ALMEIDA ADVOGADOS
DIREITO CORPORATIVO
BRASIL

SÃO PAULO
RIO DE JANEIRO
BRASÍLIA
BELO HORIZONTE

ESTUDO

Experiência, Comprometimento, Capilaridade e Entendimento

DIREITO CORPORATIVO

Segurança Cibernética no Brasil

1. INTRODUÇÃO

Esse estudo tem o objetivo de trazer uma abordagem geral acerca do tema defesa cibernética.

Ao longo desse documento, apresentaremos os maiores agentes do setor, assim como os documentos e diretrizes mais importantes no Brasil.

Para o estudo do tema, nos focamos em aspectos relacionados à guerra cibernética e à segurança cibernética.

O estudo foi dividido em três partes centrais:

- ➔ A primeira parte do estudo será dedicada à apresentação dos principais atores que lidam com defesa cibernética no Brasil;
- ➔ A segunda parte busca ilustrar o cenário jurídico atual (quase que inteiramente baseado em *"soft laws");*
- ➔ As considerações finais e a conclusão serão focadas em algumas questões críticas identificadas durante nossa pesquisa e análise do tema.

2. ASPECTOS GERAIS DA SEGURANÇA CIBERNÉTICA

A discussão sobre segurança cibernética nos leva a 2008, um ano marcante, considerado por muitos como um divisor de água do tema.

Neste ano, o Governo Brasileiro adotou, com o Decreto nº. 6.703/08, a **Estratégia de Defesa Nacional**, que classificou três setores estratégicos – espacial, cibernético e nuclear – como essenciais para a defesa nacional.

O Brasil escolheu deliberadamente atribuir às Forças Armadas a responsabilidade e competência pela segurança cibernética. Uma das principais razões para tal escolha foi o fato que a força militar está sendo reestruturada e está em busca de um novo papel como protagonista no cenário político do Século XXI, assim como em muitos países ao redor do mundo.

Em 2013, dois outros fatos relevantes reinteraram a preferência do Governo Brasileiro por seguir o caminho das Forças Armadas para a segurança cibernética. No âmbito internacional, após Edward Snowden revelar que as redes oficiais de comunicação do Brasil foram espionadas pela National Security Agency (NSA), o país reforçou suas medidas de segurança contra espionagem cibernética e guerra cibernética. Ao mesmo tempo, no âmbito nacional, os grandes protestos que ocorreram entre Junho e Agosto de 2013 coincidiram com o aumento no *hacktivismo*, o que foi considerado como uma ameaça para a segurança nacional.

Essa abordagem pode – em longo prazo – não se revelar a mais correta. Enquanto recursos são focados em soluções militares mais adequadas para casos excepcionais de guerra, uma das maiores ameaças do espaço cibernético brasileiro é o crime organizado (especialmente os movidos economicamente). Além disso, uma abordagem militarizada pode colocar em

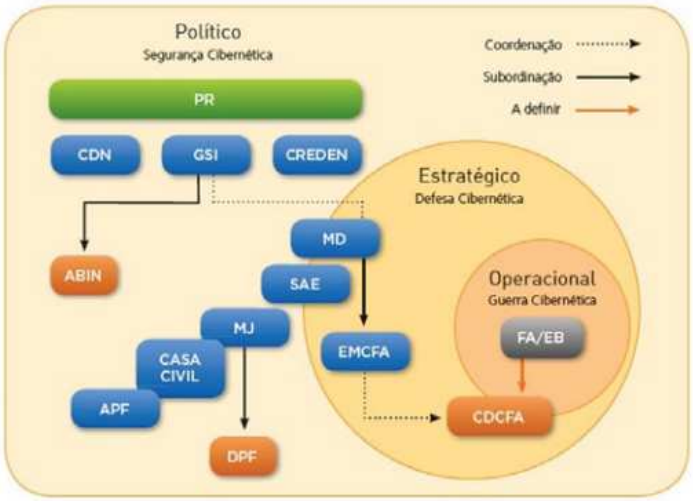
perigo outro importante *acquis* democrático, como o direito à privacidade, a neutralidade de rede e, mais amplamente, os direitos fundamentais dos cidadãos.

