteção da Infraestrutura Crítica da Informação (Fonte: UIT)

Em sua totalidade, a segurança cibernética envolveria a proteção das diversas infraestruturas críticas e não críticas e os elementos físicos e virtuais da nação, um tema de responsabilidade compartilhada entre os vários atores envolvidos, sob a liderança do Estado.

Como se infere da ilustração, o setor de telecomunicações / TICs (paralelamente aos demais), seguiria essa mesma característica, e parece lógico que também o órgão regulador das telecomunicações seja um dos atores a contribuir nessa seara.

A “Convenção de Tampere sobre o Fornecimento de Recursos de Telecomunicações para Minimização de Desastres e para Operações de Socorro”, aprovada na Conferência Intergovernamental sobre Telecomunicações de

Emergência (ICET-98), realizada em Tampere, na Finlândia, em julho de 1998, corrobora essas afirmações[31].

Definições do Tratado, tais como “Desastre”, “Minimização de Desastre”, “Assistência de Telecomunicações” e “Recursos de Telecomunicações” não são encontradas no marco regulatório do setor de telecomunicações no Brasil, mas não são conflitantes com o mesmo.

Tais termos guardam estrita relação com o conceito de “Segurança Cibernética” e “Infraestruturas críticas”, conforme definidos pela Portaria nº 45-GSI, de 8 de setembro de 2009; e de “defesa civil”, “desastre”, “situação de emergência”, “estado de calamidade pública”, “ações de socorro”, “ações de assistência às vítima”, “ações de restabelecimento de serviços essenciais”, “ações de reconstrução”, “ações de prevenção”, definidas pelo Decreto nº 7.257, de 4 de agosto de 2010, que dispõe sobre o Sistema Nacional de Defesa Civil (SINDEC) e outros.

Quanto aos “crimes cibernéticos”, esta expressão não existe na legislação jurídica nacional como um tipo ou categoria penal, e tem sido empregada de maneira genérica globalmente para se referir a “qualquer atividade delitiva em que os computadores ou redes são um instrumento, um objeto ou um local de atividade criminosa”[32].

Para fins deste trabalho, em razão do caráter transnacional e de os países abordarem essas condutas de maneiras distintas, um crime cibernético pode ser considerado “a atividade realizada mediante um computador que é ilícita ou que algumas Partes considerem ilícita e que pode se consumar por meio das redes eletrônicas mundiais”.[33]

Apesar de o Brasil não ter acedido (e possivelmente não o fará) à Convenção sobre Crimes Cibernéticos adotada pelo Conselho da Europa em 2001

---

[31] Representantes de Anatel e Ministério das Relações Exteriores (MRE) estiverem presentes à Conferência e aprovaram o texto da Convenção, que ainda não foi ratificada pelo País. O Diploma pode ser encontrado em http://www.itu.int/ITU-D/emergencytelecoms/tampere.html.

[32] UIT. *El Ciberdelito: Guía para los países en desarrollo*. p. 17. Disponível em: <http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf>. Acesso em: 11.08.2010. (Tradução Livre)

[33] Op. cit.

("Convenção de Budapeste"), em resumo e de modo ilustrativo, citam-se quatro tipos diferentes a que se refere tal Convenção:[34] [35]

> Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computação (i.e. acesso ilegal, intercepção ilegal, interferência de dados, interferência de sistema, uso indevido de equipamentos);
> Crimes relacionados a computadores (i.e., falsificações relacionadas a computadores e fraudes relacionadas a computadores);
> Crimes relacionados a conteúdo (i.e., crimes relacionados a pornografia infantil); e
> Crimes relacionados à proteção de direitos autorais (i.e., crimes relacionados a infrações de direitos autorais e diretos correlatos)

Tangenciando o tema deste trabalho, o debate sobre o Brasil assinar ou não a Convenção de Budapeste persiste e esbarra na clara oposição do Ministério das Relações Exteriores (MRE), sob o argumento de que não seria da tradição diplomática brasileira assinar instrumentos dos quais o País não tenha participado do processo negocial, e também por conflitar com interesses brasileiros no campo da propriedade intelectual.

O MRE parece preferir provocar a renegociação do tema na agenda do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), conforme se depreende da complementariedade entre (i) o apoio brasileiro à Declaração de Salvador resultante do 12º Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, realizado entre 12 e 19 de abril de 2010, na Bahia, [36] e

---

[34] *Cf.* UIT. *Cybersecurity: The Role and Responsibilities of an Effective Regulator*. p. 17. (Tradução Livre)

[35] "Esta clasificación no es totalmente coherente, ya que no se basa en un sólo criterio para diferenciar las categorías. Tres de las categorías se refieren al objeto de la protección jurídica: "delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"; "delitos informáticos" y "delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines". La cuarta categoría "delitos informáticos" no se refiere al objeto de la protección jurídica sino al método. Esta incoherencia genera cierta coincidencia entre las categorías." UIT. *El Ciberdelito: Guía para los países en desarrollo*. p. 19. Disponível em: <http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf>. Acesso em: 11.08.2010.

[36] Lê-se na Declaração de Salvador: "42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime." In: UNODC. http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf 27.02.2011

(ii) o discurso do País em painel sobre "Segurança, Abertura e Privacidade" no Forum de Governança da Internet (IGF) 2010, realizado na Lituânia entre 14 e 17 de setembro de 2010.[37]

1.3. Segurança e telecomunicações

A sequência de interrupções na prestação do serviço de banda larga Speedy, da Telefónica, no Estado de São Paulo em 2008 e 2009,[38] evidenciou a dimensão que esses incidentes podem tomar na Sociedade da Informação, particularmente quando os atores não estão preparados para lidar com elas.

Segundo relatórios produzidos pela Agência Nacional de Telecomunicações (Anatel), descompassos entre o investimento em capacidade e o crescimento da demanda pelo serviço de banda larga da companhia, associados a possíveis ataques de negação de serviço, foram capazes de interromper serviços essenciais ao cidadão, inclusive de saúde e segurança pública, e deixar

[37] No IGF 2010, o Brasil afirmou: "In the last 10 or 15 years, we have seen many regional or specific initiatives towards the question of security and the Internet, mainly of them the initiatives from industry, from the Convention of Europe, Budapest Convention, law enforcement initiatives and is so on. We understand these are all valuable contributions but they must feed international consultation process where all stakeholders, all Governments, private sector, Civil Society, can participate and write the principles and mechanisms within their own capacity towards a secure Internet. This approach of international participation is very important. [...] the experience of Brazil in that respect. We evaluated privacy, security and openness are issues that must be dealt with together. We have to treat them together. So in this sense, last year, we produced internally the principles for GovernmentGovernance and use of Internet and they are 10 principles. They were distributed alongduring all this IGF, and just to be brief, two of them are directly related to our debate today. The first principle means that the use of Internet must be driven by the principles of freedom of expression, individual privacy and the respect for Human Rights, recognizing them as essential to preservation of a fair and Democratic society. And the 8th principle means, functionality, security, and stability of Internet. The stability, security and overall functionality of the network must be actively preserved for the adoption of technical measures that are consistent with international standards and encourage the adoption of best practice." http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/658-sop 27.02.2011

[38] Como caso mais recente, e, 21 de dezembro de 2010, incêndio em central telefônica da operadora Oi na Bahia, que interrompeu a prestação de serviços de telefonia móvel, fixa e banda larga, afetou a vida de cidadãos, o esperado comércio de fim de ano, serviços essenciais e até a matrículas escolares em diversos estados.Cf. *Incêndio atinge prédio da Oi na Bahia e afeta telefonia em 6 estados* http://g1.globo.com/brasil/noticia/2010/12/incendio-atinge-predio-da-operadora-oi-na-bahia.html; *BA: incêndio na Oi prejudica matrículas escolares* http://tudoglobal.com/blog/capa/98822/ba-incendio-na-oi-prejudica-matriculas-escolares.html

incomunicáveis empresas, bancos, lotéricas, e, naturalmente, o usuário doméstico.[39]

Período da Interrupção	Usuários afetados	Causa da Interrupção
das 8:00h de 02/07/2008 às 24:00h de 05/07/2008	Aproximadamente 2 milhões de acessos, inclusive entes públicos e corporações privadas	Problemas em equipamentos da rede do SCM da empresa
das 22:00h de 06/04/2009 às 3:30h de 09/04/2009	Totalidade dos usuários	Ataques de negação de serviço (denial of service – DoS) no sistema de nomes de domínio (Domain Name System – DNS)
das 12:30h às 23:40h de 18/05/2009	Suspeita de ter atingido a totalidade de usuários	Instabilidades em seu DNS
das 13:00h às 19:30h de 02/07/2009	Totalidade dos usuários	Diminuição de desempenho dos servidores DNS

Tabela 2: Síntese do período, alcance e causa das interrupções (Fonte: Autor)

Em situações como essa, o impacto financeiro direto e indireto é sentido ao longo de toda a cadeia de valor das TICs, desde vendedores de softwares, operadores de rede, provedores de serviços de Internet a usuários, e incluem, por exemplo, custos com medidas preventivas e reativas, custos com largura de banda e equipamentos, custos de oportunidade com o congestionamento das redes.[40]

---

[39] ANATEL. Análise nº 316/2010-GCER, de 06/07/2010. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=245740&assuntoPublicacao=null&caminhoRel=Cidadao-Biblioteca-Acervo%20Documental&filtro=1&documentoPath=245740.pdf>. Acesso em: 22.09.2010.

[40] Um estudo da UIT sobre aspectos financeiros da segurança cibernética concluiu que:

"Estimates of the financial effects of malware differ widely. Figures for overall effects range from US$ 13.2 billion of direct damages for the global economy (in 2006) to US$ 67.2 billion in direct and indirect effects on U.S. businesses alone (in 2005).

In a survey of its members, the Computer Security Institute (CSI) estimated the loss caused by cybersecurity breaches per responding firm to US$ 345,0000 in 2006. This number is most likely not representative for businesses in general due to the unique membership of CSI. The 2006 number is considerably lower than its peak in 2001 but more than double the 2005 level.

Consumer Reports estimated the direct costs to U.S. consumers of damages experienced due to malware and spam to US$ 7.1 billion in 2007.

One estimate put the global cost of spam in 2007 at US$ 100 billion and the respective cost for the U.S. at US$ 35 billion. Another study found that the cost of spam management in the U.S. alone amounted to US$ 71 billion in 2007.

Como resultado, além dos prejuízos financeiros de todo esse grupo que ficou incomunicável, a Agência Nacional de Telecomunicações determinou cautelarmente a suspensão da comercialização do Speedy, enquanto a Telefónica não garantisse a qualidade da prestação de seu serviço, sob pena de multa.[41]

Episódios dessa magnitude favorecem à *Federal Communications Commission* (Comissão Federal de Comunicações / FCC, agência independente nos Estados Unidos que responde pela regulação da comunicação interestadual e internacional por rádio, televisão, par de cobre, satélite ou cabo) afirmar que "a segurança cibernética é um tema vital para a Comissão [FCC] porque a falta de confiança do usuário final na experiência online vai reprimir a demanda por serviços de banda larga". Com isso, no contexto do plano nacional de banda larga estadunidense, caberia ao regulador a promoção da segurança cibernética e a proteção da infraestrutura crítica de banda larga.[42]

Em síntese, vez que as TICs dependem intrinsecamente dos serviços e da infraestrutura de telecomunicações de um país, crê-se que o órgão regulador do setor, para garantir o cumprimento de sua missão, teria função destacada em um cenário de administração de riscos, ameaças e vulnerabilidades da Sociedade da Informação.

Uma das razões para que a Anatel se coordene decorre dos compromissos internacionais assumidos pelo País. A Agência, incumbida legalmente de adotar as medidas necessárias para o atendimento do interesse

---

In 2007, the costs of click fraud in the U.S. were estimated to be nearly US$ 1 billion.

Numbers documenting the magnitude of the underground Internet economy and transactions between it and the formal economy also vary widely. One source estimates the worldwide underground economy at US$ 105 billion.

No reliable numbers exist as to the potential opportunity costs to society at large due to reduced trust and the associated slower acceptance of productivity-enhancing IT applications. However, a considerable share of users expressed concern and indicated that it reduces their willingness to perform online transactions."

Cf. UIT. *ITU Study on the Financial Aspects of Network Security: Malware and Spam*. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf>. Acesso em: 11.08.2010.

[41] Despacho nº 4.043/2009-CD - Processo nº 53500.011781/2009, publicado no DOU, em 22 de julho de 2009. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?data=22/06/2009&jornal=1&pagina=51&totalArquivos=72>. Acesso em: 22.09.2010.

[42] BROADBAND.GOV. *Connecing America: The National Broadband Plan*. 2010. Disponível em: <http://www.broadband.gov/plan/16-public-safety/#r16>. Acesso em: 12/08/2010.

público e para o desenvolvimento das telecomunicações brasileiras, tem competência para representar o Brasil nas organizações internacionais de telecomunicações[43], sob a coordenação do Poder Executivo (art. 19, II, da Lei 9.472/97, Lei Geral de Telecomunicações / LGT)[44].

A União Internacional de Telecomunicações recebeu da Cúpula Mundial da Sociedade da Informação (CMSI) o mandato de facilitador da Linha de Ação C5, "Criação de confiança e segurança na utilização das TICs". Com isso, as atividades dessa organização no campo das TICs e da segurança cibernética são crescentes. Por ser o elo nacional com a UIT, a Agência tem sido frequentemente demandada a se manifestar e contribuir suas atividades de segurança cibernética.

Embora sem a sistematização que o tema exigiria, a Agência ousa ao cooperar com instituições nacionais e internacionais, fornecendo informações sobre normas e padrões de segurança de redes de telecomunicações, proteção de infraestruturas críticas de telecomunicações, combate a *malwares* e crimes cibernéticos. Crê-se que com melhor estruturação do papel da Anatel, sua parcela de contribuição possa ser ainda mais efetiva, superando a fase presente de atuação errática e descentralizada.

Para a UIT, o movimento de extensão da atuação do regulador nessa seara é mesmo natural.

Como preparação para o IX Simpósio Global de Reguladores (GSR), realizado no Líbano, em novembro de 2009, a UIT divulgou o artigo "*Cybersecurity: The Role and Responsibilities of an Effective Regulator*". A pesquisa constatou que o papel do regulador teria evoluído junto com a

---

[43] Entre essas, destacam-se a União Internacional de Telecomunicações (UIT), instituição do Sistema das Organizações das Nações Unidas (ONU), a Comissão Interamericana de Telecomunicações (Citel), agência da Organização dos Estados Americanos (OEA), e o Subgrupo de Trabalho nº 1 "Comunicações" (SGT 1), do Mercado Comunicações do Sul (Mercosul).

[44] "Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente:(...)

II - representar o Brasil nos organismos internacionais de telecomunicações, sob a coordenação do Poder Executivo;(...)

XXXI - promover interação com administrações de telecomunicações dos países do Mercado Comum do Sul - MERCOSUL, com vistas à consecução de objetivos de interesse comum." Lei nº 9.472, LGT.

tecnologia, a abertura de mercados à competição, o crescimento da relevância das TICs, a ampliação do objeto de atuação do regulador (de telecomunicações para TICs).

Seja como protagonista na atividade regulatória direta (na proteção de infraestrutura crítica e imposição de padrões técnicos) ou como contribuinte eventual (no combate ao crime cibernético e na formulação da estratégia nacional de segurança cibernética), o papel crescente do regulador nas atividades de segurança cibernética seria uma de suas novas atribuições.

Os autores afirmam também que apesar de sua familiaridade com a indústria de TICs e ampla disponibilidade de mão de obra especializada, o desafio primário do regulador é definir seu papel no esforço nacional de segurança cibernética. Cabe ao regulador encontrar formas de agregar valor às atividades de segurança cibernética e assessorar a formulação de políticas sem necessariamente ser a instituição a liderar essas iniciativas.

Ademais, a credibilidade do regulador determinará sua capacidade de articulação com os demais atores. Em particular, por ser o tema associado às políticas de segurança nacional, tradicionalmente sob o domínio exclusivo de forças armadas, órgãos de segurança pública e agências de inteligência, impõe-se que o regulador seja reconhecidamente uma instituição madura da Administração.

A FCC é possivelmente uma instituição com tal característica. Trata-se de uma agência reguladora com mais de setenta anos de experiência em um mercado paradigmático para a privatização do setor. Nesse momento, a Comissão goza de prestígio político perante a Casa Branca, em um governo que elevou o caráter estratégico das TICs e, em especial, da Internet, para a economia, política e segurança dos Estados Unidos.

Não é o caso da Anatel.

> As agências (…) fazem muito mais que escolher os meios para execução de uma política pública; elas redefinem o significado de tais políticas. Neste ponto, o modelo norte-americano, mais calejado no trato com sua agência reguladora de telecomunicações, vê com naturalidade a agência como fonte de política. Ele é honesto em demonstrar que é no âmbito da agência que se forma muito da vontade política do setor de telecomunicações e assim o faz por intermédio da referência à FCC como um *sistema de representação de interesses* para

> servir como *ponto de encontro das vontades políticas* gravado com o caráter de nacionalização das discussões políticas envolvendo legislações estaduais sobre um setor de extensão nacional e internacional. [45]

Por seu caráter protagonista, no que tange à defesa da atuação de reguladores da segurança cibernética, FCC e UIT servem como referencial neste trabalho de busca pelo papel da Anatel. São também bons parâmetros porque a Anatel é firme atuante na UIT (por meio das Comissões Brasileiras de Comunicação/ CBCs, responsáveis pela coordenação dos posicionamentos do País em foros internacionais[46]) e parece guardar similaridades bastante mais relevantes do que diferenças em relação ao regulador estadunidense.[47]

---

[45] ARANHA, Márcio Iorio. *Políticas públicas comparadas de telecomunicações (Brasil-EUA)*. Brasília: UnB, 2005. pp. 194-195

[46] "Para executar a atribuição definida no Art. 19, II, da LGT, a Anatel criou as Comissões Brasileiras de Comunicações (CBCs), pelas Resoluções n.º 110 de 8 de março de 1999, nº 265 de 13 de junho de 2001, nº 462 de 13 de abril de 2007, depois revogadas pela Resolução nº 502 de 18 de abril de 2008.

O objetivo primordial das CBCs é viabilizar um ambiente para discussões dos posicionamentos nacionais, permitindo que a Administração brasileira atue de forma coordenada e integrada nos foros internacionais de telecomunicações, além de: realizar estudos e análises de questões técnicas de interesse específico nacional; preparar as "Propostas de Contribuições e Posições Brasileiras" que objetivem orientar o posicionamento da Administração brasileira junto aos foros internacionais de telecomunicações; participar dos trabalhos das Comissões de Estudo dos Setores de Normalização de Telecomunicações, de Radiocomunicações e de Desenvolvimento da União Internacional de Telecomunicações (UIT-T, UIT-R e UIT-D), dos trabalhos desenvolvidos no âmbito dos Comitês Consultivos Permanentes da Comissão Interamericana de Telecomunicações - Citel, do Subgrupo de Trabalho Nº 1 - Comunicações (SGT 1) do Mercosul e de outros organismos internacionais (i.g. CPLP, Regulatel); propor a realização de seminários, reuniões e debates e fomentar a participação de novos especialistas; elaborar relatórios anuais sobre o andamento de seus trabalhos, dentre outras.

A participação nas Comissões Brasileiras de Comunicações (CBCs) é aberta aos segmentos públicos e privados da sociedade brasileira com interesse direto no setor de telecomunicações, assim como a especialistas que possam prestar colaboração nesta área, ou seja: empresas prestadoras de serviços de telecomunicações; organizações científicas e industriais; empresas de consultoria e de prestação de serviços especializados; instituições de ensino, pesquisa e desenvolvimento; agências ou órgãos governamentais com interesse na área de telecomunicações; entidades e associações de classe do setor; e profissionais que atuam isoladamente ou no âmbito de organizações em áreas ligadas às telecomunicações, como consultores, professores ou pesquisadores.

