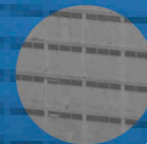


DESENVOLVIMENTO DE POLÍTICAS DE CIBERSEGURANÇA E CIBERDEFESA NA AMÉRICA DO SUL

ESTUDO DE CASO SOBRE A ATUAÇÃO
GOVERNAMENTAL BRASILEIRA



ARTICLE 19

Equipe ARTIGO 19 Brasil

Diretora-executiva

Paula Martins

Acesso à Informação

Joara Marchezini

Bárbara Paes

Henrique Goes

Paulina Bustos Arellano

Ester Borges Santos

Proteção e Segurança

Júlia Lima

Thiago Firbida

Raphael Concli

Direitos Digitais

Laura Tresca

Marcelo Blanco dos Anjos

Centro de Referência Legal

Camila Marques

Raissa Maia

Fabio Pereira

Mariana Rielli

Comunicação

João Ricardo Penteado

Rodrigo Emannuel

Vitória Oliveira

Administrativo e Financeiro

Regina Marques

Rosimeyri Carminati

Yumna Ghani

Sofia Riccardi

Conselho Administrativo e Fiscal

Eduardo Panuzzio

Luiz Eduardo Patrone Regules

Malak El Chichini Poppovic

Luciana Cesar Guimarães

Belisário dos Santos Júnior

Marcos Roberto Fuchs

Thiago Lopes Ferraz Donnini

Heber Augusto Ivanoski de Araujo

Licença da obra: CC 3.0 BY-SA

Ícones disponíveis em: <http://bit.ly/2pP08Xw>

Link da licença: https://creativecommons.org/licenses/by-sa/3.0/deed.pt_BR



Ficha técnica

Título: Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul - Estudo de caso sobre a atuação governamental brasileira

Realização: ARTIGO 19

Supervisão: Paula Martins

Coordenação executiva e editorial: Laura Tresca

Redação e análise: Marcelo Blanco

Design gráfico: Ricardo Kuraoka

Agradecimentos: Eduardo Ferreyra, Leandro Ucciferri e Maricarmen Sequera



Índice

Introdução	7
Padrões Internacionais.....	9
Relevantes de Direitos Humanos	9
Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul	18
Pedidos de Informação	26
Relações Bilaterais Brasil-Argentina	29
Relações Multilaterais: Mercosul	34
Relações Multilaterais: UNASUL.....	37
Relações Multilaterais: OEA.....	41
Relações Multilaterais: Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas	45
Pedidos de Informação no Paraguai e Argentina.....	48
Considerações finais	51
Sobre a ARTIGO 19.....	55





Introdução

Diversas iniciativas de cooperação internacional sobre defesa cibernética surgiram na América do Sul neste início do século XXI. O debate sobre a agenda aqueceu-se consideravelmente no período imediatamente posterior às denúncias de coleta massiva de dados e de espionagem feitas por Edward Snowden em 2013.

Notícias veiculadas ainda em 2013 afirmavam que o Brasil e países vizinhos buscariam adotar medidas de defesa cibernética no interior dos principais organismos internacionais regionais, como o MERCOSUL e a UNASUL. O chanceler brasileiro à época, Antonio Patriota, chegou a afirmar que o MERCOSUL buscaria adotar uma regulamentação comum sobre ciberdefesa.

Vale ressaltar que nesse estudo os termos ciberdefesa e cibersegurança utilizados neste estudo buscam assimilar uma pequena diferença conceitual ainda em disputa. Ao mencionar o termo ciberdefesa, nos referimos às ações da área de defesa nacional, à proteção contínua de infraestruturas críticas, como o sistema de abastecimento de água e de energia, contra ataques de adversários externos ou internos.¹ A todo o momento, as operações de ciberdefesa interseccionam-se às

1 Esta é uma definição similar àquela encontrada no “Cyber Defence Pledge” da OTAN, um documento de 2016 que estabelece as diretrizes da organização para a área. Já o termo cibersegurança é mais amplo, adotado por atores não estatais, e significa a proteção de qualquer rede, hardware, software ou informação de ameaças externas que possam comprometê-los total ou parcialmente.

de cibersegurança e as políticas adotadas não levam em consideração tal diferenciação. Este estudo busca analisar principalmente as ações de ciberdefesa, mas é necessário apontar tal dificuldade². O então Ministro da Defesa brasileiro, Celso Amorim, declarou dois meses depois que uma medida similar seria adotada no âmbito da UNASUL. Outras iniciativas bilaterais também são objeto deste estudo e serão mais detalhadas nas seções seguintes. Contudo, nos anos seguintes a essa movimentação, poucas informações sobre tais arranjos foram divulgadas.

Este documento, portanto, pretende abordar o tema da defesa cibernética com o objetivo de transparecer o desenvolvimento das articulações regionais e bilaterais reportadas à época. Pedidos de informação foram enviados para autoridades de Brasil, Argentina e Paraguai por três organizações de cada um dos países às suas respectivas autoridades competentes em busca de informações sobre o atual estado dessas iniciativas.

A partir de uma pesquisa sobre os organismos internacionais regionais e notícias de cooperações intergovernamentais, foram formulados e enviados oito pedidos de informação sobre a atuação internacional do Brasil. O foco das questões foram as articulações realizadas no MERCOSUL, na UNASUL, na OEA, nas relações bilaterais entre Brasil e Argentina e na realização do 1º Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas em 2017 pelo Brasil. Perguntou-se às autoridades o presente estado das iniciativas nessas organizações internacionais (OIs), o quanto os governos estariam ativos nas articulações desenvolvidas, assim como os aportes financeiros realizados.

Além do estabelecimento do panorama de iniciativas, faz-se também uma análise do nível de transparência dos pedidos de informação feitos aos órgãos públicos, conforme a precisão de suas respostas e o tempo levado para a obtenção da informação requerida.

A preocupação principal da ARTIGO 19 é que a implantação ou não dessas políticas acarrete em violações sistemáticas aos direitos à privacidade e à liberdade de expressão, pelo que devem ser levadas adiante com transparência e participação.

■ 2 Para mais informações sobre tal distinção, acesse: https://www.academia.edu/23986861/CYBER_SECURITY_VS._CYBER_DEFENSE_A_PORTUGUESE_VIEW_ON_THE_DISTINCTION



Padrões Internacionais Relevantes de Direitos Humanos

Direito à liberdade de expressão e informação

O direito à liberdade de expressão e de informação (liberdade de expressão) protege o livre fluxo de informações, opiniões e ideias, sendo aplicado a todos os meios e independentemente de fronteiras. Ele inclui o direito não só de transmitir, mas também de buscar e receber informações. A liberdade de expressão tem sido reconhecida como fundamental tanto para a autonomia individual quanto para uma sociedade livre em geral.³

O direito à liberdade de expressão é reconhecido em quase todas as constituições nacionais e na maioria dos tratados internacionais de direitos humanos, incluindo a Declaração Universal dos Direitos Humanos (DUDH)⁴, o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP)⁵, a Carta Africana dos Direitos Humanos e dos Direitos dos Povos (Carta Africana)⁶, a Declaração Americana dos Direitos e Deveres do Homem (Declaração Americana), a Convenção

3 Ver e.g. Tribunal Europeu dos Direitos Humanos (Corte Europeia), *Handyside v Reino Unido*, Appl. não. 5493/72, parágrafo 49, 07 de dezembro de 1976.