Como será destacado abaixo, o marco institucional e regulatório brasileiro sobre defesa cibernética é bastante disperso, visto que diversos órgãos estão envolvidos e muitos textos *"soft law"* foram adotados. É possível afirmar que, até agora, o Brasil não tem um quadro jurídico consolidado sobre guerra cibernética e segurança cibernética. **PRINCIPAIS ATORES**

3.1. Atores Institucionais

No nível macro, os principais atores institucionais envolvidos com defesa cibernética no Brasil são a Presidência (principalmente via o Gabinete de Segurança Institucional), o Ministério da Defesa e o Ministério da Justiça. O último é a autoridade competente pelos Crimes Cibernéticos (por meio de unidades da Polícia Federal dedicadas a esse tipo de infração) e o seu papel não será desenvolvido neste estudo, considerando que o nosso foco é diverso.

Abaixo, você poderá ver uma tabela ilustrando a arquitetura da segurança cibernética brasileira.[1]



[1] Tabela obtida da publicação: "*República Federativa do Brasil, Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações (2010). Livro Verde da Segurança Cibernética no Brasil. Mandarino, R. and Canongia, C. (Eds). Brasília.*"

LEGENDA:

PR: Presidência da República
GSI: Gabinete de Segurança Institucional
CDN: Conselho de Defesa Nacional
ABIN: Agência Brasileira de Inteligência

.1.1. Presidência

3.1.1.1. Conselho de Defesa Nacional

Órgão de consulta da Presidência da República em assuntos relacionados à soberania e à defesa nacional.

3.1.1.2. Gabinete de Segurança Institucional (GSI – PR)

O GSI, diretamente sob o comando do Gabinete da Presidência, é responsável pela segurança cibernética (questões relacionadas a civis), assuntos militares e defesa cibernética.

3.1.1.3. Departamento de Segurança da Informação e Comunicações (DSIC)

Ramo subordinado ao GSI – PR. É responsável por garantir a disponibilidade, integridade, confidencialidade e autenticidade de informações e comunicações para a Administração Pública Federal.

3.1.1.4. Secretaria de Assuntos Estratégicos (SAE) e Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN)

Há órgãos consultivos no Gabinete da Presidência, também encarregados de questões *inter alia* da segurança cibernética.

Em 2010, o DSIC, SAE e CREDEN elaboraram o Livro Verde sobre segurança cibernética no Brasil.

3.1.2. Ministério da Defesa

O Ministério da Defesa é responsável pelas Forças Armadas. O Estado-Maior Conjunto das Forças Armadas (EMCFA) coordena a resposta aos ataques cibernéticos.

Um papel de extrema importância no campo da defesa cibernética nesse Ministério é certamente detido pelo Centro de Defesa Cibernética (CDCiber).

Esse órgão, diretamente colocado sob o comando do Exército, foi criado em 2010 e é a primeira unidade militar dedicada a questões cibernéticas na América Latina. É a agência que coordena a defesa cibernética no Brasil e opera diretamente com o Ministério da Defesa, que, por sua vez, implementa as diretivas do GSI – PR.

O CDCiber coordena atividades de todas as divisões das Forças Armadas que lidam com questões tecnológicas e de inteligência. Tem a tarefa de proteger as redes públicas e militares de ataques cibernéticos e, em longo prazo, estará responsável por proteger toda a estrutura informática nacional. Ocasionalmente, também é responsável por proteger a rede de grandes eventos, como a Conferência Rio+20 de 2012, a Copa do Mundo de 2014, e as Olimpíadas do Rio de Janeiro de 2016.