Atualmente as CBCs são estruturadas de forma temática, atuando nas seguintes áreas: CBC 1: Governança e Regimes Internacionais; CBC 2: Radiocomunicações; CBC 3: Normalização de Telecomunicações; CBC 4: Desenvolvimento das Telecomunicações." www.anatel.gov.br

[47] Em estudo comparativo dos modelos de políticas públicas do setor de telecomunicações no Brasil e Estados Unidos, ARANHA conclui que "pode-se extrair uma conclusão intuitiva: as semelhanças ultrapassam em muito as diferenças; elas dominam o cenário em meio a raras divergências. (…)

A síntese das semelhanças e diferenças entre as políticas públicas dos dois países (Brasil-EUA) está nas suas agências reguladoras. Elas representam a estrutura institucional que serve de

Tendo a Anatel se comprometido a tomar providências específicas em prol da segurança cibernética, conforme determinou o Plano Geral de Atualização da Regulamentação das Telecomunicações no Brasil (PGR)[48], de 30 de outubro de 2008, a troca de informações com essas instituições pode ser útil para adequar conceitos e terminologia, desenvolver estratégias e projetos, caso de interesse brasileiro.

O PGR, que se propõe a guiar a atuação da Agência nos próximos anos, chega a estabelecer uma pretensiosa ação de curto prazo (que venceu ao final de 2010): "Realização de estudos e adoção de medidas para a proteção da infraestrutura nacional de telecomunicações contra falhas e ataques de guerra cibernética." A ação seria implementada por meio de três projetos: "(i) Proteção da infraestrutura crítica de telecomunicações; (ii) Regulamento de interrupções sistêmicas do STFC; (iii) Segurança e proteção da infraestrutura nacional de telecomunicações".

Ainda que esses três projetos se encerrem formalmente, conforme a meta estabelecida, a Agência não deve deixar de trabalhar em prol da construção de confiança e segurança das redes do setor, senão incrementar sua atuação.

---

ambiente especializado para depuração da política setorial a partir da idéia de uma nova instituição para acompanhamento conjuntural – *ongoing policy* – das transformações tecnológicas e econômicas, por intermédio de projeções político-jurídicas.

As duas agências reguladoras de telecomunicações do Brasil e dos EUA basicamente se igualam em aspectos estruturais, funcionais, procedimentais e de posição institucional, em especial, nas subdivisões orgânicas dos respectivos parlamentos, no processo de indicação dos membros, sua sabatina, e definição de mandatos, na função de aplicação da política pública elaborada por outras instâncias políticas dos respectivos países, no poder normativo, bem como na atuação as agências pró-consumidor." ARANHA. pp 184 – 197.

[48] O Plano Geral de Atualização da Regulamentação das Telecomunicações no Brasil (PGR), estabelecido pelo a Resolução nº 516, de 30 de outubro de 2008, representa a visão estratégica da Agência para a regulação do setor para os próximos anos. O PGR estabeleceu 9 objetivos e 15 propósitos estratégicos, a partir daí, definiu 23 ações de curto prazo (para implementação imediata ou em até 2 anos, a contar da publicação do plano), 9 ações de médio prazo (para implementação em até 5 anos) e 5 ações de longo prazo (para implementação em até 10 anos). Essas ações executadas por meio de 59 projetos.

2. MODELOS INTERNACIONAIS DE POLÍTICAS DE SEGURANÇA CIBERNÉTICA

Em um cenário onde as incertezas sobre a elaboração e a condução das estratégias nacionais para políticas de segurança cibernéticas são muitas, a troca de informações e experiências internacionais desponta como premissa básica. Estando os diversos países conectados, muitas vezes os interesses e ponderações das nações coincidem e convergem para aspectos comuns.

Trata-se de também de uma escolha que depende de alianças estratégicas formadas conforme a política externa de cada nação.

A seguir, indica-se, em linhas gerais, a forma como a segurança cibernética tem sido abordada na UIT e nos Estados Unidos da América. O enfoque é para o setor de telecomunicações, e para alcançar este objetivo, oferecem-se também informações generalistas de cunho introdutório, que por vezes estão diretamente relacionadas à estratégia (institucional) maior de segurança cibernética.

2.1. União Internacional de Telecomunicações

Em razão de sua amplitude temática, a UIT é uma organização que abarcaria diversas facetas da segurança cibernética, mas que, por óbvio, não deixa de ser apenas um entre tantos atores lutando para ganhar espaço na coordenação dos esforços internacionais. [49]

Estruturada em órgãos de cúpula (Conferência de Plenipotenciários e Conselho) e setores temáticos (Radiocomunicações, Normalização e Desenvolvimento, com respectivas conferências mundiais), sua governança

[49] Com a emergência do tema, diversos atores internacionais disputam a titularidade da pauta de segurança cibernética: UNODC, Interpol, OCDE, APEC, OEA. Analisar ou defender quem deveria liderar na arena internacional está fora do escopo deste trabalho. Como o foco da pesquisa é o setor de telecomunicações e a atuação do órgão regulador, elegeu-se destacar exclusivamente a legitimidade da atuação da UIT, como foro internacional primário para as telecomunicações do Sistema ONU.

institucional é bastante madura, mas, por vezes, deveras morosa. Encontrar consensos em processos deliberativos que podem envolver 192 Estados Membros e 700 diferentes empresas e organizações (Membros do Setor e Membros Associados) pode ser um processo penoso, típico do Sistema ONU, que, para a indústria de alta tecnologia, se torna imprestável.

Cada um de seus Setores e órgãos apresenta ainda subdivisões temáticas, em que Comissões de Estudo abordam Questões relevantes para as TICs, onde empresas, Academia, centros de pesquisa têm assento, lado a lado, com Estados soberanos. Em suma, a UIT é essencialmente um ambiente *multistakeholder* (com altas barreiras à entrada, mas *multistakeholder*).

Com isso, embora muitas vezes se faça alusão (inclusive neste trabalho) a "uma UIT", deve-se ter presente que a instituição não é monolítica, existem interesses difusos, posicionamentos divergentes e dissensos em seus diversos níveis. Essa afirmação, característica da abstração de qualquer pessoa jurídica, deve ser repisada, por se referir à suposta manifestação de vontade de Estados soberanos.

Desde o século XIX, a União Internacional de Telecomunicações (originalmente, União Telegráfica Internacional) é uma organização responsável por harmonizar faixas de radiofrequências, capacidades satelitais, padrões técnicos para as comunicações à distância.[50]

Com a difusão da Internet e o sedimentação de iniciativas privadas robustas como *Institute of Electrical and Electronics Engineers* (IEEE), *Internet Engineering Task Force* (IETF), *International Organization for Standardization* (ISO), *Internet Corporation for Assigned Names and Numbers* (ICANN), a UIT perdeu espaço e se esforça para redefinir seu papel no competitivo cenário convergente. Nesse sentido, alguns Estados (mormente alguns países em desenvolvimento que não conseguem se sobressair em foros como a ICANN) buscam fortalecer[51] e outros (sobretudo países desenvolvidos) almejam estreitar[52] seu mandato em temas como Governança da Internet e Segurança Cibernética.

---

[50] http://www.itu.int/en/history/Pages/default.aspx 01.03.2011

[51] Cite-se *policy statement* do Brasil na Conferência de Plenipotenciários 2010 (PP-10), principal conferência da UIT, realizada entre 4 e 22 de outubro de 2010, em Guadalajara, México: "The

2.1.1. Legitimação: Cúpula Mundial da Sociedade da Informação (CMSI)

Uma das apostas da UIT para garantir sua primazia no cenário internacional de TICs foi a Cúpula Mundial da Sociedade da Informação (CMSI)[53], cujo pano de fundo era revisar a estrutura de Governança da Internet e assegurar às Nações Unidas capacidades de gestão que permanecem nas mãos governo e instituições estadunidenses, como *Internet Assigned Numbers Authority* (IANA) e ICANN.

Realizada em duas fases (Genebra 2003 e Túnis 2005)[54] com ampla participação de governos, organizações internacionais, setor privado e sociedade

---

exponential growth of the Internet has given ITU a central role in questions related to Internet. This includes actions such as discussing Internet related public policy issues, building confidence and security in the use of ICTs and acting as a facilitator in the transition from IPv4 to IPv6. ITU needs to continue working on Internet related matters, since this is as an unquestionable need in face of convergence and of an all-IP world." http://www.itu.int/plenipotentiary/2010/statements/brazil/sardenberg.html

[52] Os Estados Unidos são os mais contundentes opositores à atuação da UIT na Governança da Internet e a segurança cibernética, nos termos de seu *policy statement* à mesma PP-10:

"Much of the effort here in Guadalajara should be devoted to seeking ways to enhance the ITU's excellent contributions to efficient and widely developed telecommunications services and infrastructure—to improving things that it does best: harmonizing radio frequency allocations, developing and disseminating best practices, and contributing to capacity building.

The United States has identified three matters that warrant special mention in this regard.

First, the ITU should be a place where the development of the Internet is fostered. The Internet has progressed and evolved in a remarkably successful way under the existing multi-stakeholder arrangements. Changes, especially changes involving inter-governmental controls, are likely to impair the dynamism of the Internet—something we all have an interest in avoiding.

Second, the ITU's interest in cybersecurity should continue to focus on capacity building and the associated development and dissemination of best practices. This is an area where an enormous amount remains to be done, and where improvements will prove very valuable to all ITU members, regardless of the state of their digital development. We believe very strongly that the ITU should not be distracted from this important responsibility by straying into areas outside of its mandate and expertise such as cybercrime and cyberwar.

Third, looking forward to the 2012 World Conference on International Telecommunications, it would be a serious mistake to seek to extend the International Telecommunications Regulations to today's world of broadband and the Internet. There is a superficial similarity between the narrowband for which the ITRs were configured and the broadband of today, but it is only superficial. Just as with the Internet, inter-governmental controls over broadband are likely to do much more harm than good." http://www.itu.int/plenipotentiary/2010/statements/usa/verveer.html

[53] http://www.itu.int/wsis/index.html

[54] "A Cúpula ou Cimeira Mundial sobre a Sociedade da Informação (CMSI) consistiu em dois eventos patrocinados pela Organização das Nações Unidas (ONU) sobre informação, comunicação e, em termos amplos, a Sociedade da Informação que ocorreu em 2003 em Genebra e em 2005 em Túnis. Uma de suas metas principais era diminuir a então chamada exclusão digital global que

civil, a CMSI reservou às agências das Nações Unidas funções estratégicas em prol da inclusão digital global e acesso à Internet.[55] Os interesses da ONU permanecem e estão refletidos, por exemplo, na recente renovação do mandato do Fórum de Governança da Internet (IGF), criticado por supostamente não apresentar resultados concretos.[56]

À UIT, a CMSI atribuiu o papel de facilitador das Linhas de Ação C2 "Infraestrutura da informação e comunicação" e C5 "Criação de confiança e segurança na utilização das TICs", sendo as metas da última as mais relevantes para este trabalho:

> Plano de Ação de Genebra[57]
>
> C5. Criação de confiança e segurança na utilização de TICs
>
> a) Promover a cooperação entre os governos nas Nações Unidas e com todos os atores interessados em outros fóruns idôneos para estimular a confiança do usuário, construir credibilidade e proteger os dados e a integridade da rede; considerar os riscos existentes e potenciais para as TICs e abordar outras questões de segurança da informação e das redes.

---

separa países ricos e pobres através da ampliação do acesso àInternet no mundo em desenvolvimento. As conferências marcaram o dia 17 de Maio como o Dia Mundial da Sociedade da Informação.

Em 2003, na cidade de Genebra, na Suíça, representantes de 175 países participaram da primeira fase do CMSI, onde eles adotaram uma Declaração de Princípios. Esse é o caminho para adquirir uma sociedade de informação acessível para todos e baseada em conhecimento compartilhado. Um Plano de Ação estabeleceu a meta de que 50% da população mundial tenha acesso à Internet em 2015. A Cúpula de Genebra também deixou questões controversas não resolvidas, como a questão do financiamento e a Governança da Internet.

Quando a Cúpula falhou em um acordo sobre o futuro da GI, o Grupo de Trabalho sobre Governança da Internet (GTGI) foi criado com a função de conseguir novas ideias em como progredir.

A segunda fase do CMSI foi realizada entre os dias 16 e 18 de Novembro de 2005, em Túnis, na Tunísia. Isso resultou no acordo sobre o Compromisso de Túnis e a Agenda de Túnis para a Sociedade da Informação, além da criação do Fórum de Governança da Internet." http://pt.wikipedia.org/wiki/CMSI

[55] As Linhas de Ação, distribuídas entre UNESCO, UNCTAD, UNDP, FAOI, OMC, UPU, OIT, OMS, ECOSOC são: C1. A função dos governos e de todos os atores envolvidos com a promoção das TICs para o desenvolvimento; C2. Infraestrutura da informação e comunicação; C3. Acesso à informação e ao conhecimento; C4. Capacitação; C5. Criação de confiança e segurança na utilização das TICs; C6. Ambiente habilitador; C7. Aplicações das TICs; C8. Diversidade e identidade cultural, diversidade lingüística e conteúdo local; C9. Meios de comunicação; C10. Dimensões éticas da Sociedade da Informação; C11. Cooperação internacional e regional.

[56] Para discussão aprofundada sobre Governança da Internet, vide KURBALIJA, J. *An Introduction to Internet Governance*. 164 p. DiploFoundation and National Internet Exchange of India (NIXI): 2008. http://www.diplomacy.edu/poolbin.asp?IDPool=806.

[57] http://portal2.tcu.gov.br/portal/pls/portal/docs/670132.PDF RITS.

> b) Os governos, em cooperação com o setor privado, devem detectar, impedir e combater o cibercrime e o uso indevido das TICs: definindo diretrizes em que se leve em conta o trabalho que já se realiza nestes âmbitos; considerando a possibilidade de promulgar normas que permitam investigar e punir efetivamente a utilização indevida; promovendo esforços mútuos efetivos de assistência; fortalecendo o apoio institucional em nível internacional para evitar, detectar estes incidentes e reagir de forma apropriada; e promovendo a educação e a sensibilização.
> c) Os governos e outras partes interessadas devem fomentar ativamente a educação e a sensibilização dos usuários em relação à privacidade on-line e aos meios de proteger a privacidade.
> d) Tomar medidas apropriadas contra o envio massivo de mensagens não solicitadas em nível nacional e internacional.
> e) Encorajar a avaliação da norma jurídica nacional para superar quaisquer obstáculos que impeçam a utilização efetiva de documentos e transações eletrônicas, inclusive dos meios eletrônicos de autenticação.
> f) Seguir consolidando o marco de confiança e segurança com iniciativas complementares e de reforço mútuo nos diversos âmbitos da segurança de utilização das TICs, com iniciativas ou diretrizes no que diz respeito ao direito à privacidade, à proteção dos dados e à segurança dos consumidores.
> g) Compartilhar boas práticas no âmbito da segurança da informação e da segurança das redes e promover sua utilização por todas as partes interessadas.
> h) Convidar os países interessados a criar centros para reação e atendimento em tempo real em caso de incidentes e desenvolver uma rede cooperativa entre estes centros de atendimento para compartilhar informação e tecnologias que permitam responder a incidentes.
> i) Encorajar o desenvolvimento de novas aplicações seguras e confiáveis que facilitem as transações on-line.
> j) Encorajar os países interessados para que contribuam ativamente com as atividades das Nações Unidas em curso, a fim de criar confiança e segurança na utilização das TICs.
> [grifou-se]

Assim, quando o Secretário-Geral afirmou, em 2010, a necessidade de um diploma internacional de segurança cibernética, aos moldes de um tratado de não-proliferação de armas nucleares[58], essa declaração não pode ser tomada

[58] "O mundo precisa de um tratado para se defender dos ciberataques antes que eles se transformem em uma ciberguerra ou guerra na internet, declarou neste sábado (30) no Fórum Econômico Mundial em Davos, na Suíça, o chefe da agência de telecomunicações da ONU, Hamadoun Touré.

como um posicionamento incontestável da organização internacional (tampouco da Anatel!). Por outro lado, com a atribuição recebida nas duas fases da CMSI, tampouco parece razoável afirmar a ilegitimidade de seu discurso.[59]

Possivelmente o Brasil tenha contribuído para tal posicionamento. Em 2009, o Presidente Luiz Inácio Lula da Silva recebeu da UIT o Prêmio "Dia Mundial das Telecomunicações e da Sociedade da Informação" (*World Telecommunication and Information Society Day* /WTISD), por contribuições do País para a proteção à criança no espaço cibernético (essencialmente, as promulgações das Leis nº 10.764/2003 e 11.829/2008[60], que alteraram o Estatuto da Criança e do Adolescente e aumentaram a abrangência dos tipos penais e a punição a determinadas condutas relacionadas à pedofilia na Internet).

Em seu discurso de agradecimento, o Presidente Lula ratificou o mandato da UIT para a criação de ambiente online seguro, nas linhas da CMSI:[61]

> A capacidade das telecomunicações de ultrapassar fronteiras também pode ser usada para atividades ilícitas. A Cúpula Mundial de Sociedade da Informação deu à UIT mandato para aumentar a segurança na internet.

Os ataques contra o Google, ocorridos na China segundo o próprio site de busca norte-americano, entraram na pauta de discussões do Fórum Econômico Mundial, que termina neste domingo na estação de esqui dos Alpes suíços.

Sobre o tema, o secretário-geral da União Internacional de Telecomunicações (UIT), Hamadoun Touré, disse que o risco de um conflito entre dois países através da internet aumenta a cada ano.

Com essa situação, Touré propôs um tratado no qual as partes se comprometam a não lançar um primeiro "ciberataque" contra outra.

'Uma ciberguerra seria pior que um tsunami, uma catástrofe', declarou Touré.

O acordo internacional "seria parecido com um tratado de guerra antes de uma guerra", acrescentou." *ONU pede tratado para evitar uma 'guerra na internet'* http://g1.globo.com/Noticias/Tecnologia/0,,MUL1469914-6174,00.html

[59] Essa mesma cautela deve existir ao citar relatórios e artigos encomendados a consultorias, como o artigo de referência em alguns tópicos deste texto, que ignora aos atores responsáveis pela definição dos posicionamentos de "uma UIT". Sabe-se, por exemplo, que os EUA têm grande participação na formulação de padrões de segurança na UIT e divulgação de melhores práticas, apesar de o governo americano obstar o avanço da organização nessa seara.

[60] Em resumo, essas leis ampliaram os núcleos dos tipos penais de crimes praticados contra a criança e o adolescente, tipificados no Estatuto da Criança e Adolescente (Lei nº 8.069, de 13 de julho de 1990), para incluir a produção, reprodução, direção, fotografia, filmagem, registro, venda, exposição, oferta, troca, disponibilização, transmissão, distribuição, publicação, divulgação, aquisição, posse, armazenamento, por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro, de qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

[61] UIT. *Laureate WTISD 2009 - Addresses by H.E. Luiz Inácio Lula da Silva, President of the Federative Republic of Brazil*. http://www.itu.int/wtisd/2009/award/laureates/lula-address.html

> Gostaria de felicitar o Secretário-Geral Hamandoun Touré pelo lançamento da Agenda Global de Cibersegurança.
> Para garantir a segurança na internet, precisamos unir nossos esforços de cooperação. A UIT, como agência especializada da ONU, é o lugar certo para coordenar esse esforço. No combate à pedofilia, a UIT poderia definir padrões a serem adotados por todos os países. No combate ao crime cibernético em geral, precisamos de um instrumento multilateral que estimule uma efetiva cooperação internacional.
> O desafio dos crimes cibernéticos demonstra a importância do debate sobre governança da internet. A Cúpula Mundial da Sociedade da Informação concluiu que essa governança deve ser transparente e democrática, com a participação de governos e sociedade civil. A UIT deve fazer parte desse esforço, inclusive no Fórum de Governança da Internet das Nações Unidas.
> Agradeço mais uma vez ao Secretário-Geral da UIT pela honra de receber o Prêmio Mundial das Telecomunicações e Sociedade da Informação. Vejo esse prêmio como resultado do esforço do Governo brasileiro para promover a inclusão digital e um espaço virtual democrático e seguro, sobretudo para nossas crianças e adolescentes.
> Com esse prêmio, o Governo brasileiro se sente ainda mais estimulado a continuar trabalhando, ao lado da UIT e dos demais parceiros, para construir uma sociedade da informação democrática e que promova o desenvolvimento. [grifou-se]

Suas palavras claras e fortes geraram grande expectativa na comunidade internacional de telecomunicações de que o Brasil (por extensão, a Anatel, o órgão competente para representar o País) passaria a atuar e defender com mais veemência o papel da UIT na segurança cibernética. Isso não seria visto na principal conferência da organização que ocorreria no ano seguinte.