4 Artigo 19 da DUDH.

5 Artigo 19 da PIDCP.

6 Artigo 9 da Carta Africana.

Americana sobre Direitos Humanos (Convenção Americana)⁷ e a Convenção Europeia dos Direitos Humanos (Convenção Europeia)⁸.

No Comentário Geral nº 34, a Comissão de Direitos Humanos da ONU (Comitê HR) – órgão que oficialmente interpreta o escopo das obrigações dos Estados sob o PIDCP – reafirmou que a liberdade de expressão é essencial para o gozo de outros direitos humanos e confirmou que o artigo 19 do PIDCP protege todas as formas de expressão e os meios de sua divulgação, incluindo todos os modos de expressão baseados por meios eletrônicos e Internet.⁹

Em outras palavras, a liberdade de expressão online é protegida do mesmo modo que está protegida offline. No entanto, essa liberdade não é absoluta, e as normas internacionais deixam claro que, apesar de ser um direito qualificado, pode ser limitado, desde que a restrição esteja em conformidade com um teste de três partes. A restrição deve:

- ser prevista por lei;
- perseguir objetivos legítimos, explicitamente enumerados no artigo 19 do PIDCP; e
- ser necessária em uma sociedade democrática. Em particular, o requisito da necessidade implica que a medida adotada deve ser proporcional ao objetivo que se almeja. Se uma medida menos intrusiva é capaz de alcançar a mesma finalidade que uma mais restritiva, a medida menos restritiva deve ser aplicada.

Direito à privacidade

A privacidade é um conceito amplo relativo à proteção da autonomia individual e da relação entre o indivíduo e a sociedade, incluindo governo, empresas e particulares. Ela abrange uma ampla gama de direitos, incluindo proteções de intrusões na vida privada e familiar, o controle sobre direitos sexuais e reprodutivos e o sigilo das comunicações¹⁰. É comumente reconhecida como um

7 Artigo 4 da Declaração Americana.

8 Artigo 13 da Declaração Americana.

9 Comitê de Direitos Humanos, Comentário Geral No.34, CCPR/C/GC/34, adotado em 12 de setembro de 2011, para 12.

10 Ver, por exemplo, Tribunal Europeu dos Direitos Humanos (Corte europeia), Handyside contra Reino Unido, Appl. Nao. 5493/72, Parágrafo 49, 07 de dezembro de 1976.

direito fundamental subjacente à dignidade humana e a outros valores, como a liberdade de expressão e a liberdade de associação¹¹.

O direito à privacidade é reconhecido na maioria dos tratados internacionais de direitos humanos¹² e em quase todas as constituições nacionais¹³. Ele já foi resguardado em julgamentos por organismos internacionais e regionais¹⁴, sendo também legalmente protegido em nível nacional através de disposições nos códigos civis e/ou criminais¹⁵.

Nas Américas, muitas nações têm formalizado direitos de privacidade, seja nas constituições ou leis, sob Habeas Data, fornecendo aos indivíduos o direito de, nas palavras da Comissão Interamericana de Direitos Humanos, “modificar, remover ou corrigir informações devido à sua natureza sensível, errônea, tendenciosa ou discriminatória” sobre sua pessoa.

O direito à privacidade não é absoluto e está sujeito ao mesmo teste de três partes, a saber: legalidade, necessidade e proporcionalidade.¹⁶

Os 13 princípios internacionais sobre a aplicação dos direitos humanos na vigilância das comunicações

Em 2013, grupos da sociedade civil, da indústria e especialistas internacionais em questões jurídicas, políticas e tecnológicas relacionadas à vigilância das comunicações se reuniram e formularam 13 princípios que buscam esclarecer

- 11 Ver e.g. Comitê de RH, CCPR Comentário Geral nº 16 sobre o artigo 17 (direito à privacidade), o direito ao respeito da privacidade, família, domicílio e da correspondência, e Proteção da Honra e da Reputação, 8 de abril de 1988; Conselho de Direitos Humanos das Nações Unidas, Relatório do Relator Especial sobre a promoção e proteção dos direitos humanos e liberdades fundamentais na luta contra o terrorismo (SR em RH e luta contra o terrorismo), A / HRC / 13/37, 28 de Dezembro de 2009; ver também Tribunal Europeu, *Bensaid v Reino Unido*, App. No. 44599/98 [2001] CEDH 82.
- 12 O artigo 12 da DUDH; O artigo 17 do PIDCP, artigo 8 da Convenção Europeia, o artigo 5, 9 e 10 da Declaração Americana sobre Direitos Humanos e o artigo 11 da Carta Africano.
- 13 Ver e.g. Departamento de Estado dos EUA, de 2010 Relatório Nacional sobre Direitos Humanos Práticas, Abril de 2011.
- 14 Ver e.g. Comitê de RH, Observações Finais sobre Holanda, CCPR / C / 82 / D / 903/1999 [2004] UNHRC 60 (15 Novembro 2004); Corte Interamericana de Direitos Humanos (Corte IDH), *Escher et al. v Brasil*, 9 de Julho de 2009.; ou um resumo da jurisprudência Tribunal Europeu sobre a proteção de dados.
- 15 Departamento de Estado dos EUA, 2010 Relatório de Direitos Humanos, op.cit.; Privacidade e Direitos Humanos, op.cit; Glasser (ed.), *Libel Internacional e Manual de Privacidade* de 2006.
- 16 Relatório do SR em RH e luta contra o terrorismo.

como os direitos humanos se aplicam ao ambiente digital, especialmente considerando o aumento e as alterações técnicas e tecnológicas da vigilância das comunicações. Eles oferecem a grupos da sociedade civil, empresas, Estados e a outros atores um instrumento para avaliar se as leis e práticas atuais ou propostas sobre monitoramento são consistentes ou não com os direitos humanos.

Assim, para que os Estados possam cumprir seus deveres no que diz respeito à vigilância das comunicações, assim como pensar suas estratégias de cibersegurança e ciberdefesa, eles devem observar cada um dos princípios abaixo:

Princípio 1: Legalidade

Qualquer limitação aos direitos humanos deve ser disposta em lei. O Estado não deve adotar ou implementar uma medida que interfere no direito à privacidade na ausência de um dispositivo legal disponível ao público e que atinja um nível de precisão e clareza suficiente para garantir que indivíduos possam prever sua aplicação. Dada a velocidade das mudanças tecnológicas, as leis que autorizam limitações aos direitos humanos devem ser sujeitas à revisão periódica por meio de um processo legislativo ou regulamentar participativo.

Princípio 2: Fim Legítimo

As leis só devem permitir a vigilância das comunicações por autoridades estatais específicas para atingir um interesse legítimo de suma importância que corresponda a um interesse necessário em uma sociedade democrática. Qualquer medida não pode ser aplicada de forma discriminatória com base em raça, cor, sexo, língua, religião, opiniões políticas e demais opiniões, nacionalidade ou origem social, propriedade, nascimento ou qualquer estado.

Princípio 3: Necessidade

As leis, regulamentos, atividades, poderes ou autoridades de vigilância devem se limitar ao que é estrito e comprovadamente necessário para atingir um fim legítimo. A vigilância das comunicações só deve ser conduzida quando for a

única forma de atingir um fim legítimo, ou, caso haja múltiplas formas, que seja a forma de menor impacto aos direitos humanos. O ônus de estabelecer esta justificativa recai sempre sobre o Estado.