3.2. Outros atores

3.2.1. Comitê Gestor da Internet no Brasil (CGI.br)

O Comitê Gestor da Internet no Brasil (CGI.br) está encarregado da coordenação e integração de todas as iniciativas de serviços da internet no país, assim como da promoção da qualidade técnica, inovação e disseminação dos serviços disponíveis. Também contribui com os debates sobre defesa cibernética.

3.2.2. Os CSIRT (CERT.br)

CERT.br é o Centro de Estudos, Resposta de Tratamento de Incidentes de Segurança no Brasil, mantido pelo NIC.br – o ramo executivo do Comitê Gestor da Internet.

CERT.br é responsável por lidar com informações sobre incidentes de segurança e atividade relacionadas as redes brasileiras conectadas a Internet. É um ponto de foco para notificações de incidentes no país, fornecendo a coordenação e suporte necessários para organizações envolvidas em incidentes.

Além da gestão de incidentes, o CERT.br também trabalha para aumentar a consciência da população sobre a questão da segurança cibernética, mantendo um projeto de alerta precoce com o objetivo de identificar novas tendências e eventos de segurança correlacionados, assim como alertar as redes brasileiras envolvidas em atividades maliciosas.

CERT.br é responsável por ajudar novos Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs) a estabelecer suas atividades no país.

4. MARCO REGULATÓRIO

Como mencionado nos comentários introdutórios deste estudo, o marco regulatório brasileiro existente sobre segurança cibernética é constituído principalmente por *soft laws.* Diversos documentos oficiais estão disponíveis, mas eles são mais descritivos do que prescritivos.

4.1. Livro Verde sobre Segurança Cibernética no Brasil (2010)

O Livro Verde sobre Segurança Cibernética no Brasil foi elaborado por um Grupo Técnico do GSI. O trabalho ressalta aspectos fundamentais da segurança cibernética no país e constitui uma primeira tentativa de estabelecer os princípios da futura Política de Segurança Cibernética. Nesse documento, segurança cibernética é vista mais como um desafio internacional do que como uma questão nacional. Partindo dessa premissa, o Livro Verde refere-se a inúmeras estratégias internacionais adotadas por organizações internacionais como a Organisation of American States (OAS), a Organisation for Economic Co-Operation and Development (OECD) e do International Telecommunication Union (ITU).

Além disso, o documento salienta a importância de envolver diferentes partes interessadas na discussão, também incluindo os atores não estatais, privilegiando, assim, a abordagem multissetorial. Uma atenção especial é dada à importância de se desenvolver programas educacionais para usuários e, mais em geral, uma campanha nacional de consciência sobre segurança cibernética.

O Livro Verde considera que segurança cibernética se relaciona com a proteção do espaço cibernético, a proteção de seus ativos de informação e suas infraestruturas críticas. O

conceito de “infraestrutura crítica” tem uma conotação mais ampla que “recursos críticos da Internet”. Infraestrutura Crítica se relaciona com “as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade.” Por exemplo, isso inclui energia, transporte, água, telecomunicação, finanças, informação e outros setores. Recursos Críticos da Internet fazem parte da Infraestrutura Crítica. Segurança cibernética é muito maior do que a proteção da infraestrutura técnica.

O documento foi colocado em consulta pública para que qualquer parte interessada pudesse elaborar comentários. Não obstante estes esforços, o Plano Nacional para Segurança da Infraestrutura do qual o Livro Verde deveria ter sido precursor ainda não foi adotado, mas está sob discussão.

4.2. Política de Segurança Cibernética (2012)

A Política de Segurança Cibernética brasileira foi elaborada pelo Ministério da Defesa em 2012 para guiar suas atividades e procedimentos relacionados à defesa cibernética e guerra cibernética nos níveis estratégicos, operacionais e táticos.

O documento ressalta os princípios, objetivos e orientações para a consolidação da segurança cibernética no domínio da defesa nos próximos anos. O Exército ficará responsável pelo desenvolvimento e implementação de

estratégias de defesa cibernética e o espaço cibernético brasileiro deve ser melhorado, promovendo o desenvolvimento da
capacidade, conhecimento de produção e inteligência. O documento também destaca que é importante não apenas responder a ameaças cibernéticas, mas também investir em educação, indústria, ciência e tecnologia da inovação.