2.1.2. Papel da UIT: Conferência de Plenipotenciários 2010 (PP-10)[62]

Entre 4 e 22 de outubro de 2010, a Conferência de Plenipotenciários 2010 (PP-10), realizada no México, tornou a discutir o mandato da UIT na segurança cibernética. Naquela ocasião, os debates ocorreram em torno

[62] O autor da pesquisa integrou a delegação brasileira à PP-10 e atuou na negociação do tema. As percepções aqui descritas, ainda que de cunho pessoal, estão registradas de modo semelhante também em Relatório de Delegação nº 80/2011-GCCBC, de 3 de maio de 2011, disponível em www.anatel.gov.br.

de dois tópicos correlacionados que veem sendo discutidos desde as Conferência de Plenipotenciários de 1998, 2002 e 2006: (i) a adoção de uma definição de "segurança cibernética", para a UIT, e (ii) o fortalecimento do papel da UIT.

Em resumo, África do Sul, Arábia Saudita, China, Irã, Síria defendiam a introdução de termos como "segurança" (Recomendação X.1141[63]) e "segurança cibernética" (Recomendação UIT-T X.800) nos atos constitutivos da UIT, o que lhe garantiria um mandato específico mais efetivo em temas afetos a conflitos no ambiente virtual. Embora aceitassem que a UIT não desempenharia papel preponderante, discordavam sobre a forma (e mesmo sobre a necessidade) de se deixar isso explícito em uma Resolução (mandato negativo) da Conferência.

Em sentido diferente, as posições de Brasil, Canadá, Estados Unidos, União Europeia coincidiram em vários aspectos, argumentando que temas como segurança e defesa nacional, crimes cibernéticos e conteúdo de comunicações estariam fora do mandato da UIT. A delegação brasileira criticou a excessiva abrangência da definição, que poderia dar margens a ingerências sobre o conteúdo de comunicações no ciberespaço (a definição proposta indica que a segurança cibernética protegeria também a totalidade de informações transmitidas ou armazenadas no ambiente cibernético[64]).

Para africanos, a PP-10 não poderia impedir que países em desenvolvimento se utilizassem da expertise da UIT em suas demandas legislativas relacionadas a crimes cibernéticos, por exemplo. Os chineses também argumentavam que o papel da UIT envolveria manter a estabilidade da rede, de modo que caberia à UIT facilitar o desenvolvimento de soluções técnicas que reduzam e reparem as vulnerabilidades da infraestrutura (mesmo nos casos de defesa nacional).

---

[63] "'Security' refers to minimization of the vulnerability of technical systems and information resources. 'Vulnerability' refers to any possibility of unauthorized access to a network or to the information it contains. A 'threat' is a potential violation of security resulting from the exploitation of vulnerability. Security also refers to a collection of systems that ensure the confidentiality of information, protect the systems or networks used to process it, and control access to them. Security encompasses the concepts of protection, confidentiality, integrity and availability"

[64] "Cybersecurity is the collection of (...) that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include (...) the totality of transmitted and/or stored information in the cyber environment..." [Grifou-se]

Ao cabo, em um texto confuso e prolixo[65], a PP-10 orientou a UIT a concentrar seus recursos e programas nas áreas de sua competência e expertise, notadamente as esferas técnicas e de desenvolvimento (capacitação e melhores práticas), que não incluem segurança e defesa nacional, crimes cibernéticos e conteúdo.[66]

A UIT segue produzindo Recomendações com padrões úteis ao gerenciamento e fruição dos recursos de telecomunicações, manuais e relatórios de melhores práticas sobre segurança cibernética. Tanto por seu mérito técnico, quanto por sua relevância política, algumas das atividades da UIT nesse tópico demandam olhar mais atento dos órgãos nacionais reguladores e formuladores de políticas de TICs.

Os itens seguintes são baseados em documentos que sugerem como um Estado deve formular suas estratégias nacionais de segurança cibernética e qual o papel do regulador nessa política, o cerne deste trabalho.

2.1.3. Sugestão de estratégia nacional da UIT

Embora os riscos, ameaças e vulnerabilidades do ciberespaço difiram bastante, a UIT defende que sejam abordados de maneira conjunta, como variáveis de um mesmo problema que coloca em xeque a confiança e a segurança no uso dessa ampla rede baseada em TICs.[67] Por essa razão, uma abordagem nacional ampla para a segurança cibernética seria fundamental.

---

[65] Res. 181 PP-10 ("Definition and terminology relating to building confidence and security in the use of ICTs") http://www.itu.int/publ/S-CONF-ACTF-2010/en

[66] Quando da aprovação da Resolução em plenária, a delegação brasileira fez ainda a seguinte declaração: "O Brasil acredita que nenhuma medida técnica, legal ou política relacionada à segurança cibernética deve dificultar ou comprometer a plena observância das normas universais, como a Declaração Universal dos Direitos Humanos. Um dos princípios para o uso e gestão da Internet no Brasil se refere à liberdade de expressão, a privacidade e os direitos humanos, reconhecendo-os como elementos essenciais à preservação de uma sociedade justa e democrática."

[67] "Until a few years ago, the most common types of malware were viruses and worms. More recently, other kinds have appeared and are widely distributed, including trojan horses, backdoors, keystroke loggers, rootkits, and spyware. Whereas spam and malware were hitherto relatively separable problems they are presently converging with the emergence of botnets. These networks of remote- controlled malware-infected computers are the origin of the majority of spam messages but they are also sustained and extended through spam." *Cf.* UIT. *ITU Study on the Financial*

Um relatório de melhores práticas do Setor de Desenvolvimento da UIT (UIT-D) sugere a preparação de uma abordagem nacional abrangente para a segurança cibernética que integre, pelo menos, cinco elementos, condizentes com a Linha de Ação C5 da CMSI:

- Formulação de uma estratégia nacional de Segurança Cibernética;
- Estabelecimento de relações de cooperação entre o Estado e o setor privado no plano nacional;
- Combate ao crime cibernético;
- Criação de capacidades nacionais para gestão de incidentes;
- Promoção da cultura nacional de Segurança Cibernética.

Como a doutrina de políticas de segurança cibernética é ainda incipiente, os atores e possíveis responsáveis são apenas parcialmente conhecidos. Não obstante, os países devem se ocupar de elaborar e implementar suas estratégias nacionais, cuja responsabilidade esteja sob os auspícios de um órgão de cúpula do Estado capaz de dialogar com os diversos setores.

Para identificar os papéis a serem desempenhados, um passo inicial seria elevar o tópico como uma política púbica nacional, paralelamente a políticas de inclusão digital e disseminação de banda larga.

Abaixo, uma distribuição primária das responsabilidades dos diversos *stakeholders*, segundo as linhas gerais de melhores práticas da UIT. Ainda que essa divisão seja superficial, não parece haver grande distinção em relação a propostas da Organização de Cooperação e Desenvolvimento Econômico (OCDE), por exemplo.[68]

Percebe-se que governo, setor privado e usuários teriam papéis complementares. Se por um lado o governo deve promover a cultura de segurança

---

Aspects of Network Security: Malware and Spam. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf>. Acesso em: 11.08.2010.

[68] Op. cit.

cibernética, cabe ao setor privado desenvolver produtos mais seguros e, ao usuário, empregar recursos de TICs de maneira responsável.[69]

Essa divisão proposta pelo artigo é particularmente útil aos reguladores do setor que pretendem sistematizar sua atuação em segurança cibernética, por serem um ente estatal cuja competência transita fundamentalmente na relação constante entre governo, setor privado e usuários.

2.1.3.1. Governo

Apenas os governos estariam em posição de liderar os esforços nacionais que englobem todos os *stakeholders*. Além de executar medidas efetivas para conter as ameaças ao ciberespaço, o governo deve também estabelecer parâmetros mínimos para o diálogo sobre segurança cibernética, em um ambiente que favoreça a identificação dos papéis e responsabilidades de cada ator.

A atuação do governo pode ser organizada nas seguintes categorias:

- Formulação de políticas públicas;
- Estabelecimento de medidas legais;
- Definição de estrutura organizacional;
- Organização e coordenação institucional; e
- Estudos, resposta e tratamento de incidentes de segurança cibernética;
- Capacitação;
- Estímulo a parcerias público-privadas e regulação setorial.

[69] *Implementation plan for the OECD guidelines for the security of information systems and networks: towards a culture of security", da Organização de Cooperação e Desenvolvimento Econômico (OCDE)*: http://www.oecd.org/dataoecd/23/11/31670189.pdf

2.1.3.2. Setor privado

Individualmente, as empresas devem adotar medidas adequadas de segurança em suas atividades. A depender da atividade empresarial, essas medidas devem ser menos ou mais rígidas. No que tange ao coletivo do setor privado, deve trabalhar junto com o governo no estabelecimento de normas, padrões, códigos de conduta, bem como na identificação e promoção de boas práticas.

2.1.3.3. Usuário

Os usuários têm um importante papel a desempenhar, adotando medidas técnicas e procedimentais de proteção preventiva. Parte das soluções técnicas mais elementares devem ser implementadas no nível direto do uso pessoal de equipamentos conectados à rede.

O despertar da sociedade civil em temas como privacidade e pedofilia na Internet trouxe à tona mais um grupo importante em prol da segurança, à medida que os impactos sociais da rede se tornaram mais evidentes. As contribuições e comentários em consultas públicas com o governo servem de material essencial para informar a atividade de formulação de políticas públicas abrangentes, de interesse não apenas de governo e empresas, mas de todo um Estado que passa a exercer novas relações em ambiente virtual.

2.1.4. O Regulador

O artigo "*Cybersecurity: The Role and Responsibilities of an Effective Regulator*" utilizado como referência neste trabalho foi, por sua vez, elaborado com base em modelos de diversos países, entre eles, Brasil (citado na abertura do *paper* como modelo de governança, com foco na delegação de competências entre múltiplos atores), Coréia do Sul, Emirados Árabes, Estados

Unidos, Estônia, Holanda, Hungria, Japão, Malásia, Nigéria, Noruega, Reino Unido, Singapura, Suécia.

A partir das pesquisas com os diversos reguladores (e homólogos), concluiu-se que há múltiplas formas possíveis para a atuação desse ente, a depender principalmente de seu mandato e status técnico-político na Administração Pública.

De maneira geral, o papel tradicional do regulador é comum à muitos países:

- Implementar arcabouço para outorgas e concessões;
- Promover competição;
- Assegurar interconexão de redes;
- Implementar mecanismos de universalização;
- Administrar espectro de radiofrequências;
- Minimizar custos decorrentes da regulação e fiscalização ao cumprimento dos serviços.

No entanto, com o tempo, seu papel teria evoluído junto com a tecnologia, a abertura de mercados à competição, o crescimento de relevância das TICs, a ampliação do objeto de atuação do regulador (de telecomunicações para TICs).[70]

Por consequência, os autores identificam que os países onde o regulador desempenha papel central na segurança cibernética são nações que abordam o tema e distribuem responsabilidades entre as instituições públicas com foco no caráter técnico e tecnológico de TICs.[71] Para tanto, o regulador cumpre também os seguintes requisitos concernentes às telecomunicações:

- É reconhecidamente uma instituição madura da Administração;
- Possui experiência técnica e industrial;

[70] *Op. cit.* p. 19-20.

[71] *Op. cit.* p. 39.

- Possui mandato e jurisdição efetivos bem definidos;
- Dispõe de recursos apropriados;
- Dispõe de instrumentos para engajamento do setor privado;
- Integra o processo de formulação de políticas sobre TICs;
- Impõe padrões técnicos obrigatórios para a indústria;
- Fiscaliza infrações relacionadas às TICs;
- Administra incidentes, riscos e crises nas comunicações;
- Promove a cultura da segurança cibernética ao consumidor.

Assim como todos os demais atores se beneficiam da troca de experiência internacional, o regulador necessariamente deve participar de plataformas que compartilhem informações sobre segurança cibernética, incluindo eventos, organizações internacionais, centros de tratamento e resposta de incidentes. A própria UIT[72] concentra muitas iniciativas e propicia ambiente para aprendizado e definições de padrões.

Há reguladores que lideram (Singapura) e que assessoram (Estados Unidos) a iniciativa nacional de segurança cibernética. A distinção entre liderar e assessorar está diretamente ligada à competência da instituição, à disponibilidade de ferramental para a implementação das políticas, à familiaridade com mecanismos de consultas públicas.

Para evitar soluções complexas que demandariam revisão de todo o marco regulatório, por exemplo, o regulador (Holanda) optou apor bordar o combate ao spam como um problema de proteção ao consumidor que gera grande impacto na infraestrutura nacional de TICs. Em última análise, spams podem ser vetores para a transmissão de BOTs, que podem levar a ataques de DDoS contra infraestruturas críticas, objetos específicos de uma política nacional eficiente.

---

[72] Entre as principais iniciativas da UIT, para as quais a Anatel tem colaborado, destacam-se: a *ITU Global Cybersecurity Agenda* (GCA), o *Cybersecurity Gateway*, a *International Multilateral Partnership Against Cyber Threats* (IMPACT), o manual *Security in telecommunications and information technology - An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications*, o relatório *Best practices for a national approach to Cybersecurity: Building blocks for organizing national Cybersecurity efforts*. Disponível em: <http://www.itu.int/cybersecurity/>. Acesso em 9.08.2010.

No que tange à esfera jurídica, reguladores podem atuar como parceiros de instituições legislativas, polícias, promotores, juízes, treinando e capacitando agentes em temas relacionados às TICs, fornecendo assistência técnica na atividade legisferante (Nigéria) ou de persecução penal de crimes cibernéticos (Malásia).

Não é comum que reguladores sejam entes da alta Administração Pública, o que dificulta a sua atuação como instituição a liderar a política nacional de segurança cibernética. No entanto, o regulador pode exercer funções de secretariado (Singapura) ou firmar termos de cooperação com outros entes públicos para exercer atividades de consultoria, assessoramento e capacitação que aprimorem a execução da atividade-fim crítica do próprio cooperado, como um Ministério do Meio Ambiente (Emirados Árabes) ou agências de inteligência.

Entre os tópicos mais sensíveis nos programas de segurança cibernética estão a detecção, investigação, análise e resposta a incidentes. Há reguladores que criaram suas Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais/ETIRs (Suécia) próprias, que participam de foros de grupos de monitoramento, como o Fórum para Grupos de Resposta a Incidentes de Segurança em Computadores/FIRST e que passaram a fazer análises de risco setorial (Singapura). Concentrar essas atividades em um único ente público, capaz de funcionar em regime de prontidão para desastres e emergência em todo um país, pode levar inclusive à redução de custos (Hungria).

Com frequência, cita-se que o usuário final é o elo mais fraco na cadeia de segurança, razão por que atividades de capacitação tendem a gerar impacto positivo na segurança cibernética. O contato direto com o consumidor pode refletir em aprimoramento da política nacional, sob a ótica do usuário. Campanhas publicitárias e programas de treinamento promovidas por reguladores em parceria com a iniciativa privada também podem apresentar bons resultados (Reino Unido).

Ao educar o consumidor, há também a possibilidade de passar a regular seu uso de modo mais enérgico, exigindo que o usuário mantenha padrões mínimos de segurança obrigatórios. Monitorado pelos provedores de serviços de

Internet, o usuário poderia ter sua conexão suspensa e ser compelido a atualizar suas soluções de segurança (Coréia).

A capacitação deve se estender não apenas a consumidores, mas também à própria comunidade técnica e acadêmica, que deve estar habilitada a tornar o ambiente online mais seguro (Coréia).

Alguns reguladores que têm capacidade de exigir a cooperação do setor privado (Estados Unidos) ou sua auto-regulamentação assim têm agido, promovendo a adoção de melhores práticas (Suíça), impondo requisitos mínimos de segurança (Estônia), fomentando pesquisas e parcerias entre governo, academia e desenvolvedores (Japão e Singapura).

O conjunto dessas práticas indica que reguladores estão se movendo em diversos sentidos, mas não há ainda consensos sobre a melhor forma de atuarem. O caso dos EUA, um dos mais ativos representantes nos trabalhos de divulgação de melhores práticas de segurança cibernética, merece destaque.

2.2. Estados Unidos da América

Por razões diversas, a segurança cibernética já está na pauta política nos Estados Unidos há vários anos. Tendo surgido em decorrência do ímpeto militar e competitivo da Guerra Fria, a ARPAnet, precursora da atual Internet, já nasceu com aspiração de recurso de comunicação útil à segurança e defesa nacional: o mote era desenvolver uma rede resiliente capaz de garantir a segurança na comunicação entre bases militares e os departamentos de pesquisa do governo americano mesmo no caso de um ataque nuclear.[73]

O objetivo do Departamento de Defesa (DoD) foi alcançado, com o desenvolvimento de protocolos como TCP/IP e a ampliação de redes de comunicação, mas o ataque nuclear aos EUA nunca se concretizou. À medida que as tensões do mundo polarizado arrefeciam, a Rede se expandiu no uso acadêmico, até se tornar o fenômeno econômico, cultural e social dos dias atuais.

[73] http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet

Mais recentemente, a retomada do embate que considera segurança e privacidade como valores opostos é geralmente associado ao ataque terrorista de 11 de setembro em Nova York e às rígidas políticas de segurança estadunidenses que se seguiram, como medidas reativas e preventivas contra ameaças terroristas (Ato Patriota). No que tange às TICs, esse país também aprovou leis que aumentam os níveis de vigilância sobre as comunicações e de poderes investigatórios de autoridades responsáveis pela aplicação da lei.[74]

2.2.1. Estratégia Nacional

Tão logo assumiu a Casa Branca, o Presidente Barack Obama determinou que especialistas em segurança nacional elaborassem em 60 (sessenta) dias um trabalho de revisão da política nacional de segurança cibernética[75],

[74] DiploFoundation. (2009). *Internet Governance Capacity Building Program 2009 – Advanced Phase on Privacy and Personal Data Protection*. Disponível em: http://campus.diplomacy.edu/lms/ClassNav.asp?IDclass=190

[75] No capítulo introdutório, pretendia-se analisar também uma definição oficial estadunidense para "segurança cibernética", mas esta não foi encontrada. Considerando que o termo vem sendo usado há mais de uma década pelo governo americano, impressiona não haver um conceito formal. Cf *Cyber security: Can the Senate make the Internet safe?*"http://blogs.techrepublic.com.com/security/?p=1276

Algumas propostas não convertidas em lei chegaram a oferecer conceitos, mas por essa mesma razão não são oficiais:

"According to H.R. 4246 'Cyber Security Information Act': cybersecurity: 'The vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United States, or that threatens public health or safety.

"According to S.I. 1901 'Cybersecurity Research and Education Act of 2002': cybersecurity: 'information assurance, including scientific, technical, management, or any other relevant disciplines required to ensure computer and network security, including, but not limited to, a discipline related to the following functions: (A) Secure System and network administration and operations; (B) Systems security engineering; (C) Information assurance systems and product acquisition; (D) Cryptography; (E) Threat and vulnerability assessment, including risk management; (F) Web security; (G) Operations of computer emergency response teams; (H) Cybersecurity training, education, and management; (I) Computer forensics; (J) Defensive information operations.

According to S.I. 1900 'Cyberterrorism Preparedness Act of 2002': cybersecurity: 'information assurance, including information security, information technology disaster recovery, and information privacy." In: PERRY, William J.; CASADO, Martin; COLEMAN, Keith; WENDLANDT, Dan. "U.S. National Cybersecurity". http://www.stanford.edu/class/msande91si/www-spr04/slides/Lecture1.pdf

incluindo planos, programas e atividades do governo. Para coordenar essa atividade, Obama indicou uma alta assessora para segurança cibernética do governo Bush, proponente de uma política agressiva de investimentos no setor.

Em 29 de maio de 2009, o presidente divulgou o relatório "*Cyberspace Policy Review – Assuring a trusted and resilient information and communication infrastructure*" (*Policy Review*)[76], cujas recomendações indicaram alguns dos passos seguintes que o governo tomaria: trabalhar em parceria com os grupos interessados, fortalecer as parcerias público-privadas, investir em pesquisa e desenvolvimento, promover a cultura de segurança cibernética desde escolas a altos escalões de governo. Por fim, salientou que permanecerá comprometido com a neutralidade de rede, promoverá a privacidade e os direitos civis e não permitirá o monitoramento de redes privadas.[77]

Os Estados Unidos já possuem certa tradição [78] em formular estratégias de segurança cibernética. Tanto a administração de Bill Clinton, em 2000[79] [80] [81], quanto a de George W. Bush, em 2002[82] e 2008, elaboraram programas com esse mote[83].