Princípio 4: Adequação

Qualquer instância de vigilância das comunicações autorizada por lei deve ser apropriada para realizar o fim legítimo identificado.

Princípio 5: Proporcionalidade

A vigilância das comunicações deve ser considerada um ato altamente intrusivo que interfere nos direitos humanos, ameaçando os fundamentos de uma sociedade democrática. As decisões sobre a vigilância das comunicações devem envolver uma consideração sobre a sensibilidade da informação e a gravidade da infração aos direitos humanos e outros interesses concorrentes.

Isso requer que um Estado, no mínimo, estabeleça os seguintes pontos à autoridade judicial competente, antes de realizar a vigilância das comunicações com o objetivo de cumprir a lei, proteger a segurança nacional ou recolher dados de inteligência:

- existe uma alta probabilidade de que um crime grave ou ameaça específica a um fim específico foi ou será cometido, e;
- existe alta probabilidade de que evidências ou materiais relevantes para tal crime grave ou ameaça específica a um fim legítimo seriam obtidos acessando as informações protegidas procuradas, e;
- outras técnicas menos invasivas foram esgotadas ou seriam inúteis, de forma que as técnicas utilizadas sejam a opção menos invasiva, e;
- as informações acessadas serão limitadas ao que é relevante e essencial ao crime grave ou ameaça específica ao fim legítimo alegado; e
- quaisquer informações coletadas a mais não serão mantidas, mas, pelo contrário, serão prontamente destruídas ou devolvidas; e

- as informações serão acessadas somente pela autoridade especificada e usadas apenas para a finalidade e pela duração para as quais foi concedida a autorização; e
- as atividades de vigilância solicitadas e técnicas propostas não comprometem a essência do direito à privacidade ou às liberdades fundamentais.

Princípio 6: Autoridade Judicial Competente

As determinações relativas à vigilância das comunicações devem ser expedidas por uma autoridade judicial competente que seja imparcial e independente. Essa autoridade deve ser:

1. separada e independente das autoridades que realizam a vigilância das comunicações;
2. familiarizada com os assuntos relacionados e competente para expedir decisões judiciais sobre a legalidade da vigilância das comunicações, as tecnologias utilizadas e os direitos humanos; e
3. ter recursos adequados ao exercer as funções que lhe são atribuídas.

Princípio 7: Devido Processo Legal

O devido processo legal requer que Estados respeitem e garantam os direitos humanos de uma pessoa ao assegurar que os procedimentos legais que interferem nos direitos humanos sejam feitos de acordo com a lei, e que esta seja respeitada e esteja disponível para o público em geral. Especificamente no que diz respeito aos direitos humanos do indivíduo, todos têm direito a uma audiência pública e justa dentro de um tempo razoável, realizada em um tribunal independente, competente e imparcial, estabelecido por lei, excetuando-se os casos de emergência nos quais há risco ou perigo iminente para a vida humana. Em tais casos, devem ser buscadas autorizações retroativas dentro de um período razoável e cabível. O mero risco de perecimento ou destruição de evidências nunca deve ser considerado como suficiente para justificar autorização retroativa.

Princípio 8: Notificação do Usuário

Aqueles cujas comunicações estão sendo vigiadas devem ser notificados da decisão que autoriza a vigilância das comunicações dentro de um tempo suficiente e ter informações necessárias para permitir-lhes o recurso contra as decisões ou a busca de outras medidas, e devem ter acesso a materiais apresentados juntamente com o pedido da autorização. O atraso na notificação só é justificado nas seguintes circunstâncias:

1. a notificação tornaria totalmente inepto o propósito para o qual a vigilância das comunicações é autorizada ou em caso de haver perigo iminente à vida humana, e;
2. a autorização para o atraso na notificação for autorizada pelo órgão judicial competente; e
3. o usuário afetado seja notificado o mais cedo possível quando o risco cessar ou quando determinado pela autoridade judicial competente.

A obrigação para a notificação recai sobre o Estado, mas os provedores de serviços de comunicação estarão livres para notificar indivíduos sobre a vigilância de comunicações, voluntariamente ou se forem assim requisitados.

Princípio 9: Transparência

Os Estados devem ser transparentes sobre o uso e o escopo das leis, regulamentos, atividades, poderes ou autoridades de vigilância das comunicações. Eles devem publicar, no mínimo, informações agregadas sobre número de pedidos aprovados e rejeitados, um detalhamento desta informação por provedor de serviços e autoridade investigatória, tipo, propósito e número específico de indivíduos afetados por cada um desses pedidos. Os Estados devem fornecer aos indivíduos informações suficientes que lhes deem a capacidade de compreender plenamente o escopo, natureza e aplicação da legislação que permite a vigilância das comunicações. Os Estados não devem interferir nos esforços empreendidos por provedores de serviço para publicar os procedimentos que

aplicam para avaliar e cumprir as exigências estatais para com a vigilância das comunicações, além de aderir a esses procedimentos e publicar arquivos dos pedidos de vigilância de comunicações por parte do Estado.

Princípio 10: Escrutínio Público

Os Estados devem estabelecer mecanismos de fiscalização independente para garantir a transparência e responsabilização da vigilância das comunicações. Esses órgãos fiscalizadores devem ter autorização para acessar toda informação potencialmente relevante sobre ações do Estado, incluindo, quando apropriado, acesso a informações secretas ou confidenciais; discernir se o Estado está fazendo uso legítimo de suas atribuições legais; avaliar se o Estado está publicando corretamente informações sobre o uso e escopo de suas técnicas e poderes de vigilância das comunicações de acordo com suas obrigações de transparência; publicar relatórios periódicos e outras informações relevantes sobre a vigilância das comunicações; e divulgar as determinações quanto à legalidade dessas ações, incluindo até que ponto eles aderem a estes Princípios. Os mecanismos de supervisão independentes devem fixar-se além de qualquer supervisão já fornecida através de outro ramo do governo.

Princípio 11: Integridade das Comunicações e Sistemas

Para garantir a integridade, a segurança e a privacidade dos sistemas de comunicações e em reconhecimento do fato de que comprometer a segurança por causa de propósitos estatais quase sempre a fragiliza de forma geral, os Estados não devem compelir provedores de serviços ou fornecedores de hardware e software a embutir capacidade de vigilância ou monitoramento em seus sistemas, a coletar ou reter informações particulares apenas para propósitos de vigilância das comunicações por parte do Estado. A retenção de dados a priori, ou sua coleta, nunca deve ser exigida de provedores de serviços. Os indivíduos têm o direito de se expressar anonimamente e, dessa forma, os Estados devem abster-se de obrigar a identificação do usuário.

Princípio 12: Salvaguardas Para a Cooperação Internacional

Em resposta às mudanças nos fluxos de informação e em serviços e tecnologias de comunicação, os Estados podem precisar buscar assistência de prestadores de serviços estrangeiros e de outros Estados. Nesse sentido, os tratados legais de assistência mútua (MLAT) e outros acordos celebrados pelos Estados devem garantir que, onde as leis de mais de um Estado poderiam se aplicar à vigilância das comunicações, o padrão disponível com o nível de proteção mais alto para os indivíduos deve ser aplicado. Quando os Estados procurarem assistência para propósito de cumprimento da lei, o princípio da criminalidade dupla deve ser aplicado. Os Estados não podem usar processos de assistência mútua e pedidos estrangeiros de informações protegidas para driblar restrições legais domésticas na vigilância das comunicações. Os processos de assistência legal mútua e outros acordos devem ser claramente documentados, publicamente disponíveis e sujeitos às garantias de equidade processual.