As diretrizes estabelecidas nessa Política devem constituir a base para uma legislação mais específica do assunto.

4.3. Livro Branco de Defesa Nacional (2012)

Esse documento, elaborado após consultas com o governo e a sociedade, esboça os objetivos da Política de Defesa Nacional nas próximas décadas.

Sobre segurança cibernética, o Livro prevê a instalação de um Centro de Defesa Cibernética e despesas de aproximadamente 840 milhões de reais até 2035.

4.4. Outras iniciativas

O Ministério da Defesa propôs a criação de uma Escola Nacional da Defesa Cibernética, cujo projeto está sendo elaborado atualmente.

Em 2014, o Ministério da Ciência e da Tecnologia, ao lado do Ministério da Defesa por meio de uma portaria interministerial, lançou um projeto para criar fundos de recursos para novos empreendimentos especializados em segurança cibernética.

Nos níveis internacionais e regionais, o Brasil assinou o Acordo de Defesa Cibernética ("*Cyber-defense Agreement*") com a Argentina em 2011. No mesmo ano, também assinou um Acordo de Não Agressão por Armas da Informação ("*Agreement of Non-Aggression by Information Weapons*") com a Rússia. O Brasil também se envolveu em iniciativas de cooperação dentro da estrutura da União das Nações Sul-Americanas (UNASUR), a Organização dos Estados Americanos (OAS) e com os outros países dos BRICS.

5. CONSIDERAÇÕES FINAIS

A segurança cibernética é, sem dúvida, um tópico importante para o Brasil no momento, mesmo que os esforços para adotar um marco regulatório mais harmonizado e consolidado não tenham sido bem sucedidos até agora.

O marco regulatório brasileiro sobre segurança cibernética ainda está evoluindo, sendo caracterizado por linhas conflitantes de responsabilidade entre as instituições envolvidas, além de certa falta de coordenação entre eles.

A ausência de uma legislação nacional uniforme em relação a segurança cibernética é um dos maiores obstáculos que devem ser superados se o governo brasileiro planeja ter um papel maior no cenário internacional.

Enquanto os principais atores estão em vigor, suas competências e jurisdições ainda não estão claramente definidas. A Polícia Federal é responsável por Crimes Cibernéticos, enquanto o Exército é responsável pela guerra cibernética e segurança cibernética. Contudo, pode ser difícil distinguir, considerando que a linha entre essas atribuições pode ser difícil de se estabelecer.

O Exército tomou a liderança nesse debate, mas a abordagem ainda está muito compartimentada e precisa estar mais integrada. Uma abordagem militar também pode não ser uma das mais apropriadas considerando os riscos reais envolvidos e a possibilidade de diminuir as liberdades civis. O Brasil está consideravelmente investindo na melhoria das capacidades militares cibernéticas, mas pode existir uma lacuna entre os esforços do Governo Brasileiro com foco na guerra cibernética, quando, na verdade, o país não é um alvo do terrorismo cibernético, ao invés de se focar em ameaças mais reais – como a Crimes Cibernéticos – e se focar no cumprimento e aplicação das leis.

É importante incluir na discussão os setores publico e privado, a indústria de defesa, parceiros acadêmicos e a sociedade civil, como o CGI e sua natureza mista busca fazer. Apesar de casos esporádicos, a ligação da sociedade civil com os problemas da segurança cibernética foi limitada até o momento. Nesse contexto, e considerando que a penetração da internet no Brasil é de 54,2%, segundo dados de 2013, é de extrema importância o desenvolvimento de uma comunicação limpa estratégia educacional, e o aumento da consciência sobre a segurança cibernética, criando, assim, a base para um debate qualitativo.

Permanecemos à disposição de nossos clientes para eventuais esclarecimentos que se falam necessários.

Cordialmente,

Almeida Advogados