---

[76] EUA. WHITE HOUSE. *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[77] EUA. WHITE HOUSE. *Remarks by the President on securing our nation's cyber infrastructure.* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (tradução livre)

Trata-se de discurso de evidente contraposição a políticas estabelecidas pelo "USA Patriot Act" (acrônimo para "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* " ou "Ato de Unir e Fortalecer a América Providenciando Ferramentas Apropriadas Necessárias para Interceptar e Obstruir o Terrorismo") de 2001, por George W. Bush, que mitigou o direito à privacidade na comunicação eletrônica, sob o argumento de combate ao terrorismo.

"Uma das maiores inovações trazidas pela lei antiterror norteamericana localiza-se na tentativa de exercer maior controle sobre as infomações transmitidas por correio eletrônico. (...) Foram, então, desenvolvidas quatro modalidades de intervenção governamental para o controle da informação que circula diariamente pela rede mundial de computadores e por vários bancos de dados eletrônicos mantidos por empresas privadas. Essas formas de controle significam uma visível interferência nos domínios da privacidade, tal como estabelecidos em textos constitucionais." PAIXÃO, Cristiano. Dicotomias deslizantes: público e privado em tempos de terror. In: PEREIRA, Cláudia Fernanda de Oliveira (Coord). "O novo direito administrativo brasileiro: o público e o privado em debate". Belo Horizonte: Fórum, 2010. v. 2. pp. 25-26.

[78] *Timeline: The U.S. Government and Cybersecurity*. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true

[79] WHITE HOUSE. *Defending America's Cyberspace – National Plan for Information Systems Protection Version 1.0.* http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

Especificamente, o relatório da administração Obam[84] é construído sobre as bases estabelecidas pela "*Comprehensive National Cybersecurity Initiative* (CNCI)", por meio da *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (NSPD-54/HSPD-23) de janeiro de 2008, um documento confidencial [85] que apenas em julho de 2010 foi

---

[80] *Clinton Administration announces new cyber security proposals* http://articles.cnn.com/2000-07-17/politics/net.security_1_encryption-cyber-security-trap-and-trace?_s=PM:ALLPOLITICS

[81] "Jan. 2000: The Clinton administration releases its cybersecurity strategy. The document earns a cool reception from industry, which was left out of much of the drafting process. Civil liberties and privacy groups say it advocates a government-wide intrusion detection network. They also say it could dramatically expand government surveillance of the nation's communications networks. Plans for an intrusion detection network are dropped." Cf. *Timeline: The U.S. Government and Cybersecurity*. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true

[82] "The Bush administration today unveiled the nation's first homeland and cybersecurity strategy, which calls for an unprecedented partnership between federal, state and local governments and the private sector to battle terrorism. The strategy was released at a White House-sponsored briefing in Washington. The cybersecurity portion of the strategy, the National Plan for Protecting Cyberspace, builds upon work started by the Clinton administration to enlist the help of the private sector, which owns and operates the bulk of the nation's critical infrastructure." Cf. *Cybersecurity strategy released*. http://www.computerworld.com/s/article/72753/Cybersecurity_strategy_released. O Plano "National Strategy to Secure Cyberspace" pode ser encontrado em http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf"

[83] Uma demonstração da intensa atividade legislativa estadunidense são os mais de 30 (trinta) atos introduzidos no Congresso entre 2009 e 2010, versando sobre tópicos como: Organizational Responsibilities; Compliance and Accountability; Data Accountability, Personal Data Privacy, Data Breach Handling and Identity Theft; Cybersecurity Education, Research and Development and Grants; Critical Electric Infrastructure Protection and Vulnerability Analysis; International Cooperation and Addressing Cybercrime; Procurement, Acquisition and Supply Chain Integrity. Cf. HATHAWAY, Melissa E. *Cybersecurity: The U.S. Legislative Agenda*. http://belfercenter.ksg.harvard.edu/files/legislative-landscape-publish-final.pdf

[84] Em oportunidade anterior à eleição do presidente Barack Obama, Schneider elaborou artigo "*Memo to Next President [of USA]: How to Get Cybersecurity Right*", onde sugeria três aspectos políticos principais sobre o tema, "coisas que somente o governo pode fazer" para aprimorar a segurança da informação e toda a segurança nacional, de maneira ampla: "Um, use seu imenso poder de compra para aprimorar a segurança de produtos e serviços comercias. (…) Dois, legisle sobre resultados, não sobre metodologias. (…) Três, invista amplamente em pesquisa." In: SCHNEIDER, Bruce. *Memo to Next President: How to Get Cybersecurity Right*. Disponível em: http://www.schneier.com/essay-231.html.

[85] "The Bush administration's newly created National Cyber Security Center remains shrouded in secrecy, with officials refusing to release information about its budget, what contractors will run it, and how its mission relates to Internet surveillance. In correspondence with the U.S. Senate posted on Thursday, the Bush administration said it would not provide that information publicly. An 18-page, partially redacted letter from DHS said that disclosure could affect "the conduct of federal programs, or other programs or operations essential to the interests of our nation." Cf. *DHS stays mum on new 'Cyber Security' center*: http://news.cnet.com/8301-13578_3-10004266-38.html#ixzz1AnH2qWV5

parcialmente revelado pelo governo[86], após pressão pública, particularmente de grupos defensores de direitos de privacidade[87].

A resultante da NSPD-54/HSPD-23 e das recomendações do relatório foi sintetizada pela Casa Branca nas seguintes iniciativas:

> Iniciativa nº 1. Gerenciar a Rede Corporativa Federal como uma única rede corporativa com *Trusted Internet Connections* (Conexões de Internet Confiáveis);
> Iniciativa nº 2. Lançar um sistema de sensores para detecção de intrusos ao longo da Rede Corporativa;
> Iniciativa nº 3. Buscar o lançamento de sistemas de prevenção de intrusos ao longo da rede federal;
> Iniciativa nº 4: Coordenar e redirecionar esforços de pesquisa e desenvolvimento;
> Iniciativa nº 5. Conectar centros de operações atuais para aumentar a consciência situacional;
> Iniciativa nº 6. Desenvolver e implementar um plano de contrainteligência cibernética que abranja todo o governo.
> Iniciativa nº 7. Aumentar a segurança de nossas redes restritas;
> Iniciativa nº 8. Expandir a educação cibernética;
> Iniciativa nº 9. Definir e desenvolver tecnologias, estratégias e programas de ponta contínuos;
> Iniciativa nº 10. Definir e desenvolver programas e estratégias de intimidação contínuos;
> Iniciativa nº 11. Desenvolver uma abordagem de múltiplas frentes para gestão de risco de cadeias de fornecimento global;
> Iniciativa nº 12. Definir o papel federal para estender a segurança cibernética às searas de infraestrutura críticas.

A coordenação dessas amplas iniciativas gerou um ambiente de disputa sobre quem, na Administração Pública, deveria liderar a execução da estratégia nacional[88]. Seguindo a primeira recomendação[89] da *Policy Review*,

---

[86] EUA. WHITE HOUSE. *The Comprehensive National Cybersecurity Initiative*. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[87] "The Obama administration on Tuesday gave the public a peek at the Bush administration's classified plan to secure the nation's computer systems, but the newly revealed list of broad goals provided few surprises and key provisions remain secret.

The decision to publish a summary of the cyber initiative on the White House blog came just a month after the Washington-based Electronic Privacy Information Center filed a lawsuit in federal court seeking release of the computer security document.

Privacy advocates and other groups have long fought to get the Bush cyber plan made public, concerned that it discussed surveillance activities and Internet traffic monitoring by intelligence agencies that could violate Americans' personal privacy." Cf. *White House Reveals Secret Cybersecurity Plan Developed Under Bush Administration*. http://www.huffingtonpost.com/2010/03/02/nspd54-secret-cybersecuri_n_483103.html

[88] "The National Security Agency has been campaigning to lead the government's rapidly growing cybersecurity programs, raising privacy and civil liberties concerns among some officials who fear

criou-se o cargo de Coordenador de Segurança Cibernética na Casa Branca, um assessor direto do Presidente responsável pela articulação global da política de segurança cibernética.

A CNCI é fundamentada no compartilhamento de responsabilidades entre inúmeros atores, uns mais nitidamente inclinados à formulação estratégica, segurança nacional, inteligência (*National Security Agency*/NSA, *Department of Defense*/DoD, *Department of Homeland Security* /DHS, *Departament of Justice*/DoJ, *Central Intelligence Agency*/CIA), outros à pesquisa e desenvolvimento (*National Science and Technology Council*/NSTC, *National Science Foundation*/NSF, *United States Computer Emergency Readiness Team*/US-CERT academia, setor privado) e alguns à regulação setorial (FCC, *National Telecommunications and Information Administration*/NTIA, *Federal Trade Commission*/FTC, *Department of Energy*/DoE).

As iniciativas voltadas para prevenção de intrusos à rede federal, pesquisa e desenvolvimento, tecnologias de ponta, gestão de risco de cadeias de fornecimento, proteção de infraestrutura crítica parecem ter inspirado as atividades que vêm sendo empreendidas pela FCC, com foco em comunicações.

2.2.2. O regulador

FCC e UIT mereceram referência destacada na *Policy Review* de Obama, em Anexo que detalha a evolução da atividade regulatória do Estado sobre o setor de telecomunicações.[90] Como já afirmado, com prestígio perante a

---

that the move could give the spy agency too much control over government computer networks. (...) The security agency's interest in taking over the dominant role has met resistance, including the resignation of the Homeland Security Department official who was until last month in charge of coordinating cybersecurity efforts throughout the government." Cf. *Control of Cybersecurity Becomes Divisive Issue*. http://www.nytimes.com/2009/04/17/us/politics/17cyber.html

[89] "1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy." Cf. *Cyberspace Policy Review.* Op.cit.

[90] "Appendix C: Growth of Modern Communications Technology in the United States and Development of Supporting Legal and Regulatory Frameworks." Op.cit.

Casa Branca [91], a FCC seria possivelmente uma instituição regulatória que satisfaria os requisitos enunciadas pelo artigo da UIT para que reguladores desempenhem papel relevante em políticas de segurança cibernética.

Talvez por capacidade técnica e status político reconhecidos, a FCC atua como o agente central na elaboração e execução do Plano Nacional de Banda Larga (PNBL) estadunidense, conforme determinação de lei que estabeleceu o pacote de estímulos para recuperação da economia americana pós (*American Recovery and Reinvestment Act of 2009*)[92] que destinou 10,5 bilhões de dólares para gastos federais com "comunicações, informação e tecnologias de segurança".

O PNBL apresentado ao Senado em março de 2010, identificou o potencial da banda larga para o aprimoramento da segurança nacional dos EUA e caberia ao regulador a promoção da segurança cibernética e a proteção da infraestrutura crítica de banda larga. Para isso, a FCC deveria[93]:

- Lançar um plano (*roadmap*) da segurança cibernética;
- Estender requisitos de registro de interrupções sistêmicas aos provedores de serviços de banda larga;
- Criar um regime de certificação voluntária de segurança cibernética;
- Com o DHS, criar um sistema de repositório de informações sobre segurança cibernética;
- Expandir seu alcance comunitário e participação internacional;

---

[91] "For Senator Barack Obama's 2008 Presidential Campaign, Genachowski was Chairman of the Technology, Media and Telecommunications Policy Working Group, which created the Obama Technology and Innovation Plan. He also advised and guided the Campaign's innovative use of technology and the Internet for grassroots engagement and participation.

After the November election, he co-led the Technology, Innovation, and Government Reform Group for President-Elect Obama's Transition Team. On January 12, 2009, several news outlets reported that Genachowski would be President-Elect Obama's choice to head the FCC. This was confirmed by a press release on March 3, 2009." In: WIKIPEDIA. *Julius Genachowski*. http://en.wikipedia.org/wiki/Julius_Genachowski

[92] EUA. *Recovery.gov – Track the money*. http://www.recovery.gov/Pages/default.aspx

[93] EUA. *Connecing America: The National Broadband Plan*. 2010. Disponível em: <http://www.broadband.gov/plan/16-public-safety/#r16>. Acesso em: 12/08/2010.

- Averiguar a resiliência e a prontidão de redes;
- Com o *National Communications System*, criar acesso a redes de prioridade e roteamento para comunicações de banda larga;
- Averiguar a resiliência e a confiabilidade das redes de comunicações de banda larga.

Desde abril de 2010, três consultas públicas foram lançadas pelo "*Public Safety and Homeland Security Bureau*" (Bureau de Segurança Nacional) da FCC[94], com o intuito de receber contribuições sobre (i) a resiliência das redes de banda larga, (ii) o impacto de um regime de certificação voluntária de segurança cibernética e (iii) um eventual plano (*roadmap*) de segurança cibernética.[95] Embora a conclusão dos trabalhos ainda não tenha sido apresentada, estão disponíveis algumas das respostas do setor.

2.2.2.1. Resiliência das redes de banda larga[96]

Apesar de as redes de banda larga serem tidas como resilientes, haveria fragilidades nas pontas. A consulta solicita comentários sobre os níveis de resiliência e redundância nas redes de banda larga e sua capacidade de sobreviver a crises e danos severos.

---

[94] "One means by which the FCC has previously sought to address cyber security has been through the Network Reliability and Interoperability Council (NRIC), a former Federal Advisory Committee composed of private sector representatives that cataloged proven operational best practices for carrying out network engineering, monitoring, and maintenance functions.[16] The NRIC has been superseded by the Communications Security, Reliability, And Interoperability Council (CSRIC), but NRIC cyber security best practices remain available on PSHSB's website and are increasingly relevant. NRIC's work on cyber security was conducted by leading network operators from the communications sector and resulted in over 200 best practices to help service providers secure their networks against accidental events and criminal activities. NRIC cyber security best practices can be categorized into four basic areas: (1) updating software; (2) secure equipment management; (3) intrusion prevention and detection; and (4) intrusion analysis and response.

As the number of best practices concerning cyber security would indicate, the potential for harm to computer and communications systems due to cyber security attacks is immense. As a result, cyber security is a rapidly evolving and growing interest within the critical infrastructure community and within the FCC." http://www.fcc.gov/pshs/techtopics/techtopics20.html

[95] http://www.cybertelecom.org/security/fcc.htm

[96] http://fjallfoss.fcc.gov/ecfs/comment/view?id=6015650358

Para tanto, a FCC procurou conhecer (i) os principais aspectos de falha na arquitetura das redes de banda larga, (ii) as medidas que provedores de banda larga já implementam, (iii) as soluções de melhores práticas mais difundidas, (iv) a necessidade de o tráfego de agências de primeiros socorros ser priorizado em situações de crise.

2.2.2.2. Certificação voluntária[97]

Os objetivos do programa seriam (i) aumentar a segurança da infraestrutura das comunicações nos EUA; (ii) promover uma cultural mais vigilante ao longo da cadeia de mercado para serviços de comunicações; (iii) oferecer aos consumidores e usuários finais informações mais completas sobre as práticas de segurança de seus fornecedores.

A FCC buscava contribuições dos *stakeholders* sobre custos e benefícios; incentivos aos fornecedores para aumentarem seus níveis de segurança; a logística, critérios, autorizações e validade de certificação.

2.2.2.3. Plano (“*roadmap*”) de segurança cibernética[98]

O programa pretende (i) identificar vulnerabilidades de redes e usuários finais de comunicações, (ii) com o fito de desenvolver medidas e soluções de preparação e resposta a ameaças e ataques cibernéticos, em coordenação com outros entes da Administração federal. Tratar-se-ia de um plano de curto prazo, com marcos predeterminados para a FCC lidar com tais ameaças.

A FCC estava interessada em contribuições sobre (i) as principais vulnerabilidades, (ii) como abordá-las, (iii) o papel da FCC, (iv) que as medidas (caso haja alguma) que a FCC deveria tomar, (v) como a FCC deve interagir com outros entes de governo.

---

[97] http://fjallfoss.fcc.gov/ecfs/comment/view?id=6015650380

[98] http://fjallfoss.fcc.gov/ecfs/document/view?id=7020701500

2.2.2.4. Respostas às consultas públicas da FCC[99]

Responderam às consulta operadoras (AT&T, Verizon, Sprint Nextel, Comcast), associações (US Telecom Association, CTIA, National Cable & Telecommunications Association, National Telecommunications Cooperative Associatioin), fabricantes (Cisco, Microsoft, Qualcomm), representantes do setor de energia (DTE Energy, Edison Electric Institute, American Petroleum Institute), centros de estudos.

2.2.2.4.1. Argumentos favoráveis às intenções da FCC

- Do setor financeiro, energético (eletricidade e petróleo) e centros de estudo;
- Deve educar consumidores e se coordenar com outras agências;
- O caráter voluntário da certificação não seria real. À medida que algumas empresas acatassem tal certificado, as demais se sentiriam compelidas a segui-las, particularmente se a certificação da FCC passar a ser exigida em alguma situação (compras governamentais, por exemplo);
- Já haveria iniciativas de certificação disponíveis no mercado, como ISO e NIST;
- Demonstraram interesse no incremento da resiliência das redes, particularmente com a utilização de *smart grids*, que dependerão de capacidade de comunicação robusta;
- Querem espectro para operar *smart grids* de maneira adequada;

[99] http://fjallfoss.fcc.gov/ecfs/proceeding/view?name=10-92 ; http://fjallfoss.fcc.gov/ecfs/proceeding/view?name=10-93; http://fjallfoss.fcc.gov/ecfs/proceeding/view?name=10-146

- Com a dependência das atividades econômica e financeira por capacidades de comunicações, as soluções de melhor esforço já não seriam suficientes;
- A FCC deve estimular que provedores forneçam informações sobre interrupções em sua rede de maneira obrigatória (sobre resposta e tratamento de incidentes). Os relatórios fornecidos hoje são voluntários e não revelam o retrato realista do estado das redes;
- FCC deve estimular provedores de banda larga a adotar soluções de monitoramento do estado da rede, quando incidentes de rede significativos fossem identificados, os provedores deveriam notificar a Comissão para evitar prejuízos ao longo da cadeia;
- O *roadmap* deve destacar e permitir a flexibilidade e agilidade na troca de informações entre operadoras;
- A formulação do *roadmap* deve incluir entes públicos, indústria, operadoras, especialistas, que desenvolveriam melhores práticas;
- A FCC poderia iniciar suas atividades primordialmente com provedores de serviços de Internet (ISPs) que estão em pontos estratégicos da rede, que, porque carregam todo o tráfego de entrada e saída seus consumidores, podem contribuir bastante com soluções de mitigação de *malwares*;
- ISPs necessitarão fazer um balanço sobre soluções que garantam a segurança e privacidade;
- Podem ser oferecidos incentivos como selos de qualidade, financiamento, limitar a responsabilização de provedores.

2.2.2.4.2. Argumentos contrários às intenções da FCC

- A FCC não teria competência tão clara para desenvolver essas iniciativas (evidenciado pelo caso Comcast);
- Em todas as consultas, afirmaram que as iniciativas da FCC obstariam a inovação e desenvolvimento característicos dos serviços de Internet;
- Diversos entes de governo e associações privadas já desempenham atividades sobre segurança cibernética, razão por que FCC deveria evitar duplicação de esforços (Casa Branca, DHS, FBI, CIA, CERT/CC, IETF, FIRST);
- Deve haver política unificada de governo, para isso a FCC deve trabalhar em conjunto com os demais entes de governo, para evitar duplicação de esforços;
- As parcerias público-privadas (PPPs) seriam o caminho ideal para a condução de esforços de segurança cibernética, inclusive troca de informações;
- Afirmaram que as redes de banda larga já seriam resilientes em níveis bastante satisfatórios, que as redes responderam muito bem a cenários de desastres mais significativos (11 Setembro, Furação Katrina) e que incidentes mais graves seriam pontuais;
- O *Domain Name System Security Extensions* (DNSSEC) estaria avançando na ICANN;
- As empresas já investiriam pesado em segurança e resiliência de suas redes, o que as torna robustas, resilientes e seguras;
- A consulta sobre certificação estaria baseada em pressupostos falsos. Haveria também incentivos de mercado para que fornecedores implementem medidas de segurança.