Princípio 13: Salvaguardas Contra Acesso Ilegítimo e o Direito a Medidas Eficazes

Os Estados devem promulgar legislação criminalizando a vigilância das comunicações ilegal realizada por atores públicos e privados. A lei deve fornecer sanções civis e criminais suficientes e significativas, proteções para os denunciantes e caminhos de reparação para aqueles afetados. As leis devem estipular que quaisquer informações obtidas de maneira inconsistente com estes princípios são inadmissíveis como prova, ou não consideradas em nenhum procedimento, bem como evidências derivadas dessa informação obtida ilegalmente. Os Estados também devem elaborar leis determinando que, após o material obtido pela vigilância das comunicações ter sido utilizado para o propósito para o qual a informação foi dada, esse material não seja retido, mas destruído ou devolvido àqueles afetados.



Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul

Conforme apontado anteriormente, diversas iniciativas de cooperação internacional sobre ciberdefesa surgiram na América do Sul neste início do século XXI, e o debate aqueceu-se consideravelmente no período imediatamente posterior às denúncias de coleta massiva de dados e de espionagem a governos da região feitas por Edward Snowden em 2013. A nível sub-regional, Brasil e Argentina se posicionaram, em certo momento, como os principais países articuladores de algumas iniciativas, sejam elas bilaterais ou multilaterais.

A atuação do Brasil, especificamente, nessa agenda se intensificou após revelações de que a então presidenta Dilma Rousseff e a Petrobras foram espiadas por órgãos de inteligência do governo estadunidense. Tais denúncias fizeram a preocupação do governo brasileiro aumentar em relação à segurança e à defesa cibernética nas esferas nacional e regional.

O primeiro parceiro a ser procurado diretamente pelo governo brasileiro, pelo que se tem notícia, foi a vizinha Argentina. Em reunião com seu par porteño, Agustin Rossi, o então ministro da Defesa do Brasil, Celso Amorim, discutiu em 13 de setembro de 2013 um projeto de parceria na área de defesa cibernética com a criação de um grupo bilateral para estudar ações de cooperação. Des-

ta reunião, elaborou-se a Declaração de Buenos Aires¹⁷, na qual os ministros, além de concordarem sobre a necessidade de criação de um grupo de trabalho relacionado ao tema, também planejaram a visita de oficiais argentinos ao Centro de Defesa Cibernética do Exército Brasileiro e a participação de membros do exército argentino no Curso de Guerra Cibernética para Oficiais, realizado em 2014, e para suboficiais, realizado em 2015.

O desenvolvimento da agenda bilateral continuou durante visita do Ministro Rossi à Brasília, onde foi elaborada a Declaração Conjunta de Brasília¹⁸, em 21 de novembro de 2013. O oficial argentino visitou a sede do Centro de Defesa Cibernética do Exército Brasileiro, conforme acordado na declaração anterior, e, durante os dias 20 e 21 de novembro, foi realizada a I Reunião do Subgrupo de Trabalho Bilateral em Cooperação de Defesa Cibernética.

Enfim, o Subgrupo de Cooperação em Defesa Cibernética (SCDC) foi criado nos dias 18 e 19 de março de 2014 durante a VIII Reunião do Grupo de Trabalho Conjunto (GTC) Brasil-Argentina. Com a consolidação do grupo, uma série de atividades conjuntas foram planejadas para os anos seguintes, cujos resultados serão detalhados nas próximas seções do estudo.

Outro gesto do Brasil neste sentido se deu cerca de um mês após as denúncias de Snowden em junho de 2013. Durante uma entrevista coletiva, o então ministro das Relações Exteriores, Antônio Patriota, afirmou que os países do bloco econômico do MERCOSUL¹⁹ “buscariam reduzir a dependência tecnológica estrangeira como forma de evitar novas espionagens em telecomunicações”²⁰.

O tema foi abordado no bloco já em julho de 2013 com a aprovação da “Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da Amé-

17 http://www.defesanet.com.br/br_ar/noticia/12270/BR-AR---DECLARACION-DE-BUENOS-AIRES-DE-LOS-MINISTROS-DE-DEFENSA-DEL-BRASIL-Y-ARGENTINA/

18 http://www.defesa.gov.br/arquivos/2013/mes11/borrador_castellano_final.pdf

19 O Mercado Comum do Sul (MERCOSUL) é um bloco econômico regional consolidado com a assinatura do Tratado de Assunção em 1991. Inicialmente, o acordo foi celebrado por Argentina, Brasil, Paraguai e Uruguai, sendo hoje composto por 10 países da região, considerando que um deles, a Venezuela, encontra-se suspenso em fevereiro de 2017. No site oficial do bloco, diz-se que o objetivo deste é consolidar a integração política, econômica e social entre os países que o integram, fortalecer os vínculos entre os cidadãos do bloco e contribuir para melhorar sua qualidade de vida. Link: <http://www.mercosur.int/>

20 <http://computerworld.com.br/seguranca/2013/07/17/mercosul-investira-em-ciberseguranca-e-quer-reduzir-dependencia-tecnologica>

rica nos Países da Região”²¹, que foi assinada por presidentes de cinco países membros do bloco (Argentina, Bolívia, Brasil, Uruguai e Venezuela). Os compromissos assumidos pelos países foram:

- Trabalhar em conjunto para garantir a segurança cibernética dos Estados Partes do MERCOSUL, aspecto essencial para a defesa da soberania de nossos países.
- Exigir aos responsáveis dessas ações o encerramento imediato das mesmas e as explicações sobre suas razões e consequências.
- Sublinhar que a prevenção ao crime, assim como a repressão aos delitos transnacionais, inclusive o terrorismo, deve enquadrar-se no estado de direito e na estrita observância do Direito Internacional.
- Promover nas instâncias multilaterais pertinentes a adoção de normas relativas à regulamentação da internet, com ênfase nos aspectos de segurança cibernética, com vistas avançar na adoção de normas que garantam a proteção adequada das comunicações, em particular para preservar a soberania dos Estados e a privacidade dos indivíduos.
- Manifestar nossa total solidariedade com todos os países, dentro e fora de nossa região, que tenham sido vítimas dessas ações.
- Promover a gestão conjunta dos Chanceleres junto ao Secretário-Geral da Organização das Nações Unidas (ONU) para informar sobre os fatos e solicitar mecanismos de prevenção e sanção em nível multilateral na matéria.
- Instruir as Delegações dos Estados Partes que participarão da próxima Assembleia-Geral da ONU a realizar conjuntamente pleito formal no mesmo sentido.
- Além disso, solicitar à República Argentina que submeta esse assunto à consideração do Conselho de Segurança.
- Acordar a constituição de um Grupo de Trabalho para coordenar esforços, junto com o Conselho de Defesa Sul-Americano e o Conselho Sul-Americano de Infraestrutura e Planejamento, com o propósito de implementar ações que tornem mais seguras nossas telecomunicações e reduzam nossa dependência da tecnologia estrangeira.

Um mês depois, em agosto, representantes do bloco reuniram-se com o Secretário Geral da ONU, Ban Ki-moon, para expressar a insatisfação e a

■ 21 http://www.mercosur.int/innovaportal/file/4677/1/decisao_espionagem_pt.pdf

preocupação com relação às práticas de vigilantismo. Duas novas reuniões em setembro e novembro, na Venezuela, reafirmaram o posicionamento do bloco e houve a renovação do comprometimento a fim de criar uma instância permanente para tratar de assuntos relacionados à segurança na Internet e telecomunicações.