Grandes empresas e clientes governamentais já estariam bem informados sobre políticas de segurança cibernética, o que acarreta inclusive perda de clientes. Com isso, os provedores com as melhores soluções de segurança apresentam resultados favoráveis no mercado aberto;

- A ampla competição entre AT&T, IBM, British Telecom, Orange, Symantec, T-Systems, Tata Communications, Verizon e Telefonica Multinational Solutions promove a inovação e eficiência do mercado, dispensando a implementação de política de eventual política de certificação;
- FCC deve levantar perguntas básicas de AIR sobre custos e benefícios do programa, existência de externalidades e assimetrias de informação que inviabilizem o mercado definir o nível adequado de segurança e certificação;
- Um programa de certificação poderia gerar descompassos com a evolução tecnológica e o setor poderia apenas oferecer os requisitos mínimos colocados pela FCC, sem contudo garantir a eficácia de seus objetivos;
- Um programa de certificação poderia gerar descompassos com a evolução tecnológica e o setor poderia apenas oferecer os requisitos mínimos colocados pela FCC, sem contudo garantir a eficácia de seus objetivos;
- Países que não se balizaram por PPPs, adoção de padrões internacionais e melhores práticas tendem a enfrentar problemas de interoperabilidade e segurança;
- IPS podem não perceber incentivos para isso: pode ser caro e não refletir em lucros. Como muitas das soluções são caras e baseadas em *deep packet inspection*, implicaria compromissos e responsabilidades sobre a privacidade da informação trafegada.

2.2.2.5. Lições das consultas públicas da FCC

A reação às consultas é conservadora, possivelmente porque a maioria é apresentada pela iniciativa privada, que se vê ameaçada com a possibilidade de novas imposições sobre suas atividades.

Seria natural esperar tal posicionamento de empresas como AT&T, Cisco, T-Mobile e associações classistas como *National Cable & Telecommunications Association* (NCTA), *United States Telecom Association* (USTelecom) e *CTIA – Wireless Association*, relacionadas à indústria e provedores de telecomunicações. Em outro sentido, organizações certificadoras (também esperado) e Academia ofereceram comentários mais favoráveis à intervenção regulatória.

Parece razoável que não haja duplicação de esforços em âmbito nacional, que a atuação do regulador seja pautada por uma ampla estratégia nacional e também que as ações da FCC sejam precedidas de análise de impacto regulatório, que não foram objeto desta pesquisa e que podem ser explorados em próxima oportunidade.

3. UMA POLÍTICA NACIONAL DE SEGURANÇA CIBERNÉTICA E A ANATEL

O Brasil está empenhado em identificar o papel dos atores interessados em segurança cibernética. O primeiro passo, reconhecimento do problema, já foi dado, o momento é de desenvolvimento de mecanismo para abordá-lo. Embora não se conheça ainda o nível de coordenação ótima entre todos os atores interessados, o País já traça as linhas iniciais de sua estratégia nacional.[100]

Este trabalho objetiva identificar especificamente o papel que a Anatel teria a desempenhar como *stakeholder* em uma política nacional de segurança cibernética. Ao cabo, com base nas fases anteriores, são oferecidas recomendações e propostas sobre políticas para a segurança cibernética no Brasil, particularmente, no que tange à atuação do órgão regulador de telecomunicações.

3.1. Os formuladores de uma estratégia nacional

3.1.1. Estratégia Nacional de Defesa (END)

Em 18 de dezembro de 2008, por meio do Decreto nº 6.703, o senhor Presidente da República aprovou a Estratégia Nacional de Defesa. A partir dela, "[os] órgãos e entidades da administração pública federal deverão considerar, em seus planejamentos, ações que concorram para fortalecer a Defesa Nacional." (art. 2º).

A Estratégia Nacional de Defesa identifica três setores de importância estratégica para a defesa nacional: o espacial, o cibernético e o

[100] BRASIL. PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. *Livro verde: segurança cibernética no Brasil*. (org. Claudia Canongia e Raphael Mandarino Junior). Brasília: GSIPR/SE/DSIC, 2010. p. 11

nuclear. Em seguida, o Decreto enuncia ações estratégicas que orientam a END, entre elas[101]:

i. Infraestrutura: "Compatibilizar os atuais esforços governamentais de aceleração do crescimento com as necessidades da Defesa Nacional."

> *1. O Ministério da Defesa, em coordenação com a Secretaria de Assuntos Estratégicos da Presidência da República proporá aos ministérios competentes as iniciativas necessárias ao desenvolvimento da infraestrutura de energia, transporte e comunicações de interesse da defesa, de acordo com os planejamentos estratégicos de emprego das Forças.*

ii. Segurança Nacional: "Todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase sobre:"

> *- as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR);*
>
> *- o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI-PR;*

[101] Trechos do Decreto nº 6.703/2008, de 18 de dezembro de 2008. Grifou-se.

Embora a Estratégia Nacional de Defesa esteja em seu bojo voltada às Forças Armadas, é precisamente seu caráter militar que expõe a magnitude que a segurança cibernética adquire no Brasil.

No que tange ao setor de telecomunicações, que disponibiliza grande parte da infraestrutura de rede essencial à subsistência da Sociedade da Informação, a END corrobora que o Ministério das Comunicações (MC) e a Anatel, no desempenho de suas atribuições, atuem de maneira a contribuir para a segurança e a manutenção do ciberespaço, em prol do desenvolvimento socioeconômico e da soberania do País. E assim seriam convidados a atuar, segundo suas competências.

3.1.2. Câmara de Relações Exteriores e Defesa Nacional (CREDEN)

A Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo[102], é responsável por formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do governo federal, em atividades pertinentes à segurança para as infraestruturas críticas (incluindo serviços), segurança da informação e segurança cibernética.

Ao analisar a recente ampliação da finalidade e composição da CREDEN, que passou a abarcar também o Ministério do Meio Ambiente (MMA) e o Ministério da Ciência e Tecnologia (MCT), por exemplo, conjugando-se com o enfoque em comunicações da END, percebe-se espaço para a atuação efetiva do MC.

Em outubro de 2008, o GSI apresentou à CREDEN um esboço dos atores interessados na segurança cibernética, oportunidade em que o Ministério das Comunicações participou como convidado. Tendo identificado alguns dos agentes públicos que, de diversas maneiras, seriam interessados em segurança cibernética, o Gabinete indicou aos dez ministérios presentes à reunião por que

---

[102] "Órgão que tem por finalidade pronunciar-se sobre questões relevantes apresentadas pelo Estado brasileiro, incluída a estabilidade das instituições e problemas emergentes, de grave complexidade e implicações sociais." Essencialmente, integram-no Ministérios e Secretarias Especiais. http://www.presidencia.gov.br/estrutura-da-presidencia/orgaos-de-assessoramento-imediato

muitos não participariam do cerne da elaboração da Estratégia Nacional de Segurança Cibernética: seriam tantos os órgãos, que seria impossível coordená-los.

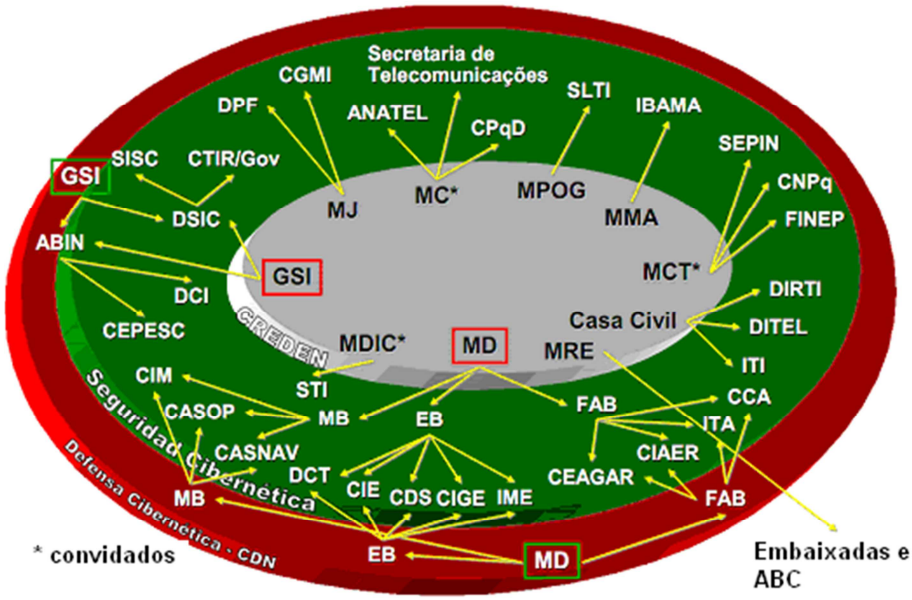


Figura 2: Segurança do ciberespaço brasileiro[103] (Fonte: Mandarino Jr.)

Um ano mais tarde, em setembro de 2009, por meio da Portaria nº 45, o GSI institui o Grupo Técnico de Segurança Cibernética (GT SEG CIBER), que se reporta diretamente à CREDEN.

Pela composição do Grupo Técnico[104], cujo objetivo é "propor diretrizes e estratégias para a segurança cibernética, no âmbito da Administração Pública Federal", somando-se às definições estabelecidas, percebe-se que o País reserva à segurança cibernética o viés da segurança e defesa nacional.

Ainda sob a CREDEN, paralelamente ao GT SEG CIBER, cabe ao Ministério das Comunicações, juntamente com a Anatel, integrar Grupo Técnico de Segurança de Infraestruturas Críticas de Telecomunicações (GTSIC –

[103] MANDARINO Jr., Raphael. *La seguridad cibernética en el Gobierno de Brasil*. http://www.youtube.com/watch?v=qVAhMxwJFEE; http://www.arcert.gov.ar/10_aniv/presentaciones/la_seguridad_cibernetica_en_%20el_gobierno_%20de_brasil.pdf (tradução livre).

[104] Integrantes do GT SEG CIB: GSI, Ministério da Justiça, Ministério da Defesa, Ministério das Relações Exteriores, Comando da Marinha, Comando do Exército, Comando da Aeronáutica.

Telecom)[105], para propor a implementação de medidas e ações relacionadas à segurança das infraestruturas críticas, com foco em radiodifusões, telecomunicações e serviços postais.

As demais áreas prioritárias de infraestruturas críticas (energia, transporte, água e finanças) também mereceram a criação de GTSICs próprios,[106] cada qual responsável por desenvolver seus planos setoriais específicos.

3.1.3. Comitê Gestor de Segurança da Informação (CGSI)

Como formulador de políticas de segurança da informação, o MC integra formalmente, no âmbito do Conselho de Defesa Nacional[107], o Comitê Gestor de Segurança da Informação (CGSI)[108], que tem função de assessorar na execução da Política de Segurança da Informação (PSI) nos órgãos e nas entidades da Administração Pública Federal, nos termos do Decreto nº 3.505/2000.

O foco da PSI é a atividade interna dessas instituições, que devem incorporar práticas de segurança da informação em seu âmbito administrativo, com estímulos também a uma indústria nacional que elimine a dependência de

---

[105]Embora denominado "GTSIC – Telecom", melhor seria designá-lo "GTSIC – Comunicações", em razão de seu escopo mais amplo. *Cf.* GSI. Portaria Interministerial nº 16 – GSIPR/CH, de 18 de julho de 2008. http://www.gsi.gov.br/infraestruturas-criticas/Port%20Interm%2016%20-%2018%20Jul%2008%20GTSIC%20Telecom.pdf

[106] GSI. Portaria nº 2, de 8 de fevereiro de 2008. http://www.gsi.gov.br/infraestruturas-criticas/Port%202%20-%2008%20Fev%2008%20GTSIC.pdf

[107] "Previsto na Constituição, é órgão de consulta da Presidenta da República nos assuntos relacionados com a soberania nacional e a defesa do Estado democrático, tendo como Secretário Executivo o Chefe do GSI. Compete ao Conselho opinar nas hipóteses de declaração de guerra e de celebração de paz; sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal; propor os critérios e condições de utilização das áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo." http://www.presidencia.gov.br/estrutura-da-presidencia/orgaos-de-consulta

[108] Integrantes do CGSI: Ministério da Justiça, Ministério da Defesa, Ministério das Relações Exteriores; Ministério da Fazenda; Ministério da Previdência e Assistência Social; da Saúde; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Ministério das Comunicações; Ministério da Ciência e Tecnologia; Casa Civil da Presidência da República; GSI, Secretaria de Comunicação de Governo e Gestão Estratégica da Presidência da República, Ministério de Minas e Energia; Controladoria-Geral da União; e Advocacia-Geral da União. Cf. Decreto nº 3.305/2000. http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm

atores externos na cadeia de sistemas de informação. Para tanto, pode, inclusive, estabelecer normas sobre Política Nacional de Telecomunicações voltadas à Defesa Nacional.

O Decreto que instituiu a PSI oferece uma definição de "Segurança da Informação"[109] próxima da de "Segurança Cibernética"[110] do Grupo Técnico de Segurança Cibernética, mas que com esta não se confunde. A primeira faz referência principalmente a seu objeto ("segurança dos sistemas de informação"), ao passo que a segunda se desenvolve em torno de sua finalidade ("assegurar a existência e a continuidade da Sociedade da Informação de uma Nação").

No âmbito do CGSI, a Portaria nº 34/2009/CDN/SE criou o Grupo de Trabalho de Segurança de Infraestruturas Críticas da Informação (GTSICI) para estudo e análise de matérias relacionadas à IEC. A mesma ausência sentida no GT SEG CIBER, tampouco o Ministério das Comunicações integra tal Grupo de Trabalho.

Ao conhecer a composição e funções de mais esse Grupo, cogita-se haveria espaço técnico para a participação permanente do MC, que agregaria valor aos trabalhos desenvolvidos também por Ministério da Saúde, Ministério da Ciência e Tecnologia, CAIXA, PETROBRAS, DATAPREV.[111]

---

[109] "Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento." (art. 2º, II, Decreto nº 3.305/2000)

[110] "Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas." (art. 2ª, GSI. Portaria nº 45, de 8 de setembro de 2009).

[111] Integrantes do GTSIC: GSI, Casa Civil, Ministério da Defesa, Ministério da Saúde, Ministério da Ciência e Tecnologia, Ministério do Planejamento, Orçamento e Gestão, Ministério das Relações Exteriores, Banco Central do Brasil, Banco do Brasil, Caixa Econômica Federal, SERPRO, PETROBRAS, DATAPREV.

3.1.4. A atuação formal de órgãos do setor de comunicações

Como visto, o Ministério das Comunicações, a quem cabe a elaboração e o cumprimento das políticas públicas do setor de comunicações, atua apenas tangencialmente no processo formal de formulação da política nacional de segurança cibernética. Sob o viés da regulamentação, há indicativos de que o setor de comunicações estaria sub-representado na atividade de cúpula.

Seguindo a metodologia desta pesquisa, limitada essencialmente a documentos públicos disponíveis na Internet, não se identificou a razão para essa arquitetura:

- No Conselho de Governo, o MC não integra a CREDEN, participa do *Grupo Técnico* de Segurança de Infraestruturas Críticas (GTSIC/CREDEN), mas não participa do *Grupo Técnico* de Segurança Cibernética (GT SEG CIBER), conforme Anexo I;
- no Conselho de Defesa Nacional, o MC integra o CGSI, mas não participa do *Grupo de Trabalho* de Segurança de Infraestruturas Críticas da Informação (GTSICI/CGSI), conforme Anexo II.

Seguindo a metodologia da pesquisa, a aparente ausência de MC (e Anatel) nessas atividades sugere contradição à luz da expressiva manifestação política do Presidente Lula em favor da atuação da UIT na segurança cibernética, em 2009, quando recebeu o Prêmio WTISD[112], gerando riscos de assimetria nos posicionamentos brasileiro no âmbito internacional seriam menores.

3.2. As linhas de uma possível política nacional

Se por um lado nota-se a atuação limitada dos órgãos de comunicação na estrutura de governança da segurança cibernética no Brasil,

[112] Vide 2.1.1

vários pontos da política nacional nascente merecem destaque. Mormente pelo GSI, tem-se produzido material, realizado eventos, capacitado mão de obra e estimulado a participação da comunidade especializada.

Em fins de 2010, o GT SEG CIBER apresentou seu "Livro Verde: Segurança Cibernética no Brasil". Como dita a prática europeia, o "livro verde" é mero relatório de governo com propostas não vinculantes, mas que visam a possível modificação ou elaboração de lei sobre o tema em pauta. Da mesma maneira, abre espaço para que especialistas contribuam para a discussão, com vistas à edição de um possível "livro branco". Ou seja, embora o País não conte ainda com uma política estabelecida, ela estaria a caminho.

À semelhança da *Policy Review* de Obama, UIT e FCC também mereceram citações no livro brasileiro, que faz referência ainda à atuação da Citel. No documento, introduz-se um projeto de futuro para a segurança cibernética no Brasil e reinterpreta recomendações da Organização de Cooperação e Desenvolvimento Econômico (OCDE), originalmente desenhadas para indicar competências essenciais para a proteção de infraestruturas críticas:

- Definir a política e normas específicas, com objetivos claros, no âmbito do mais alto nível de governo;
- Promover a cultura da segurança cibernética; [113]
- Promover mútua cooperação entre os stakeholders;
- Atuar com transparência;
- Rever sistematicamente a política, normas e marcos legais;
- Estreitar relações com o setor privado, por meio de PPPs;
- Estimular a inovação, via pesquisa e desenvolvimento

[113] O professor Yochai Benkler argumenta que a melhor abordagem para a segurança cibernética não seria criar super barreiras cibernéticas, mas garantir a sustentabilidade do sistema por meio de esforços compartilhados, à semelhança das soluções de compartilhamento música. O modelo de compartilhamento de música apresentaria características estratégicas a serem transladas para a segurança: capacidade de redundância, diversidade geográfica e topológica, capacidade de auto-organização e autocura. De sua tese, pode-se depreender que o benefício de segurança de um usuário implicaria beneficiar a sobrevivência de toda a rede, de modo que a promoção da cultura de segurança cibernética pode de fato ser uma proposta de grande impacto. Cf. GRADY, M.; PARISI, F. *The Law and Economics of Cybersecurity: An Introduction*. Cambridge University Press: 2006. http://www.law.gmu.edu/faculty/papers/docs/04-54.pdf

- Promover a cooperação bilateral e multilateral.

Identificaram-se oportunidades, desafios e diretrizes nos vetores propostos, condizentes com os modelos propostos neste trabalho, destacando-se os seguintes imperativos:

a) Político Estratégico: caracterizar a segurança cibernética como alta prioridade; lançar, no curto prazo, a Política Nacional de Segurança Cibernética; criar órgão central para a macrocoordenação dessa política; estabelecer programas de cooperação entre governo, sociedade, comunidade internacional; desenvolver arcabouço conceitual;

b) Econômico: elaborar e promover a regulação do mercado, no médio e longo prazo, por meio da adoção de padrões técnicos, modelos de gestão, de acompanhamento e de auditoria da segurança cibernética; estimular parcerias com o setor privado;

c) Social e ambiental: promover a cultura de segurança cibernética em redes sociais; defender os direitos de privacidade;

d) Educação: desenvolver programa nacional de capacitação interdisciplinar; desenvolver programa de conscientização nacional;

e) Marco legal: colaborar para a construção e atualização do marco nacional e internacional; protagonizar a articulação e elaboração de Convenção global sobre o crime cibernético, no âmbito da ONU;

f) Ciência, Tecnologia e Inovação: fortalecer pesquisa e desenvolvimento; articular a aplicação de recursos do Funttel para o desenvolvimento continuado de CT&I do setor cibernético, especialmente no que tange à segurança cibernética;

g) Cooperação internacional: promover a cooperação técnica, em diversos níveis, visando à troca de experiências e fortalecimento da estratégia nacional; institucionalizar a autoridade nacional de segurança; promover visão alinhada e consensada entre os atores-chave atuantes na segurança cibernética, visando à definição de posicionamento estratégico do país, no tema, no âmbito internacional;

h) Segurança das infraestruturas críticas: lançar a Política Nacional de Segurança das Infraestruturas Críticas; conhecer o grau de vulnerabilidade do país em relação aos seus sistemas de informação e infraestruturas críticas de informação; elaborar e/ou adaptar metodologias para avaliação de risco e continuidade de negócio em segurança cibernética; desenvolver programa de capacitação de gestores atuantes nas infraestruturas críticas.

3.3. Sugestões de atuação da Anatel

A pesquisa evidenciou que as nações estão apenas iniciando suas abordagens ao tema.[114] Mesmo os EUA, que já estão em estágio mais avançado de construção de uma política de segurança cibernética, em que as instituições já disputam espaço por representatividade e liderança nos esforços nacionais, as atividades concretas são incipientes.

A maior parte das iniciativas parece estar voltada a estudos inicias que identifiquem os papéis dos múltiplos *stakeholders*. Parece razoável que a maturação da política brasileira ocorra no curto a médio prazo, de maneira que as críticas devem ser ponderadas, mas também criativas.

Embora o PNBL estadunidense e as consultas públicas da FCC apresentem indicações sobre o que se pode esperar da atuação de um regulador, a

[114] Cf. *Segurança cibernética: desafio é cultural*. http://wap.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=20291&sid=11

aceitação pública desse papel ainda não é universal. As respostas aos chamamentos da Comissão acenderam a luz amarela para investidas da instituição, sob o risco de usurpar de seu mandato e obstar a inovação, obrigando empresas do setor a incorrer em custos contrapostos por benefícios incertos.

A UIT, por sua vez, apresenta um compilado dos papéis desempenhados por reguladores bastante diversos; alguns podem assumir o papel de formulador de políticas e responder diretamente ao chefe de Estado. Assim, não se extrai do trabalho uma proposta única para reguladores.

Os modelos apresentados poderiam ser transpostos ao Brasil com cautela, vez que a Anatel não é uma instituição que desponta em seu caráter político, o que oprime o exercício (a manifestação) de sua capacidade técnica e obstrui as oportunidades de se apresentar à cúpula da Administração Pública e ao setor como um ente estatal maduro, apto a exercer funções de ponta nas políticas estratégicas nacionais de segurança cibernética.

Inspirando-se nas oportunidades, desafios e diretrizes enunciadas pelo Livro Verde, parece razoável propor à Agência atuar inicialmente de maneira discreta, em sua função de agente normativo e regulador da atividade econômica. Em sua atribuição de garante da qualidade da prestação de serviços de telecomunicações, caberia papel mais incisivo, já que alguns padrões mínimos são reconhecidos no setor.

Com a iminência dos grandes eventos esportivos a serem sediados no Brasil, a infraestrutura crítica do Brasil será posta à prova. Argumenta-se que a demanda prevista para a Copa do Mundo 2014 e os Jogos Olímpicos 2016 desafiará os gargalos em aeroportos, transportes públicos, rede hoteleira. No setor de telecomunicações não será diferente.

3.3.1. Possível Mandato da Anatel

A revisão da regulamentação relacionada ao provimento de serviço de Internet facilitaria a atuação da Anatel. O moroso embate entre serviços de telecomunicações e serviços de valor adicionado (SVA) impede grande parte das

atividades da Agência relacionadas à regulamentação de tópicos relevantes da Internet moderna, muitos relacionados à proteção direta de interesses do consumidor.

A distinção entre atores e atividades desempenhadas ao longo da cadeia estabelecida, em 1995, para uso de meios da rede pública de telecomunicações para acesso à Internet foi econômica e tecnicamente oportuna para fomentar a promoção da Internet no País.

Já há alguns anos, no entanto, o descompasso dos critérios regulamentares nacionais dá margem a incertezas em relação a direitos e deveres de provedores de conexão à Internet, provedores de conteúdo e aplicações, prestadoras de serviços de telecomunicações, usuários de conexão à Internet e usuários de serviços de telecomunicações, conforme definidos pela Norma MC nº 04/95 (sobre o uso de meios da rede pública de telecomunicações para acesso à Internet[115]) e pela LGT.

No cenário presente, os limites expressos na regulamentação se confundem e dificultam a responsabilização (administrativa, civil, penal) de pessoas físicas e jurídicas que cometam ou viabilizem o cometimento de atos danosos ou ilícitos penais por meio da Internet.

Embora discussões sobre os poderes investigatórios de uma Comissão Parlamentar de Inquérito (CPI) transcendam aos objetivos desta pesquisa, cite-se que a dificuldade de responsabilização de provedores, prestadoras e usuários esteve no cerne das discussões sobre a competência da CPI da Pedofilia para requerer a quebra de sigilo de dados de seus clientes. À época, o que se viu foi um jogo de empurra-empurra, onde a estratégia era se esquivar das solicitações de dados de acesso e dados cadastrais feitas, em diferentes momentos, por Anatel, Polícia Civil, Polícia Federal, Ministério Público e a própria CPI.

Os argumentos empregados são conhecidos e recorrentes:

a) A violação do sigilo das comunicações telegráficas e de dados seria inconstitucional, ainda que por mandado judicial e para fins de investigação criminal ou instrução processual penal.

[115] http://www.anatel.gov.br/Portal/exibirPortalRedireciona.do?caminhoRel=Cidadao-Biblioteca-Acervo%20Documental&codigoDocumento=10283&caminhoRel=Cidadao-Internet-D%FAvidas%20freq%FCentes

Suscita-se inconstitucionalidade[116] da "interceptação do fluxo de comunicações em sistemas de informática e telemática", admitida pela Lei nº 9.626/96[117], que regulamentou a interceptação de comunicações telefônicas, autorizada pelo inciso XII, parte final, do art. 5° da Constituição Federal[118];

b) Em se entendendo que a violação do sigilo das comunicações telegráficas e de dados seja constitucional, sê-lo-ia exclusivamente por meio de mandado judicial e para fins de investigação criminal ou instrução processual penal, de modo que a requisição da autoridade investigatória seria insuficiente;

c) Os custos de armazenamento das informações dos usuários (dados cadastrais, de acesso, conexão, conteúdo, tráfego) úteis à identificação e localização de suspeitos de envolvimento com pornografia infantil, durante longos períodos (de seis meses a três anos, por exemplo), seriam bastante elevados, por consequência, inviável para as empresas arcarem com esse compromisso;

d) Os provedores não estariam sujeitos à regulamentação específica e à fiscalização da Anatel, uma vez que o Serviço de Conexão à Internet (item 3, "a", Norma MC nº 04/95) é considerada Serviço de Valor Adicionado (item 3, "b", da Norma MC nº 04/95, c/c art. 61, da LGT) e que o SVA não constitui serviço de telecomunicações (art. 61, § 1º, da LGT). Nesse

---

[116] Em 22 de julho de 2008, o Supremo Tribunal Federal (STF) recebeu a Ação Direta de Inconstitucionalidade (ADI) nº 4112, proposta pelo Partido Trabalhista Brasileiro (PTB) contra a Lei nº 9.626/96.

[117] "Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática." (Lei nº 9.296, de 24 de julho de 1996).

[118] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;" Cf. *Constituição da República Federativa do Brasil de 1988.*

> diapasão, a Agência não poderia solicitar informações sobre as atividades dos provedores, realizar busca e apreensão de bens destes, obrigá-los a manter recursos tecnológicos disponíveis no caso de ser necessária à quebra de sigilo das comunicações de dados, tampouco fiscalizar o cumprimento de procedimentos de segurança impostos ou recomendados por autoridades públicas (em contraposição à competência da Anatel para adotar medidas para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, exemplificadas pelo art. 19, LGT).

Em razão do apelo público do objeto da CPI, essa postura evasiva assumida por provedores e prestadoras repercutiu negativamente, dando vazão a críticas de que o setor estaria criando empecilhos ao combate à pedofilia no País. Ainda que questões técnicas e jurídicas levantadas não estejam legalmente sob atribuição da Agência, elas seriam inerentes aos "serviços de telecomunicações", sob a ótica do consumidor.

Como citado no texto da UIT, um mandato claro é fundamental para que a Anatel venha a contribuir para a política de segurança cibernética de maneira integralmente legítima, com diminuição de óbices jurídicos que causem disputas entre a Agência e demais órgãos públicos ou setor privado.

3.3.2. Combate ao spam e botnets

A solução encontrada pelo regulador holandês parece compatível com a questão vivenciada pela Anatel. Já que reformas na LGT e na Norma 04/95 do Ministério das Comunicações enfrentam forte oposição, emitir regulamentos que mitiguem a proliferação de spams e o crescimento de botnets, sob o argumento de proteção ao consumidor (inclusive com obrigações de universalização e continuidade, nos termos do art. 79, LGT [119]), seria um

[119] "Art. 79. A Agência regulará as obrigações de universalização e de continuidade atribuídas às prestadoras de serviço no regime público.

§ 1° Obrigações de universalização são as que objetivam possibilitar o acesso de qualquer pessoa ou instituição de interesse público a serviço de telecomunicações, independentemente de sua

mecanismo a contribuir para o incremento na qualidade do serviço percebida pelos usuários de Internet.

Ha soluções técnicas, como bloqueio de Porta 25[120], que diminuem o volume de *spam* e que, sendo implementados pelas operadoras, seriam fiscalizadas pela Anatel, como um requisito para o pleno funcionamento da infraestrutura de telecomunicações nacional.

3.3.3. Infraestrutura Crítica e tratamento de incidentes

Em momento próximo, exigências sobre proteção de infraestruturas críticas de telecomunicações implicarão necessidade de fiscalização. A Anatel é um órgão que teria alcance nacional para fiscalizar a adoção de medidas e padrões obrigatórios eventualmente impostos sobre o setor, nos termos de uma política nacional de segurança cibernética (art. 5º c/c art. 19, IV, X, XII, XIII, XIV[121]).

---

localização e condição sócio-econômica, bem como as destinadas a permitir a utilização das telecomunicações em serviços essenciais de interesse público.

§ 2° Obrigações de continuidade são as que objetivam possibilitar aos usuários dos serviços sua fruição de forma ininterrupta, sem paralisações injustificadas, devendo os serviços estar à disposição dos usuários, em condições adequadas de uso." Cf. Lei nº 9.472.

[120] "A medida não é nova, órgãos internacionais aconselham o bloqueio da porta 25 desde 1998, mas apenas em 2005, provedores e operadoras de todo o mundo começaram a adotá-la em massa.

(...) 'Pela porta 25 a mensagem é enviada direto para o destinatário. É o que chamamos de 'envio direto'. Com a porta 587, o usuário precisa se autenticar em um servidor, por onde passa o e-mail. Então é mais fácil barrar spams. A ideia é deixar a porta 25 apenas para tráfego entre servidores.'" *Bloqueio da porta 25 por provedores de e-mails passa a vigorar*. http://tecnologia.uol.com.br/seguranca/ultimas-noticias/2010/01/05/bloqueio-da-porta-25-por-provedores-de-e-mails-passa-a-vigorar-nesta-terca.jhtm

[121] "Art. 5º Na disciplina das relações econômicas no setor de telecomunicações observar-se-ão, em especial, os princípios constitucionais da soberania nacional, função social da propriedade, liberdade de iniciativa, livre concorrência, defesa do consumidor, redução das desigualdades regionais e sociais, repressão ao abuso do poder econômico e continuidade do serviço prestado no regime público. (...)

Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente:

I - implementar, em sua esfera de atribuições, a política nacional de telecomunicações; (...)

IV - expedir normas quanto à outorga, prestação e fruição dos serviços de telecomunicações no regime público; (...)

X - expedir normas sobre prestação de serviços de telecomunicações no regime privado; (...)

O mapeamento das infraestruturas críticas de telecomunicações no País já se encontra em fase avançada, com dados fornecidos pelas próprias operadoras. Mecanismos cogentes serão necessários.

Nesses termos, a Agência poderia buscar informações diretamente nos sistemas das empresas, respeitando os direitos à privacidade e ao sigilo das comunicações. Essas atividades não deveriam depender da voluntariedade na divulgação-troca de informações das operadoras, que não percebem incentivos para enunciar seus riscos e vulnerabilidades ao regulador.

Uma equipe de tratamento e resposta a incidentes em redes computacionais própria da Agência voltada a monitorar o comportamento e coletar dados sobre incidentes de redes de operadoras do setor complementaria tal estrutura.

Algumas operadoras anunciam participar de redes de trocas de informações,[122] mas a Anatel dispõe de parca informação a esse respeito, e, por consequência, pouco conhece da dimensão de ataques e comportamentos de segurança nas redes. Integrar a Impact-Alliance, parceira internacional da UIT, também tende a aumentar o conhecimento sobre padrões de ameaças e incidentes nas redes globais.

Essas informações seriam aperfeiçoadas por meio de cooperação com grupos já sedimentados, como o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov).

XII - expedir normas e padrões a serem cumpridos pelas prestadoras de serviços de telecomunicações quanto aos equipamentos que utilizarem;

XIII - expedir ou reconhecer a certificação de produtos, observados os padrões e normas por ela estabelecidos;

XIV - expedir normas e padrões que assegurem a compatibilidade, a operação integrada e a interconexão entre as redes, abrangendo inclusive os equipamentos terminais;" LGT

[122] Alguns prestadores de serviços de telecomunicações que afirmam dispor de CSIRTs: CTBC Telecom, Embratel, Oi, Star One, Telefonica, Tim, Vivo. Sob autorização das empresas, o CERT.br divulga seus contatos, mas a Anatel desconhece oficialmente quantos são, quais são e o que fazem. Cf. CERT.br. *Informações de Contato de Grupos de Segurança Brasileiros*. http://www.cert.br/contato-br.html

Para que a Anatel legitime sua atuação, suas práticas internas devem ser revistas. Em 17 de março de 2011, o Tribunal de Contas da União (TCU) divulgou o Acórdão nº 465, referente à avaliação de controles gerais de tecnologia da informação da Agência, e constatou diversas irregularidades, precariedades e oportunidades de melhoria.[123]

O desempenho da Anatel ficou bastante aquém do determinado pelo marco legal de segurança da informação e comunicações. O TCU constatou: inexistência de Política de Segurança da Informação e Comunicações, inexistência de inventário dos ativos de informação, inexistência de ETIR, inexistência de processo de gestão de riscos de segurança da informação.

As muitas deficiências de segurança da informação e comunicações, em evidente descumprimento de normas estabelecidas pelo CGSI e GSI, dificultam o reconhecimento da Agência como instituição madura o suficiente para desempenhar papel significativo de segurança cibernética perante os demais entes da Administração Pública (e também a iniciativa privada), apta a exercer parcerias com CTIR Gov, CERT.br e ETIRs de operadoras.

3.3.4. Pesquisa e Desenvolvimento

A prestação de serviços de telecomunicações alimenta o Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel), cujo mote seria estimular o processo de inovação tecnológica, incentivar a capacitação de recursos humanos, fomentar a geração de empregos e promover o acesso de pequenas e médias empresas a recursos de capital, de modo a ampliar a competitividade da indústria brasileira de telecomunicações (art. 1º, Lei nº 10.052/2000).

Foi com recursos do Funttel que CPqD e Anatel desenvolveram o projeto de Proteção de Infraestruturas Críticas de Telecomunicações (PICT), citado nacional e internacionalmente como uma importante iniciativa de proteção

[123] http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20110321/AC_0465_06_11_P.doc

de infraestrutura crítica e merece continuidade. O Funttel não deve ser a única fonte de fomento, mas pode ser uma das principais do setor.

A END e os planos setoriais de infraestrutura crítica devem também promover o desenvolvimento de padrões nacionais, sob os critérios de interesse nacional e pesquisas com desenvolvimento de tecnologia do País. O setor privado haveria de explorar esse nicho, sob o estímulo governamental (art. 76 c/c art. 78, LGT[124]).

Constam das comunicações diplomáticas estadunidenses divulgadas pelo site Wikileaks, por exemplo, menções a oportunidades de investimento e cooperação em segurança cibernética e infraestrutura crítica no Brasil, no contexto dos grandes eventos desportivos programados para o médio prazo.

3.3.5. Harmonização de ações

À Anatel não caberia formular a política nacional de segurança cibernética, mas esta deve manter íntima relação com sua formulação. A razão para a coordenação com o GSI é a mesma já apresentada em outros tópicos: a especialidade do corpo técnico da Agência, essencialmente formada por engenheiros e tecnólogos, com amplo conhecimento em TICs e inovação, que propiciaram a vida em um mundo cibernético.

Para intermediar essa relação, o Ministério das Comunicações deveria ser incluído como membro permanente do Grupo Técnico de Segurança Cibernética (GT SEG CIBER) e do Grupo de Trabalho de Segurança de Infraestruturas Críticas da Informação (GTSICI). Quanto mais distantes os órgãos trabalharem, menor será o grau de completude do plano nacional.

---

[124] "Art. 76. As empresas prestadoras de serviços e os fabricantes de produtos de telecomunicações que investirem em projetos de pesquisa e desenvolvimento no Brasil, na área de telecomunicações, obterão incentivos nas condições fixadas em lei.

Art. 78. A fabricação e o desenvolvimento no País de produtos de telecomunicações serão estimulados mediante adoção de instrumentos de política creditícia, fiscal e aduaneira." Cf. Lei nº 9.472.

A relação entre Ministério das Comunicações, Anatel e Telebrás ainda é incerta. Para que o plano nacional de banda larga nasça conforme práticas de segurança, sua execução deve ser acompanhada também pelo GT SEG CIBER.

A Telebrás tem priorizado em suas licitações equipamentos com tecnologia nacional. O discurso de governo é que questões de segurança nacional não poderiam ficar à mercê de redes de telecomunicações de capital e insumos puramente estrangeiros, cujas demandas de segurança sejam pouco conhecidas no Brasil. A empresa alega estar alerta para a segurança de seu patrimônio e das informações nela trafegadas, o que justificaria os leilões bastante restritivos a fornecedores estrangeiros.

Não se questiona neste trabalho o mérito dos leilões, tampouco as razões para a retomada da empresa, mas aspectos de segurança devem estar no bojo do planejamento e dimensionamento de redes de telecomunicações de quaisquer operadoras desde seus momentos iniciais.

3.3.6. Compartilhamento de informação

Conforme a END, as comunicações continuam sendo um tema estratégico. Desde a privatização do setor (mesmo antes, com o esvaziamento da Doutrina de Segurança Nacional), criou-se um hiato entre um papel da propriedade/gerenciamento das redes publicas pelo Sistema Telebrás e a exploração privada atual.

Para que o setor privado coopere com os interesses da nação, será necessário tê-lo como parceiro no compartilhamento de informações e integrá-lo em diferentes momentos da formulação da política nacional. Naturalmente, não se defenderá censura ou ameaça à propriedade privada, na verdade, vislumbra-se que privacidade e segurança não sejam considerados aspectos antagônicos, mas complementares.[125]

---

[125] A maior parte das novas legislações sobre segurança cibernética está centrada nesse *tradeoff* entre privacidade e segurança, bem como no emprego de técnicas de filtragem de informação (em prejuízo à privacidade) para solucionar problemas de assimetria da informação entre o possível infrator e a autoridade de segurança. Para Schneider, "[s]egurança e privacidade não são extremos

Na mesma linha, Termos de Cooperação firmados entre Anatel e outros órgãos da Administração Pública tenderiam a facilitar a execução da política nacional.

Com os órgãos de polícia, a área de fiscalização da Anatel trabalharia em conjunto para a identificação de pontos da rede em que conteúdos impróprios estivessem sendo trocados; com o Congresso Nacional, que considera a possibilidade de legislar sobre crimes cibernéticos, auxiliaria nos conceitos técnicos e as tendências do setor de TICs; com o Ministério da Justiça, que patrocina estudos sobre um marco civil da Internet no Brasil e a proteção a bancos de dados, a experiência de seus profissionais agregaria valor e reduziria o risco de uma lei nascer inócua por razões essencialmente tecnológicas.

3.3.7. Estrutura permanente de segurança cibernética na Agência

Nos termos anteriores, deve-se promover na Agência a cultura de segurança cibernética desde estágios embrionários, com políticas preventivas, até fases avançadas de tratamento de incidentes. Para tanto, sugere-se a criação de comissão permanente de segurança cibernética apta a abordar os diversos temas aventados neste texto, incluindo a proteção de infraestruturas críticas.

Idealmente um órgão ligado ao Conselho Diretor poderia ser instituído com mandato amplo que alcance toda a estrutura regulatória e fiscalizatória da Agência, à semelhança do Bureau de Segurança Nacional da instituído no âmbito da FCC e que mantém relacionamento direto com o DHS. Esse órgão seria o responsável pela coordenação da atividade externa da Anatel em todos os foros e instâncias da Administração que abordassem o tema, segundo diretrizes do GT SEG CIBER e CREDEN, com foco também nos grandes eventos esportivos internacionais que o País sediará.