A estratégia brasileira e argentina para defesa cibernética se expande para a União de Nações Sul-Americanas (UNASUL), sendo que o Conselho de Defesa Sul-Americano foi, à época, um dos principais foros para a implementação desta estratégia.²² Aproveitando o encontro na Argentina em 2013, o ministro brasileiro sugeriu que fosse criada uma comissão de assessoria militar que funcione permanentemente junto à UNASUL.

Em 2014, no âmbito da UNASUL, foi criado um grupo de trabalho sobre defesa cibernética, que, em 2017 tem como responsáveis os representantes de Equador e Peru. No entanto, o grupo não conseguiu realizar o seminário internacional sobre o tema previsto no plano de ação de 2016, que se daria em conjunto com o COSIPLAN (Conselho Sul-Americano de Infraestrutura e Planejamento) e remarcou a realização para o ano de 2017.

Por sua vez, a OEA possui um programa regional de segurança cibernética, no âmbito do Comitê Interamericano Contra o Terrorismo (CICTE), que busca promover e fortalecer as capacidades de segurança cibernética dos Estados-membro por meio de assistência técnica e treinamento, mesas redondas sobre política, exercícios de gestão de crises e intercâmbio de melhores práticas para o uso de tecnologia da informação e comunicação. A OEA tem se ocupado com a temática pelo menos desde 2004, quando divulgou a “Declaração sobre o Fortalecimento da Segurança Cibernética nas Américas”, que posteriormente foi complementada pela “Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética”, em 2012.

22 A União de Nações Sul-Americanas (UNASUL) é uma organização intergovernamental composta por todos os 12 Estados sul-americanos. Seu objetivo é a criação de um espaço de integração cultural, econômico, social e político, assim como eliminar a desigualdade econômica, alcançar a inclusão social, aumentar a participação cidadã, fortalecer a democracia e reduzir as assimetrias existentes. O Conselho de Defesa Sul-Americano é o órgão da UNASUL responsável por tratar dos assuntos de defesa regionais. Link para o site do Conselho de Defesa Sul-Americano (<http://www.unasursg.org/es/consejo-defensa-suramericano>)

Além das articulações internacionais, em 2016, o Centro de Instrução de Guerra Eletrônica (CIGE) brasileiro realizou o 1º Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas. Este estágio contou com a participação de militares de 12 países, além dos brasileiros, e foi totalmente organizado pelas Forças Armadas brasileiras.

A Hacking Team latina

A Dígitro é uma companhia brasileira de Santa Catarina focada no desenvolvimento de soluções tecnológicas no ramo das telecomunicações com ênfase em comunicação, segurança e inteligência. Grande parte dos clientes da empresa são entes governamentais nacionais e internacionais. Um exemplo que se tornou público foi o caso uruguaio em 2013, no qual o governo desse país negou-se a fornecer informações a respeito da compra da ferramenta “Guardião” da empresa brasileira por um valor de cerca de US\$ 2 milhões, capaz de interceptar chamadas telefônicas, correios eletrônicos e redes sociais sem a necessidade de concessões das grandes empresas de Internet. A compra do programa foi duramente criticada por organizações da sociedade civil uruguaia, que, por meio de pedidos de informação e pressão popular, conseguiram trazer o debate sobre a utilização da ferramenta ao grande público.

Em dezembro de 2015, foi firmado um protocolo diferenciado para a utilização dessa ferramenta, requerendo, por exemplo, que a autoridade policial considere indispensável sua utilização e comunique essa necessidade à justiça, além de realizar o preenchimento de um formulário com informações detalhadas da operação de vigilância em questão e a análise da solicitação de uso do sistema pela justiça. Mesmo com a criação do protocolo de uso acima descrito, as organizações da sociedade civil discordam da necessidade e legalidade de um programa como o “Guardião” por ser por si só um potencial violador de direitos básicos dos cidadãos uruguaiois, tais quais a privacidade e a liberdade de expressão²³.

23 Texto produzido com informações fornecidas pela CAINFO.

Internamente, questões relacionadas à cibersegurança já possuem regulações, diretrizes e organismos próprios. As iniciativas da defesa cibernética brasileira antecederam as denúncias de Edward Snowden. Inicialmente, em 2010, foi criado o Núcleo do Centro de Defesa Cibernética (NuCDCiber) no Exército para coordenar e executar um projeto de estrutura sobre a área cibernética, o desenvolvimento de um Centro de Defesa Cibernética, planejar e executar a segurança cibernética, coordenar a Rede Nacional de Segurança da Informação e Criptografia, entre outras responsabilidades. Essas atividades foram alocadas para diferentes órgãos dentro do Exército, como o Centro de Comunicações e Guerra Eletrônica do Exército Brasileiro (CCOMGEX), Centro Integrado de Telemática do Exército (CITEX) e o Centro de Defesa Cibernética. Em novembro de 2012, foi fundado o Centro de Defesa Cibernética (CDCiber), vinculado ao Ministério da Defesa (MD). Isso implicou na alteração da estrutura regimental da Marinha, Exército e Aeronáutica (Decreto nº 7.809) e, posteriormente, na atribuição da responsabilidade pela coordenação e integração da defesa cibernética junto ao MD (Portaria nº 3.028). Resumidamente, o CD-Ciber é criado para o país realizar ações ofensivas, defensivas e exploratórias, isto é, de ataques online até mitigar ações de sabotagem e espionagem.

Após as revelações de Snowden, de maneira imediata, algumas reestruturações e investimentos no CDCiber foram anunciados, como o aumento do corpo de oficiais e a compra de equipamentos. O centro recebeu R\$ 400 milhões até 2015 para investimentos em seus projetos²⁴. Além disso, houve a criação de uma Escola Nacional de Defesa Cibernética, cujo projeto entrou em vigor em 2015 como o Instituto de Defesa Cibernética (IDCIBER), vinculado à UnB. Também, houve a implementação do Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), dentro do Comando Militar do Planalto (CMP). O primeiro teve como objetivo a criação dos cursos de ensino à distância (EAD) que buscam desvincular o papel de capacitar recursos humanos para a atuação de defesa cibernética no país, deixando

24 <https://medium.com/brasil/por-dentro-do-cdciber-o-centro-de-defesa-cibernetica-do-exercito-brasileiro-40ce637d119>

o CDCiber com a única prerrogativa de atuar em operações de guerra cibernética. Segundo o próprio IDCIBER em sua página menciona: “desde sua concepção, tem como responsabilidade contemplar também, o acesso à Lista de Discussão e à Ferramenta de Cooperação (Twiki) da Rede Nacional de Excelência em Segurança da Informação e Criptografia (RENASIC) e às bibliotecas digitais de interesse das Forças Armadas”.

Também em 2015, foi lançada a Estratégia de Segurança da Informação e Comunicações e da Segurança Cibernética da Administração Pública Federal do Brasil para 2015-2018²⁵. Uma das metas estabelecida no documento é interessante para resumir o objetivo da estratégia e, portanto, o caminho e o foco do governo brasileiro com relação à defesa cibernética:

“É essencial avançar na articulação para o fortalecimento e aceleração da implantação do ecossistema digital (SIC+SegCiber+Empresas+ICT) com a finalidade de apoiar o desenvolvimento de tecnologias de SIC e de SegCiber, a exemplo de soluções de reconhecimento de artefatos maliciosos e outras ferramentas cibernéticas, alavancando a criação do mesmo e promovendo maior sinergia com o ecossistema da defesa cibernética. Para tanto, faz-se necessário aprimorar os mecanismos de fomento e de financiamento que favoreçam parcerias entre o setor privado e as universidades e institutos de pesquisa, para o desenvolvimento e a produção de soluções de SIC e de SegCiber.”