---

opostos de uma gangorra, você não tem que aceitar menos de um para obter mais do outro.” Cf. SCHNEIDER, Bruce. *What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposite*. http://www.schneier.com/essay-203.html

3.3.8. Brasil, UIT e cooperação internacional

No que tange à representatividade dos países na Organização, à medida que as atribuições da UIT evoluem, novos atores devem ser chamados a participar de seus processos. Se a UIT foi um foro essencialmente técnico, em que engenheiros calculavam as melhores soluções para harmonização de frequências que garantissem a viabilidade das telecomunicações, por certo, o cenário não é mais esse. A UIT é também um foro com vertentes políticas relevantes, cujas vicissitudes demandam um esforço de coordenação nacional elevado que reflitam a política externa do País.

Ao passo que o Brasil é usualmente representado apenas pela Anatel e, em situações pontuais, pelo Ministério das Relações Exteriores e alguns poucos centros de pesquisa que participam das CBCs, as delegações de países desenvolvidos incluem representantes dos diversos níveis de governo.

Na PP-10, por exemplo, a delegação americana, apenas para lidar com o tema segurança cibernética, incluía, além de delegados da FCC, representantes da Casa Branca, do Departamento de Estado, do Departamento de Defesa, do Departamento de Comércio, do Departamento de Justiça, e, naturalmente, da iniciativa privada.

Durante a Conferência, sob a liderança da Chancelaria, o Brasil se pautou, ao longo de todo o processo negocial, pelas análises técnicas da Anatel, pelo decálogo de princípios para a governança da Internet no Brasil[126] e por instruções apresentadas pelo MRE[127].

Em especial, reuniões provocadas pela Anatel, sob coordenação do MRE e com representantes de MD e GSI, foram decisivas para o posicionamento

---

[126] Resolução CGI.br/RES/2009/003/P - *Princípios para a governança e uso da internet no Brasil*. http://www.cgi.br/regulamentacao/resolucao2009-003.htm

[127] O MRE entendeu que o tema de segurança cibernética tem pelo menos três acepções complementares: segurança das redes (continuidade do uso e funcionamento em nível global), segurança das pessoas (combate ao crime pela e na Internet e garantias dos direitos fundamentais) e segurança nacional (uso de recursos da rede como armas contra Estados). Segundo o Itamaraty, o papel da UIT estaria diretamente ligado à primeira acepção (segurança das redes), enquanto que segurança das pessoas e dos países parece fugir ao mandato e ao escopo técnico da organização.

que o País tomaria na PP-10. Como resultado desse esforço multi-institucional, a UIT não seria prioridade para a segurança cibernética brasileira.

O desfecho da PP-10 é favorável à atuação da Agência, embora tenha contido investidas mais ousadas. Com a prevalência dos argumentos em favor do mérito técnico da UIT em temas de segurança cibernética, legitimou-se que órgãos reguladores e o setor privado de TICs avancem na formulação e divulgação de padrões e de melhores práticas voltados essencialmente ao gerenciamento de sistemas de redes e serviços de telecomunicações seguros.

Caso os Estados estendessem o mandato da UIT para abarcar também aspectos de segurança das pessoas e segurança nacional,[128] a politização da agenda implicaria a condução obrigatória de órgãos como polícias, ministérios de justiça, forças armadas, em prejuízo à primazia do setor técnico.

Cabe à Anatel dar ampla divulgação sobre o contexto e os resultados decorrentes das negociações sobre segurança cibernética havidas à PP-10. Em razão das vicissitudes do tema, tornou-se transparente que o interesse político-estratégico transcende à atuação autônoma do órgão regulador. Sob instrução do Conselho Diretor da Agência, deve-se apresentar e divulgar no plano nacional as atividades da UIT, com vista à obtenção de direcionamento estratégico para a atuação do País na organização, por meio das CBCs.

Naturalmente, aproximar-se de outros reguladores, como a FCC, e conhecer a fundo suas experiências citadas neste trabalho tendem a encurtar o caminho para a definição do papel do regulador no Brasil.

A cooperação internacional é reconhecidamente uma frente que deve ser explorada. A interdependências das redes, a transnacionalidade dos atos, a responsabilidade compartilhada, características intrínsecas às telecomunicações implicam necessidade de cooperação. A Anatel deve explorar essa seara internacional, não para seguir às cegas as melhores praticas definidas alhures, mas para influenciar a organização, conforme interesses nacionais.

[128] Uma hipótese extrema dos posicionamentos dos países na PP-10, conforme item 2.1.2.

CONCLUSÃO

Tendo analisado os modelos de UIT e Estados Unidos para a Segurança Cibernética, percebe-se bastante semelhança entre as propostas para reguladores. São desenhos que indicam a participação qualificada do regulador de telecomunicações nos esforços nacionais em manter um ambiente virtual seguro.

No caso brasileiro, identificaram-se poucas atividades concretas (para além do plano ideológico) empreendidas pela Anatel, tampouco a inclusão da Agência ou do Ministério das Comunicações na atividade central de formulação das políticas de segurança cibernética.

Com base na experiência internacional, acredita-se que as propostas de atuação da Anatel em temas como infraestrutura crítica, combate a spam e botnets, pesquisa e desenvolvimento dependem de clareza no mandato da Agência. Para atuar efetivamente na Segurança Cibernética, sua relação com outros entes da Administração precisa ser aprimorada e coordenada, em particular, com os órgãos de inteligência do Estado.

A atuação internacional da Anatel não pode ser desvinculada da atividade de coordenação nacional. Ainda que a Agência tenha o mandato de representante brasileiro em foros de telecomunicações, as demandas que surgem nesses foros extrapolam suas atribuições tradicionais e correspondem à competência de outros órgãos da Administração.

Sob pena de expressão desarmônica, a atuação do País em instituições como UIT deve ser analisada e balizada pelo grupo responsável pela formulação da estratégia nacional de segurança cibernética, onde Ministério das Comunicações deveria ter assento, em razão de sua competência legal e capacidade de vincular os representantes do setor de comunicações.

BIBLIOGRAFIA

Livros, artigos e legislação

AFONSO, Carlos A. FONSO, Carlos A. “Que banda larga queremos?” In: CGI.br (Comitê Gestor da Internet no Brasil). *Pesquisa sobre o uso das tecnologias da informação e da comunicação 2009*. São Paulo, 2010, pp. 65-72. http://www.cgi.br/publicacoes/artigos/artigo67.htm.

AMERICAN NATIONAL STANDARDS INSTITUTE. *The financial management of cyer risk. An Implementation Framework for CFOs.* Disponível em: http://webstore.ansi.org/cybersecurity.aspx.

ARANHA, Márcio Iorio. Políticas públicas comparadas de telecomunicações (Brasil-EUA). Brasília: UnB, 2005. http://www.getel.org/sites/default/files/0TESE_CEPPAC_MarcioIorioAranha_0.pdf

BRASIL. ANATEL. Análise nº 316/2010-GCER, de 06/07/2010. http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=245740&assuntoPublicacao=null&caminhoRel=Cidadao-Biblioteca-Acervo%20Documental&filtro=1&documentoPath=245740.pdf.

_____. Despacho nº 4.043/2009-CD - Processo nº 53500.011781/2009, publicado no DOU, em 22 de julho de 2009. http://www.in.gov.br/imprensa/visualiza/index.jsp?data=22/06/2009&jornal=1&pagina=51&totalArquivos=72.

_____. Resolução nº 516, de 30 de outubro de 2008. *Plano Geral de Atualização da Regulamentação das Telecomunicações no Brasil*. http://www.anatel.gov.br/Portal/exibirPortalInternet.do.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL. *Guia de referência para a segurança das infraestruturas críticas da informação*”. (org. Claudia Canongia e Raphael Mandarino Junior). Brasília: GSIPR/SE/DSIC, 2010. http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf

_____. Instrução Normativa GSI/PR nº 1/2008. *Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências*. http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf.

_____. *Livro verde: segurança cibernética no Brasil*. (org. Claudia Canongia e Raphael Mandarino Junior). Brasília: GSIPR/SE/DSIC, 2010. http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

_____. Norma Complementar nº 5, de 17 de agosto de 2009. *Criação de Equipes de Tratamento e resposta a Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Publica Federal*. http://dsic.planalto.gov.br/legislacaodsic.

_____. Portaria nº 16, de 05 de agosto de 2009. *Institui, no âmbito do CGSI, um Grupo de Trabalho de Política Nacional de Telecomunicações voltado para Defesa Nacional, para, até 31 de dezembro de 2003, analisar e apresentar proposta de normalização da Política Nacional de Telecomunicações e os serviços de valor agregado de interesse da Defesa Nacional*. http://dsic.planalto.gov.br/legislacaodsic.

_____. Portaria nº 2, de 8 de fevereiro de 2008. *Institui Grupos Técnicos de Segurança de Infra-estruturas Críticas (GTSIC) e dá outras providências*. http://www.gsi.gov.br/infraestruturas-criticas/Port%202%20-%2008%20Fev%2008%20GTSIC.pdf.

_____. Portaria nº 34, de 05 de agosto de 2009. *Institui Grupo de Trabalho de Segurança das Infraestruturas Criticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI*. http://dsic.planalto.gov.br/legislacaodsic.

_____. Portaria nº 45, de 08 de setembro de 2009. *Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e da outras providencias.* http://dsic.planalto.gov.br/legislacaodsic.

BRASIL. MINISTÉRIO DAS COMUNICAÇÕES. Norma nº 4/95. Uso de meios da rede pública de telecomunicações para acesso à Internet. http://www.anatel.gov.br/Portal/exibirPortalRedireciona.do?caminhoRel=Cidadao-Biblioteca-Acervo%20Documental&codigoDocumento=10283

BRASIL. PRESIDÊNCIA DA REPÚBLICA. *Constituição da República Federativa do Brasil de 1988*.

_____. Decreto nº 3.305, de 13 de junho de 2000. *Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*. http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm.

_____. Decreto nº 7.257, de 4 de agosto de 2010. *Regulamenta a Medida Provisória nº 494 de 2 de julho de 2010, para dispor sobre o Sistema Nacional de Defesa Civil - SINDEC, sobre o reconhecimento de situação de emergência e estado de calamidade pública, sobre as transferências de recursos para ações de socorro, assistência às vítimas, restabelecimento de serviços essenciais e reconstrução nas áreas atingidas por desastre, e dá outras providências*. http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7257.htm

_____. Lei nº 9.296, de 24 de julho de 1996. *Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.* http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm

_____. Lei nº 9.472, de 16 de julho de 1997. *Lei Geral de Telecomunicações*. http://www.planalto.gov.br/ccivil_03/Leis/L9472.htm

BRASIL. SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade (ADI) nº 4112, proposta pelo Partido Trabalhista Brasileiro (PTB) contra a Lei nº 9.626/96. http://m.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=2630565

BRUCE, Robert *et alli*. *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues*. http://www.ists.dartmouth.edu/library/158.pdf.

CABINET OFFICE. *Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space*. UK Office of Cyber Security (OCS) and UK Cyber Security Operations Centre (CSOC). http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf.

CANONGIA, Claudia; MANDARINO Jr., Raphael (org.). *Guia de referência para a segurança das infraestruturas críticas da informação*". Brasília: GSIPR/SE/DSIC, 2010.

_____. *Segurança Cibernética: o desafio da nova Sociedade da Informação.* Parcerias Estratégicas. http://www.cgee.org.br/parcerias/p29.php.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. *Securing Cyberspace for the 44th. Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). *Cartilha de Segurança para Internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2006. http://cartilha.cert.br/

_____. *Informações de Contato de Grupos de Segurança Brasileiros.* http://www.cert.br/csirts/brasil/.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Resolução CGI.br/RES/2009/003/P - *Princípios para a governança e uso da internet no Brasil*. http://www.cgi.br/regulamentacao/resolucao2009-003.htm.

CONSELHO DA EUROPA. *Convenção sobre Crimes Cibernéticos adotada pelo Conselho da Europa em 2001* ("*Convenção de Budapeste*"). http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf

DIPLOFOUNDATION. *Internet Governance Capacity Building Program 2009 – Advanced Phase on Privacy and Personal Data Protection*. http://campus.diplomacy.edu/lms/ClassNav.asp?IDclass=190.

_____. http://www.diplomacy.edu/ig/default.asp.

EASTWEST INSTITUTE. *The Cybersecurity Agenda*. http://www.ewi.info/cybersecurity-agenda.

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME (UNODC). *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*.

ESTADOS UNIDOS DA AMÉRICA (EUA). BROADBAND.GOV. *Connecing America: The National Broadband Plan*. 2010. http://www.broadband.gov/plan/16-public-safety/#r16.

EUA. BROADBAND.GOV. *Connecing America: The National Broadband Plan*. 2010 http://www.broadband.gov/plan/16-public-safety/#r16.

EUA. FEDERAL COMMUNICATIONS COMMISSION. *Notice of Inquiry. Cyber Security Certification Program.* http://fjallfoss.fcc.gov/ecfs/proceeding/view?name=10-93.

_____. *Notice of Inquiry. Effects on Broadband Communications networks of damage to or failureof network equipment or severe overload.* http://fjallfoss.fcc.gov/ecfs/proceeding/view?name=10-92.

_____. *Public Notice. FCC seeks public comment on National Broadband Plan recommendation to create a cybersecurity roadmap.* http://fjallfoss.fcc.gov/ecfs/proceeding/view?name=10-146.

_____. *Tech Topic 20: Cyber Security and Communications*. http://www.fcc.gov/pshs/techtopics/techtopics20.html.

EUA. RECOVERY.GOV. *Track the money.* http://www.recovery.gov/Pages/default.aspx.

EUA. WHITE HOUSE. *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

_____. *Defending America's Cyberspace – National Plan for Information Systems Protection Version 1.0* http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf.

_____. *Remarks by the President on securing our nation's cyber infrastructure.* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

_____. *The Comprehensive National Cybersecurity Initiative*. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

_____. *The National Strategy to Secure Cyberspace* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. *Security Economics and the Internal Market*. http://www.enisa.europa.eu/act/sr/reports/econ-sec

FARROW, S.; SHAPIRO, S. *The benefit-cost analysis of security focused regulations*. http://www.umbc.edu/economics/wpapers/wp_09_101_DHSFarrowShapiro.pdf.

FRAGOSO, S. "Espaço, ciberespaço, hiperespaço". *Textos de educação e cultura*, n. 42. UFBA, 2000. http://www.scribd.com/doc/33757586/Espaco-ciberespaco-hiperespaco.

GHERNAOUTI-HÉLIE, S. SCHJØLBERG, S.; *A Global Protocol on Cybersecurity and Cybercrime: An initiative for peace and security in cyberspace*. http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

GRADY, M.; PARISI, F. *The Law and Economics of Cybersecurity: An Introduction*. Cambridge University Press: 2006. http://www.law.gmu.edu/faculty/papers/docs/04-54.pdf

HATHAWAY, Melissa E. *Cybersecurity: The U.S. Legislative Agenda*. http://belfercenter.ksg.harvard.edu/files/legislative-landscape-publish-final.pdf.

KIM, Yongsoo; KELLY, Tim; RAJA, Siddhartha. *Building Broadband: strategies and policies for the developing world*. http://go.worldbank.org/7EP6QCMY40.

KURBALIJA, J. *An Introduction to Internet Governance*. DiploFoundation and National Internet Exchange of India (NIXI): 2008. http://www.diplomacy.edu/poolbin.asp?IDPool=806.

MANDARINO Jr. *Segurança e defesa no espaço cibernético brasileiro*. Recife: Cubzac, 2010.

MANDARINO Jr., Raphael. *La seguridad cibernética en el Gobierno de Brasil*. http://www.youtube.com/watch?v=qVAhMxwJFEE; http://www.arcert.gov.ar/10_aniv/presentaciones/la_seguridad_cibernetica_en_%20el_gobierno_%20de_brasil.pdf.

MANDARINO JR., Raphael. *Um estudo sobre a Segurança e Defesa do Espaço Cibernético Brasileiro*. 2009. Monografia (especialização). Universidade de Brasília (UnB). Departamento de Ciência da Computação – DCE: Brasília. Jun 2009. http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf.

ORGANIZAÇÃO DE COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Implementation plan for the OECD guidelines for the security of information systems and networks: towards a culture of security*. http://www.oecd.org/dataoecd/23/11/31670189.pdf.

PAIXÃO, Cristiano. "Dicotomias deslizantes: público e privado em tempos de terror." In: PEREIRA, Cláudia Fernanda de Oliveira (Coord). *O novo direito administrativo brasileiro: o público e o privado em debate*. Belo Horizonte: Fórum, 2010. v. 2. pp. 25-26.

PERRY, William J.; CASADO, Martin; COLEMAN, Keith; WENDLANDT, Dan. "U.S. National Cybersecurity". http://www.stanford.edu/class/msande91si/www-spr04/slides/Lecture1.pdf.

SCHNEIDER, Bruce. *Memo to Next President: How to Get Cybersecurity Right*. Disponível em: http://www.schneier.com/essay-231.html.

_____. *The Problem Is Information Insecurity*. Disponível em http://www.schneier.com/essay-233.html.

_____. *What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposite*. http://www.schneier.com/essay-203.html

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. *Connectivity, openness and vulnerability: challenges facing regulators.* http://www.ictregulationtoolkit.org/en/Publication.3821.html.

_____. *Cybersecurity: The Role and Responsibilities of an Effective Regulator*. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

_____. *El Ciberdelito: Guía para los países en desarrollo*. http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf.

_____. *ITU Activities related to Cybersecurity*. http://www.itu.int/cybersecurity/.

_____. *ITU Study on the Financial Aspects of Network Security: Malware and Spam*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

_____. *ITU Toolkit for Cybercrime Legislation*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.

_____. *ITU-D Question 22/1: Securing information and communication networks: best practices for a developing country*. http://www.itu.int/publ/D-STG-SG01.22-2010/en.

_____. *ITU-T approved security definitions*. http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0003ZIPE.zip.

_____. *Key Global Telecom Indicators for the World Telecommunication Service Sector*. http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html.

_____. *Laureate WTISD 2009 - Addresses by H.E. Luiz Inácio Lula da Silva, President of the Federative Republic of Brazil*. http://www.itu.int/wtisd/2009/award/laureates/lula-address.html.

_____. *Overview of Cybersecurity*. Recomendação X.1205 da UIT-T. http://www.itu.int/rec/T-REC-X.1205-200804-I.

_____. *Understanding Cybercrime: a guide for developing countries*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

WANG, Q.; KIM, S. *Cyber Attacks: Cross-Country Interdependence and Enforcement*. http://weis09.infosecon.net/files/153/paper153.pdf.

WIKIPEDIA. *Julius Genachowski*. http://en.wikipedia.org/wiki/Julius_Genachowski.

Matérias jornalísticas

BA: incêndio na Oi prejudica matrículas escolares http://tudoglobal.com/blog/capa/98822/ba-incendio-na-oi-prejudica-matriculas-escolares.html.

Bloqueio da porta 25 por provedores de e-mails passa a vigorar. http://tecnologia.uol.com.br/seguranca/ultimas-noticias/2010/01/05/bloqueio-da-porta-25-por-provedores-de-e-mails-passa-a-vigorar-nesta-terca.jhtm.

China redirecionou tráfego da web para seus servidores, dizem EUA http://www1.folha.uol.com.br/mundo/832324-china-redirecionou-trafego-da-web-para-seus-servidores-dizem-eua.shtml.

China Telecom Denies Hijack of Web Traffic After U.S. Report http://www.bloomberg.com/news/2010-11-18/china-telecom-denies-hijack-of-web-traffic-after-u-s-government-report.html.

Clinton Administration announces new cyber security proposals. http://articles.cnn.com/2000-07-17/politics/net.security_1_encryption-cyber-security-trap-and-trace?_s=PM:ALLPOLITICS.

Com foco na segurança nacional, Telebrás quer acesso aos códigos-fontes http://www.teletime.com.br/30/09/2010/com-foco-na-seguranca-nacional-telebras-quer-acesso-aos-codigos-fontes/tt/200579/news.aspx.

Control of Cybersecurity Becomes Divisive Issue. http://www.nytimes.com/2009/04/17/us/politics/17cyber.html.

Cyber security: Can the Senate make the Internet safe? http://www.techrepublic.com/blog/security/cyber-security-can-the-senate-make-the-internet-safe/1276.

Cyber War: Johnnatan Zitrain weighs in. http://www.theatlantic.com/technology/archive/2011/02/cyber-war-jonathan-zittrain-weighs-in/71027

Cybersecurity strategy released http://www.computerworld.com/s/article/72753/Cybersecurity_strategy_released.