Entretanto, o esforço de integrar atividades e atuar mais no ambiente da rede já é conhecido desde julho de 2013, quando, em reportagem amplamente divulgada pela imprensa, o general José Carlos dos Santos, oficial do Exército à frente do CDCiber, revelou que o Centro estava realizando acordos com os ministérios da Justiça e da Defesa com o objetivo “de coordenar e integrar os esforços da segurança cibernética desses grandes eventos”, através do monitoramento de fontes abertas, como as redes sociais. Tal ação coordenada seria apenas uma “atribuição temporária”, aparentemente visando grandes eventos, como foi o caso da Copa do Mundo, em 2014, e da visita do Papa, em 2013.

■ 25 http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf

No contexto da Copa do Mundo, a ARTIGO 19 enviou pedidos de informação ao exército, mencionando a reportagem e solicitando mais informações sobre o monitoramento das redes sociais, bem como a utilização do Sistema Guardião, a ferramenta de investigação que realiza monitoramento de dados e gravações de voz, para análise de autoridades com poder de polícia. Em resposta aos pedidos, o Exército não se manifestou a respeito do monitoramento online durante a Copa e ainda negou a utilização do Sistema Guardião, apesar da existência da notícia e da declaração do próprio general do Exército.



Pedidos de Informação

A partir de uma pesquisa sobre os organismos internacionais regionais e notícias de cooperações intergovernamentais sobre o tema, a ARTIGO 19 realizou oito pedidos de informação sobre a atuação do governo brasileiro no que toca a segurança e a defesa cibernética tanto em organizações e blocos internacionais quanto nas relações bilaterais. Os órgãos consultados foram, principalmente: o Ministério da Defesa (MD) e órgãos a ele vinculados, como as forças armadas, e o Ministério das Relações Exteriores (MRE).

O foco das questões foi a atuação brasileira no MERCOSUL, na UNASUL, na OEA, nas relações bilaterais com a vizinha Argentina e na realização do 1º Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas em 2017. Perguntou-se às autoridades o presente estado das iniciativas nessas organizações internacionais, o quanto o governo brasileiro estaria ativo nas articulações desenvolvidas, assim como os aportes financeiros realizados.

Além do estabelecimento do panorama de iniciativas, faz-se também uma análise do nível de transparência dos pedidos de informação feitos aos órgãos públicos brasileiros, conforme a precisão de suas respostas e o tempo levado para a obtenção da informação requerida.

Os oito pedidos de informação foram:

Pedido de informação	Nº de recursos	Respondido/ negado
Solicitamos as atas das reuniões do Conselho de Defesa da União de Nações Sul-Americanas dos anos de 2013 até a presente data.	2	Respondido
Solicitamos uma lista de projetos e seus respectivos orçamentos e documentos-base que estão sendo desenvolvidos na área de Defesa Cibernética no Conselho de Defesa da União de Nações Sul-Americanas – UNASUL desde junho 2013.	1	Respondido
Solicitamos receber lista de parcerias estabelecidas entre os Estados-membro da UNASUL com entidades privadas na área de defesa cibernética desde junho 2013 até a presente data.	0	Respondido
A OEA possui um programa regional de segurança cibernética, através do Comitê Interamericano Contra o Terrorismo (CICTE). Quais são as contribuições financeiras, tecnológicas, de experiências de conteúdo brasileiras ao programa? Quais órgãos públicos brasileiros participam deste programa regional? E o que este programa auxiliou o país em suas ações na área?	1	Respondido
No período de 9 a 20 de maio de 2016, o Centro de Instrução de Guerra Eletrônica (CIGE) realizou o 1º Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas. Gostaríamos de cópia do programa deste estágio, assim como da lista de participantes do mesmo, com seus respectivos países de origem.	2	Respondido
Solicitamos uma lista de projetos e seus respectivos orçamentos e documentos-base que estão sendo desenvolvidos na área de Defesa Cibernética no grupo de trabalho criado para debater o tema da segurança cibernética no âmbito do MERCOSUL a partir de 2013.	3	Negado

Pedido de informação	Nº de recursos	Respondido/negado
Em 13 de setembro de 2013, os ministros da Defesa de Brasil e Argentina discutiram um projeto de parceria na área de defesa cibernética com a criação de um grupo bilateral para estudar cooperações nesta área. Solicitamos os registros desta reunião e as atas das reuniões do grupo criado.	1	Respondido
Solicitamos receber os relatórios das atividades desenvolvidas pelo Subgrupo de Cooperação de Defesa Cibernética (SCDC) desde março de 2014 até a presente data.	3	Negado

É possível observar que dos oito pedidos de informação realizados somente um não necessitou de um recurso, pois a resposta foi uma afirmação contundente de que a UNASUL não mantém nenhuma relação com entidades privadas na área de ciberdefesa. Todos os outros pedidos de informação necessitaram de um ou mais recursos para que alguma informação fosse finalmente concedida. Em dois deles, não foi possível obter sequer uma resposta, com as justificativas de que a informação já havia sido enviada ou que era uma informação sigilosa. Nos pedidos restantes foram necessárias uma ou duas vias recursais até que a informação fosse enviada de forma integral ou uma resposta contundente fosse dada.



Relações Bilaterais Brasil-Argentina

O primeiro pedido foi endereçado ao Ministério das Relações Exteriores (MRE) em 19 de julho de 2016 e fez referência às atividades bilaterais realizadas entre Brasil e Argentina desde 13 de setembro de 2013 quando os então ministros de Defesa dos dois países se reuniram e acordaram a criação de um grupo de estudo para possíveis cooperações na defesa cibernética.

O MRE julgou que o órgão mais competente para a resposta seria o Ministério da Defesa (MD) e reencaminhou o pedido. Por sua vez, o MD respondeu o pedido em 02 de setembro, após uma prorrogação do prazo para resposta, provendo acesso parcial às informações solicitadas. Apesar de não fornecer os documentos solicitados, como as atas de reunião do grupo criado alegando a inexistência das mesmas, o MD respondeu de forma detalhada sobre todos os processos que foram e ainda estão sendo desenvolvidos entre Brasil e Argentina em defesa cibernética desde o acontecimento da reunião entre os ministros.

Na resposta, o MD detalha que a criação do Subgrupo de Cooperação de Defesa Cibernética (SCDC) se efetivou em março de 2014, durante a VIII Reunião do Grupo de Trabalho Conjunto (GTC) Brasil-Argentina, de

acordo com o que foi estabelecido na Declaração de Buenos Aires²⁶, de 13 de setembro de 2013, e na Declaração Conjunta de Brasília²⁷, de 20 de novembro de 2013.

O SCDC passou a atuar e desde então já desenvolveu uma série de ações, conforme descrito pelo próprio MD na resposta:

1. “O Brasil ofertou uma vaga no Curso de Guerra Cibernética no Centro de Instrução de Guerra Eletrônica (CIGE) e uma vaga para o Curso de Guerra Cibernética, a ocorrer em 2016 no Centro de Instrução de Guerra Eletrônica (CIGE) do Exército Brasileiro, para militares das Forças Armadas Argentinas.
2. A Argentina ofereceu uma vaga, anualmente, para o curso presencial de pós-graduação no nível de especialização em Criptografia e Segurança Teleinformática, a ser desenvolvida na Faculdade de Engenharia do Exército Escola Superior Técnica (EST).
3. O Ministério da Defesa Argentino declarou realizar cooperação no intercâmbio de informações de interesse, por intermédio do ARCERT, que pudessem reforçar as ações de segurança e defesa cibernética durante os grandes eventos a serem realizados no Brasil, em 2014;.
4. Foi admitido por ambas as partes iniciarem um processo de discussão de conceitos doutrinários de Defesa Cibernética, por meio de uma reunião a ser realizada no Centro de Defesa Cibernética do Exército Brasileiro, em agosto de 2014.
5. Ambos os países assinalaram a oportunidade de analisar a possibilidade de estabelecer níveis de alerta cibernético comuns.
6. Defenderam a possibilidade de estabelecer procedimentos para intercâmbios de informações de segurança cibernética entre as equipes de tratamento de incidente de rede (computer security incident response team ±CSIRT), no âmbito do Ministério da Defesa dos países, implementando inicialmente canais de comunicação mínimos (pontos de contato e procedimentos de segurança criptográfica) para a troca dessas informações.
7. Concordaram que, deveria ser tratado no subgrupo de trabalho quais as linhas de pesquisa que poderão ser desenvolvidas por ins-

26 <http://www.defesa.gov.br/arquivos/2013/mes09/comunicado.pdf>

27 http://www.defesa.gov.br/arquivos/2013/mes11/borrador_castellano_final.pdf

tituições de ensino e pesquisa brasileiras e argentinas que tenham o potencial de contribuir para as ações de desenvolvimento conjunto da defesa cibernética.

8. Consentiram em analisar a possibilidade de intercâmbio de pesquisadores para integrar as equipes de pesquisa nos projetos em andamento e realizados no Setor Cibernético de ambos os países.
9. Os Ministérios da Defesa de ambos os países concordaram em analisar a possibilidade de receber observadores durante a realização de um evento relacionado à defesa cibernética a ser determinado.
10. O Ministério da Defesa Argentino convidou o Ministério de Defesa do Brasil para participar, como palestrante, de um Seminário de Defesa Cibernética realizado no período de 14 a 16 de maio de 2014, na cidade de Buenos Aires.
11. O Brasil propôs substituir as vagas ofertadas para o Curso de Guerra Cibernética, no CIGE, por vagas em um estágio de Guerra Cibernética para militares de Nações Amigas. A Argentina considerou seu interesse na nova proposta, mas solicitou a manutenção das vagas já oferecidas, a fim de fortalecer a integração entre ambos países.
12. Visando à preparação para os cursos citados acima foram oferecidas 3 (três) vagas, para cada curso na fase de ensino a distância.
13. A Argentina disponibilizou 2 (duas) vagas, anualmente, para o curso de pós-graduação no nível de especialização em Criptografia e Segurança Teleinformática, efetivado na Faculdade de Engenharia do Exército – Escola Superior Técnica.
14. O Ministério da Defesa da Argentina ofertou a cooperação no intercâmbio de informações de interesse, por intermédio do ArCERT²⁸, que possam reforçar as ações de Segurança e Defesa Cibernéticas durante grandes eventos, a serem realizados no Brasil, em 2016. Ambas as partes mantiveram o interesse no processo de discussão de conceitos doutrinários de Defesa Cibernética.
15. Ambas as partes propuseram programar uma reunião para trabalhar no estabelecimento de procedimentos para intercâmbios de informações de Segurança Cibernética, entre as equipes de tratamento de rede (computer security incidente response team - CSIRT), no âmbito dos Ministérios da Defesa de ambos países.

28 Grupo técnico responsável por resolver incidentes relacionados à segurança em sistemas computacionais do setor público na Argentina.

16. Concordaram intercambiar experiências sobre gestão de projetos de pesquisa em Defesa Cibernética.
17. Ambas as partes concordaram desenvolver, em conjunto, a partir do 2o semestre de 2016, as bases para um exercício de Defesa Cibernética a realizar-se em 2017.

A partir dessa descrição das atividades desenvolvidas pelo SCDC, nota-se que a principal intenção dos Ministérios de Defesa com essa parceria é a capacitação de seus efetivos na matéria. As 17 atividades mencionadas na resposta podem ser divididas em quatro grandes categorias, conforme quadro abaixo:

Categoria	Número de incidências
Capacitação (oferta de vagas em cursos de um país a outro)	6 (números 1, 2, 11, 12, 13, 17)
Doutrina (estabelecimento de ideias fundamentais sobre defesa cibernética)	1 (número 4)
Pesquisa científica (atividades para descobrimento de novos conhecimentos e/ou participação de seminários)	5 (números 7, 8, 9, 10, 16)
Cooperação direta (troca de informações entre órgãos/estabelecimento de procedimentos em comum)	5 (números 3, 5, 6, 14, 15)

Dentre as quatro categorias, vale ressaltar a cooperação direta entre os governos e a troca de informações ocorrida. A Argentina forneceu informações ao governo brasileiro nos períodos de realização dos grandes eventos no país (Copa do Mundo em 2014 e Olimpíadas em 2016). Infelizmente, o MD não detalhou os tipos de informações recebidas, o que torna difícil afirmar que houve compartilhamento ilegal de dados pessoais entre os países.

A ARTIGO 19 realizou um outro pedido sobre o SCDC requerendo fontes documentais das reuniões. No entanto, esse pedido foi negado na primeira e segunda instâncias, sendo novamente negado pela Controladoria Geral da União

que considerou suficientes as informações concedidas no primeiro pedido. O tempo total de tramitação do pedido de informação chegou a quatro meses.

A ARTIGO 19 desconhece outras cooperações bilaterais em defesa cibernética desse porte na América do Sul. Brasil e Argentina têm protagonizado um movimento de estreitamento de cooperação nessa área e ambos os países também demonstram interesse e ações concretas para levar esses tipos de ações a foros multilaterais, como na UNASUL e no MERCOSUL, conforme detalhado a seguir.



Relações Multilaterais: Mercosul

Em 2013, a reação brasileira às denúncias de espionagem online foi para além da parceria com a Argentina. A ARTIGO 19 fez um pedido de informação referente à iniciativa brasileira, apresentada pelo então ministro das Relações Exteriores, Antônio Patriota, em julho de 2013, sobre a criação de uma regulamentação regional sobre segurança cibernética durante encontro do MERCOSUL²⁹ e os outros compromissos assumidos pela cúpula de presidentes do MERCOSUL com a “Decisão sobre o repúdio à espionagem por parte dos Estados Unidos da América nos países da região”. O pedido de informação foi enviado tanto ao MRE – responsável pela atuação brasileira no MERCOSUL quanto ao MD – responsável pela área de defesa cibernética.

As respostas obtidas de ambos os órgãos foi surpreendente, pois enquanto o MD afirmou que não atuava no âmbito do MERCOSUL, o MRE encaminhou a resposta ao MD, pois não seria o responsável pela pauta de defesa cibernética. Dessa maneira, a ARTIGO 19 teve que recorrer às diversas instâncias do sistema de acesso à informação no intento de receber algum dado sobre as tratativas ocorridas.