DHS stays mum on new 'Cyber Security' center: http://news.cnet.com/8301-13578_3-10004266-38.html#ixzz1AnH2qWV5.

FCC Cybersecurity. http://www.cybertelecom.org/security/fcc.htm

Huawei opens UK Cyber Security Centre http://www.mobilenewscwp.co.uk/2010/12/huawei-opens-uk-cyber-security-centre/.

Huawei, ZTE Growth to Slow on U.S., India Fears, ISuppli Says http://www.businessweek.com/news/2010-08-24/huawei-zte-growth-to-slow-on-u-s-india-fears-isuppli-says.html.

Incêndio atinge prédio da Oi na Bahia e afeta telefonia em 6 estados http://g1.globo.com/brasil/noticia/2010/12/incendio-atinge-predio-da-operadora-oi-na-bahia.html.

India Said to Block Orders for ZTE, Huawei Technologies Telecom Equipment http://www.bloomberg.com/news/2010-04-30/india-said-to-block-china-s-huawei-zte-from-selling-phone-network-gear.html.

ONU pede tratado para evitar uma 'guerra na internet' http://g1.globo.com/Noticias/Tecnologia/0,,MUL1469914-6174,00.html.

Report: Sprint Rejected Huawei, ZTE for Security Concerns http://www.pcworld.com/businesscenter/article/209963/report_sprint_rejected_huawei_zte_for_security_concerns.html.

Sabotagem e alta espionagem são os maiores temores do mundo digital em 2011 http://veja.abril.com.br/noticia/vida-digital/sabotagem-e-alta-espionagem-sao-os-maiores-temores-do-mundo-digital-em-2011.

Segurança cibernética: desafio é cultural. http://wap.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=20291&sid=11.

Stuxnet pode ser parte de problemas atômicos do Irã http://exame.abril.com.br/tecnologia/noticias/stuxnet-pode-ser-parte-de-problemas-atomicos-do-ira.

Stuxnet virus set back Iran's nuclear program by 2 years http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475.

Stuxnet worm 'targeted high-value Iranian assets' http://www.bbc.co.uk/news/technology-11388018.

Telebrás decide comprar apenas equipamento local e irrita múltis http://www.outroladodanoticia.com.br/component/content/article/2-noticias/1134-telebras-decide-comprar-apenas-equipamento-local-e-irrita-multis-.html.

Telebrás: Acesso aos códigos-fonte é procedimento de segurança http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=23908&sid=10.

Timeline: The U.S. Government and Cybersecurity. *http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true*.

US accuses China Telecom of internet hijack http://www.computerweekly.com/Articles/2010/11/18/243984/US-accuses-China-Telecom-of-internet-hijack.htm.

Veja lista traduzida dos locais "vitais" para segurança dos EUA revelada pelo WikiLeaks http://www1.folha.uol.com.br/mundo/841676-veja-lista-traduzida-dos-locais-vitais-para-seguranca-dos-eua-revelada-pelo-wikileaks.shtml.

Was Stuxnet Built to Attack Iran's Nuclear Program? http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

White House Reveals Secret Cybersecurity Plan Developed Under Bush Administration. http://www.huffingtonpost.com/2010/03/02/nspd54-secret-cybersecuri_n_483103.html.

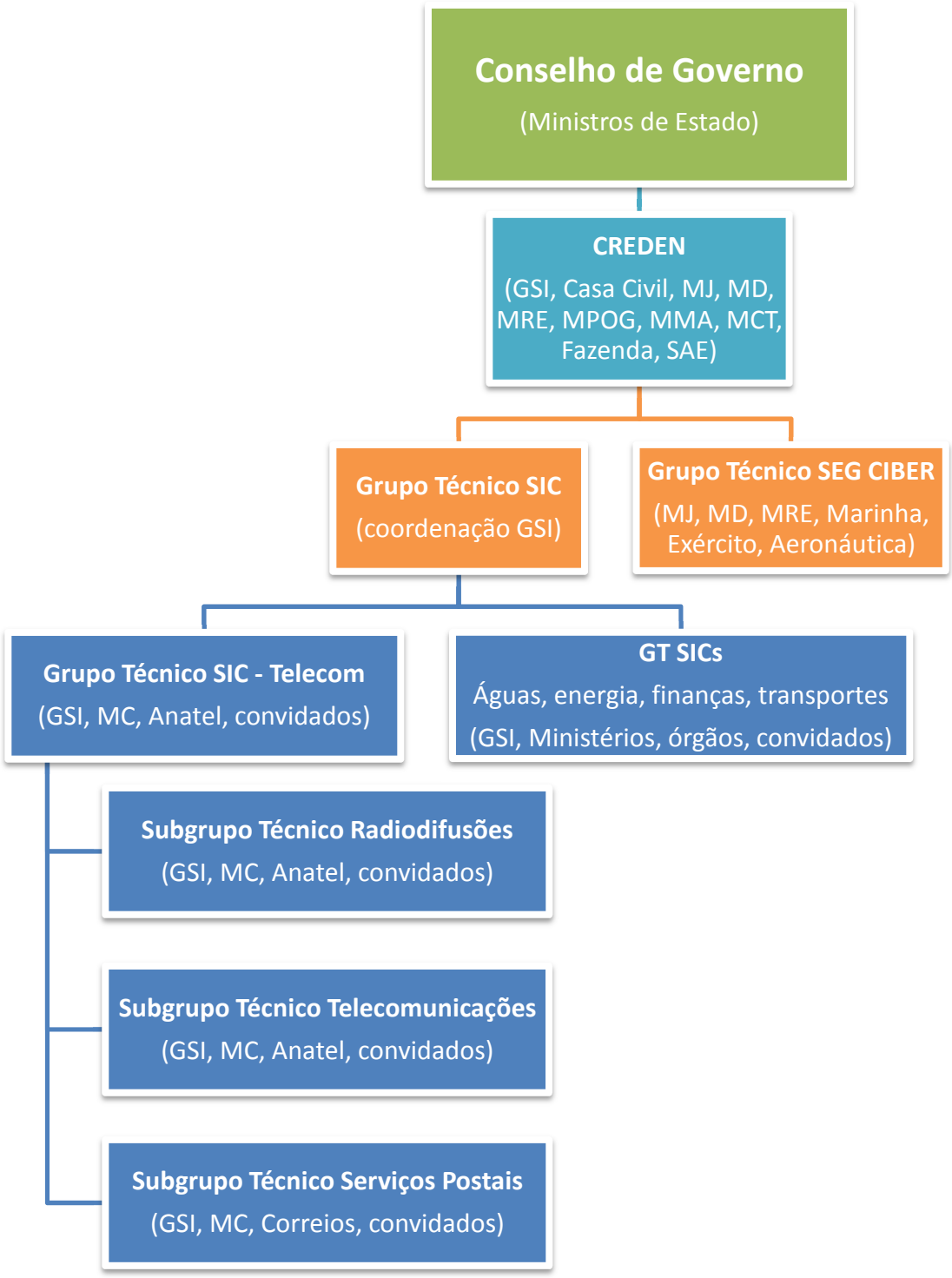
WikiLeaks backlash: The first global cyber war has begun, claim hackers http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war.

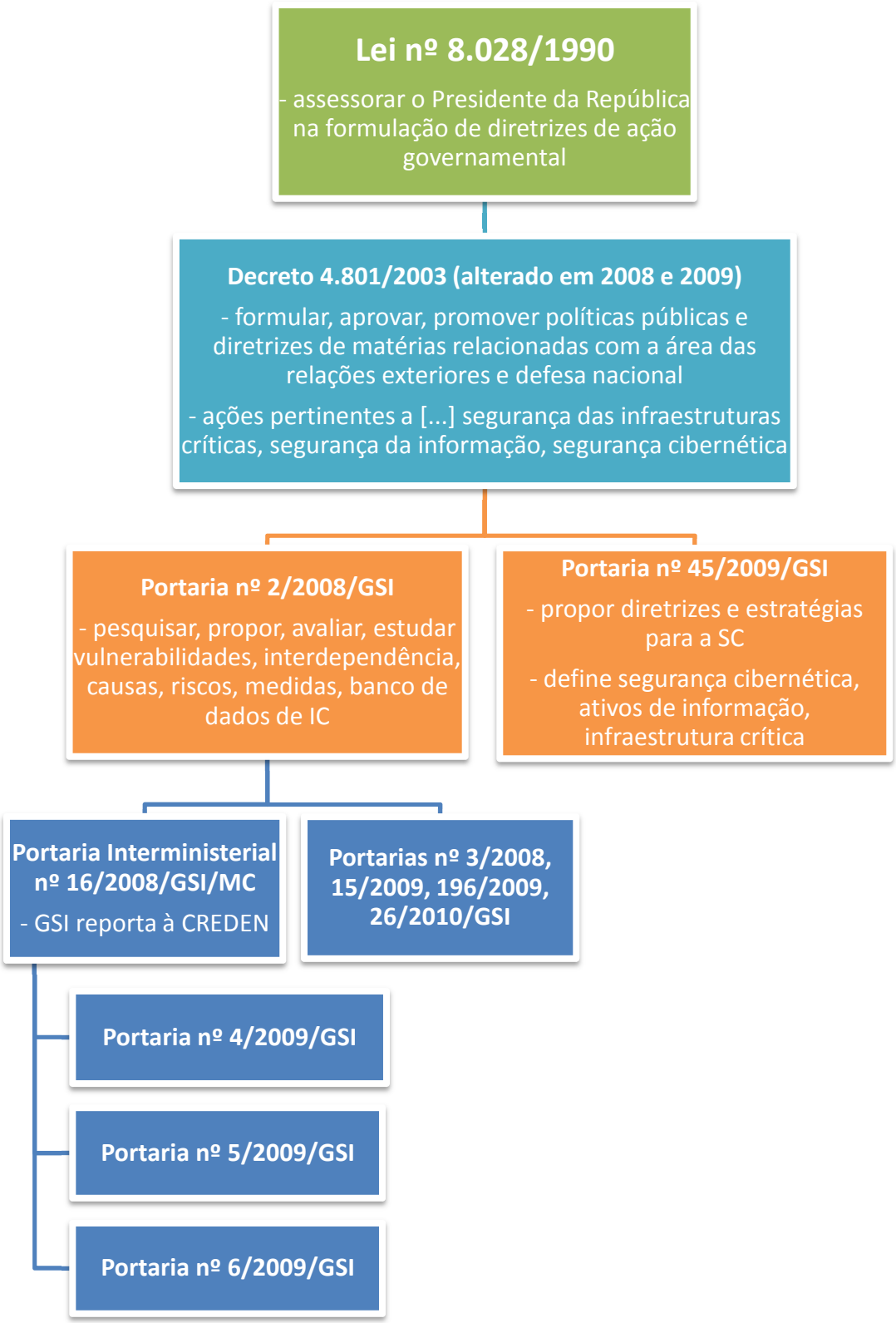
WikiLeaks divulga locais "vitais" para segurança dos EUA; Brasil está incluso http://www1.folha.uol.com.br/mundo/841393-wikileaks-divulga-locais-vitais-para-seguranca-dos-eua-brasil-esta-incluso.shtml.

WikiLeaks Releases Secret List of Critical Infrastructure Sites http://www.wired.com/threatlevel/2010/12/critical-infrastructures-cable/.

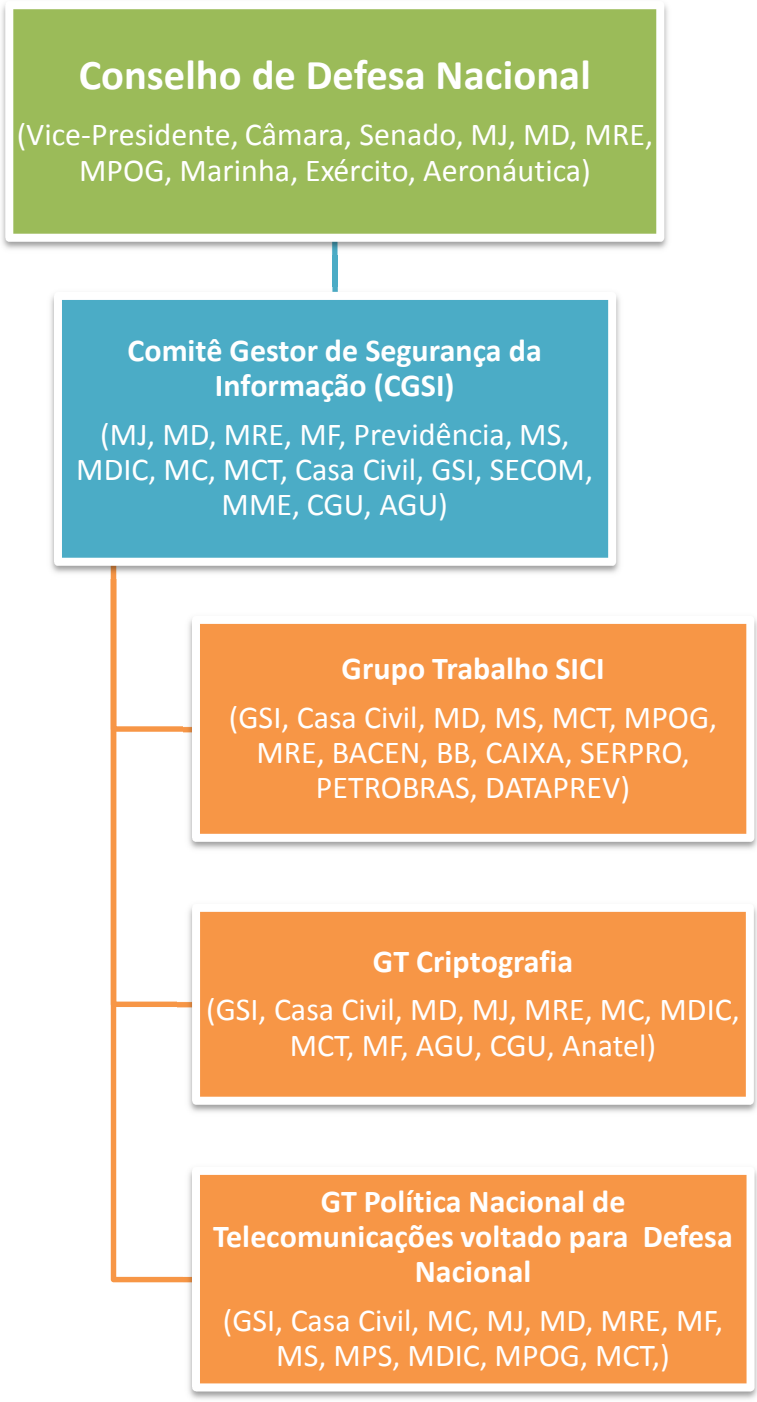
ANEXOS

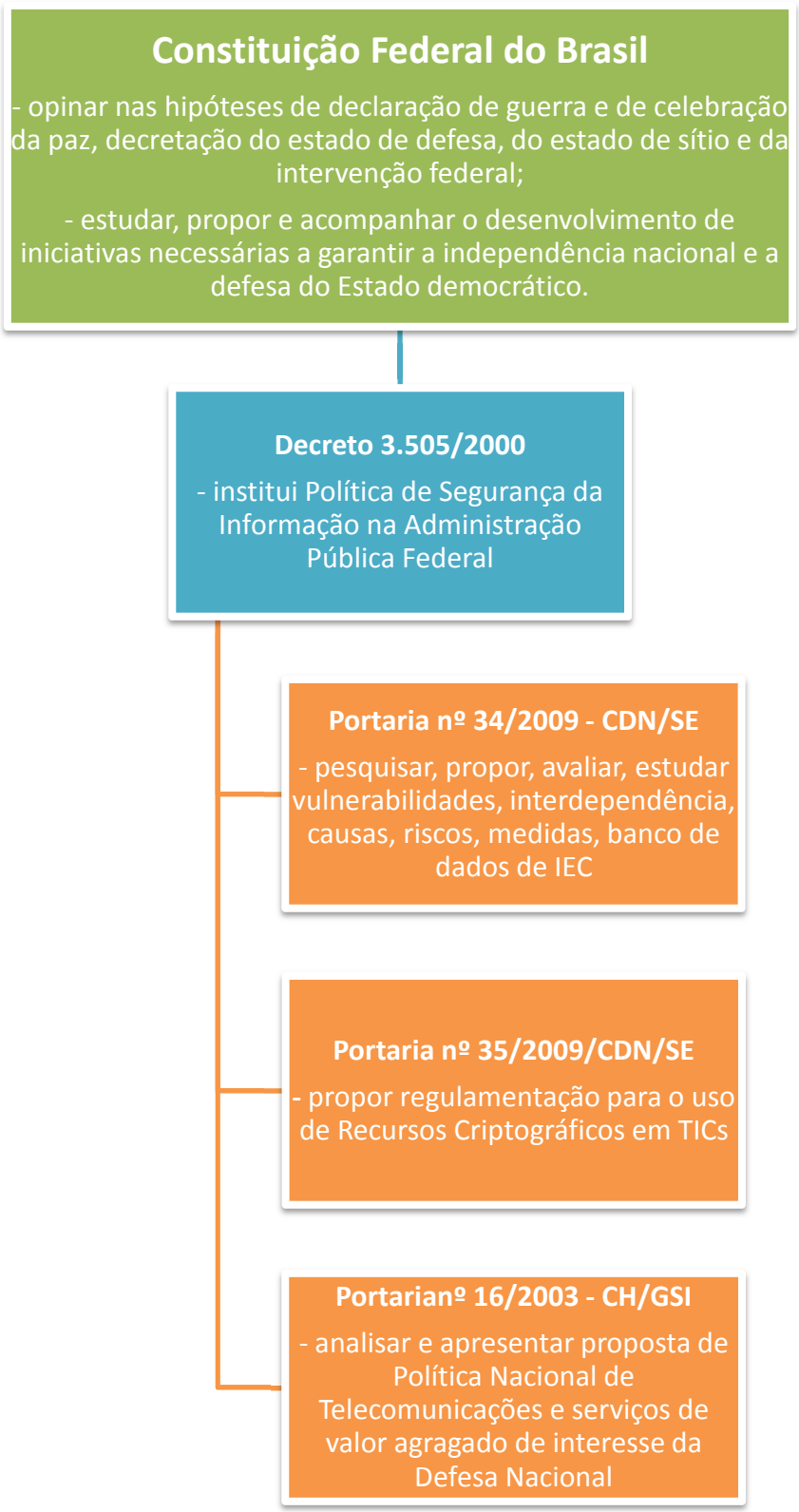
ANEXO I – Organogramas CREDEN/Conselho de Governo




Lei nº 8.028/1990
- assessorar o Presidente da República na formulação de diretrizes de ação governamental
Decreto 4.801/2003 (alterado em 2008 e 2009)
- formular, aprovar, promover políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional
- ações pertinentes a [...] segurança das infraestruturas críticas, segurança da informação, segurança cibernética
Portaria nº 2/2008/GSI
- pesquisar, propor, avaliar, estudar vulnerabilidades, interdependência, causas, riscos, medidas, banco de dados de IC
Portaria nº 45/2009/GSI
- propor diretrizes e estratégias para a SC
- define segurança cibernética, ativos de informação, infraestrutura crítica
Portaria Interministerial nº 16/2008/GSI/MC
- GSI reporta à CREDEN
Portarias nº 3/2008, 15/2009, 196/2009, 26/2010/GSI
Portaria nº 4/2009/GSI
Portaria nº 5/2009/GSI
Portaria nº 6/2009/GSI

ANEXO II – Organogramas CGSI/Conselho de Defesa Nacional




Constituição Federal do Brasil
- opinar nas hipóteses de declaração de guerra e de celebração da paz, decretação do estado de defesa, do estado de sítio e da intervenção federal;
- estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.
Decreto 3.505/2000
- institui Política de Segurança da Informação na Administração Pública Federal
Portaria nº 34/2009 - CDN/SE
- pesquisar, propor, avaliar, estudar vulnerabilidades, interdependência, causas, riscos, medidas, banco de dados de IEC
Portaria nº 35/2009/CDN/SE
- propor regulamentação para o uso de Recursos Criptográficos em TICs
Portarianº 16/2003 - CH/GSI
- analisar e apresentar proposta de Política Nacional de Telecomunicações e serviços de valor agragado de interesse da Defesa Nacional