■ 29 <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=34294&sid=11>

Optou-se por recorrer ao MD, já que o MRE havia encaminhado o pedido de informação para o órgão. As recusas seguiram-se na primeira e segunda instâncias, sendo que o MD afirmou que não haveria se constituído nenhum grupo de trabalho no MERCOSUL, assim como a Controladoria-Geral da União (CGU) também considerou que o órgão não teria tal informação.

Uma das justificativas dada pela CGU foi a de que o MD já teria respondido uma série de pedidos sobre o tema e que o grupo de trabalho nunca haveria se constituído de fato no MERCOSUL. A explicação da CGU se deu nos seguintes termos:

“5. O presente recurso solicita lista de projetos, seus respectivos orçamentos e documentos-base que estão sendo desenvolvidos na área de Defesa Cibernética em Grupo de Trabalho criado para debater o tema da segurança cibernética, no âmbito do MERCOSUL. Ressalta-se que a criação do GT é mencionada em reportagem, cujo o link é disponibilizado pelo recorrente e, portanto, não se trata de informação oficial. O recorrido informa não ter participação no referido grupo de trabalho e declara inexistência da informação (Súmula 06/2015 da CMRI). Além disso, destaca que disponibilizou, em resposta a outros pedidos de acesso deste solicitante, informações relacionadas ao tema de defesa cibernética produzidas por outro Grupo de Trabalho. Este é relacionado ao Conselho de Defesa Sul-Americano, no âmbito da União de Nações Sul-Americanas (UNASUL).

6. Em razão de o recorrido ter indicado o Ministério das Relações Exteriores (MRE) como órgão competente para tratar deste pedido de acesso. E o MRE, por sua vez, ter remetido um pedido de acesso idêntico ao próprio MD, entendeu-se por bem colher esclarecimentos adicionais.

7. Assim, na fase de interlocução, esta Ouvidoria buscou confirmar se existe ou existiu em algum momento um GT sobre segurança cibernética, no âmbito do MERCOSUL em que o MD tenha feito parte. Caso a resposta fosse positiva, questionou-se sobre a possibilidade de disponibilizar as informações solicitadas. Além disso, indagou-se o MD a fim de confirmar se o recorrido tinha conhecimento de normas relativas à regulamentação da internet, com ênfase nos aspectos de segurança cibernética, adotadas pelo MERCOSUL, que pudesse disponibilizar ou indicar onde as mesmas podem ser consultadas via internet. Por último, perguntamos se o MD tem conhecimento de outros documentos ou materiais relacionados ao tema que poderiam ser disponibilizados ou indicados ao requerente.

8. Os esclarecimentos prestados e transcritos no quadro resumo confirmam o posicionamento adotado pelo órgão, desde as respostas ao pedido inicial e recursos. Nesse sentido, destaca-se que o MD reforçou não ter conhecimento de um GT sobre segurança cibernética, no âmbito do MERCOSUL, e caso este exista, afirmou não ter feito ou fazer parte dele. Por fim, voltou a mencionar a existência do GT do Conselho de Defesa Sul-Americano, no âmbito da UNASUL, na área de Defesa Cibernética, cujas as informações existentes sobre o tema já foram disponibilizadas, em outros pedidos de acesso.

9. É importante registrar que esta Ouvidoria analisou os pedidos de acesso à informação citados ao longo do processo. Foi possível averiguar que, até o momento, com exceção do pedido 09200.000681/2016-08 que tem recurso em análise nesta Ouvidoria, os pedidos foram concluídos com registro de entrega da informação, no e-SIC. O material disponibilizado refere-se ao GT do Conselho de Defesa Sul-Americano, no âmbito da UNASUL.

10. Assim, entende-se que o recorrido dirimiu as dúvidas relacionados ao caso e comprovou não ter mais informações a disponibilizar. Por isso, sugere-se a adoção da súmula no 06/2015 da CMRI, como embasamento para a tomada de decisão deste Ministério. A seguir, a transcrição da referida súmula:

Súmula CMRI no 6/2015

“INEXISTÊNCIA DE INFORMAÇÃO – A declaração de inexistência de informação objeto de solicitação constitui resposta de natureza satisfativa; caso a instância recursal verifique a existência da informação ou a possibilidade de sua recuperação ou reconstituição, deverá solicitar a recuperação e a consolidação da informação ou reconstituição dos autos objeto de solicitação, sem prejuízo de eventuais medidas de apuração de responsabilidade no âmbito do órgão ou da entidade em que tenha se verificado sua eliminação irregular ou seu descaminho.”

A ARTIGO 19 não encontrou nenhum indício de que houve prosseguimento de atividades relacionadas à ciberdefesa no MERCOSUL, contudo poderiam ter sido entregues documentos relativos às negociações ocorridas em junho de 2013, especialmente sobre os registros relativos à elaboração da “Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da América nos Países da Região” – o que demonstra pouco cuidado do Estado brasileiro em fornecer as informações requisitadas.



Relações Multilaterais: UNASUL

A ARTIGO 19 fez três pedidos de informação sobre a atuação do Grupo de Trabalho (GT) na área de Ciberdefesa, operante no Conselho de Defesa Sul-Americano da UNASUL (CDS). O GT foi criado em 2012 com o objetivo de estabelecer e manter uma política e mecanismos regionais de coordenação e assistência mútua para enfrentar as ameaças cibernéticas, que ponham em risco as infraestruturas críticas no âmbito da Defesa dos Estados membros da UNASUL.

Este GT realizou reuniões anuais nos anos de 2012 e 2013, em Lima, no Peru, e em 2014 em Buenos Aires, na Argentina. Desde então, anualmente, são planejadas atividades do subgrupo no Plano de Ação do CDS.

Em relação ao GT, a ARTIGO 19 requisitou ao Ministério da Defesa:

- (1) uma lista de projetos e o orçamento destinado à defesa cibernética no órgão sul-americano;
- (2) as atas das reuniões do CDS;
- (3) e se havia alguma parceria com entidades privadas no estabelecimento de políticas regionais de defesa cibernética.

Em resposta, o MD afirmou em (1) que não havia qualquer projeto ou orçamento destinado ao desenvolvimento da defesa cibernética. Em recurso,

a ARTIGO 19 contestou e identificou a presença do grupo de trabalho voltado às questões de defesa cibernética no interior do CDS. Em resposta ao recurso, o MD reconheceu a existência do subgrupo, contudo afirmou que: “realmente existe no âmbito do CDS um Grupo de Trabalho (GT) na área de Ciberdefesa que foi criado no ano de 2012, decorrente da atividade 1.F do Plano de Ação 2012 do CDS. O GT foi criado com o objetivo de trabalhar em atividades concretas para estabelecer uma política regional da UNASUL de defesa cibernética. Este GT realizou reuniões anuais nos anos de 2012 e 2013, em Lima no Peru, e 2014 em Buenos Aires na Argentina, cujas atas seguem anexas.”

Desta resposta, foi possível obter os objetivos específicos do grupo de trabalho. Eles estão descritos na ata de formação do GT em 15 de maio de 2012. Nela, o Peru ficou como país responsável pela coordenação, tendo como corresponsáveis o Uruguai e a Venezuela. Seus objetivos são:

- Estabelecer uma rede de contatos de autoridades competentes para o intercâmbio de informação e colaboração ante incidentes de forma permanente.
- Definir a plataforma e procedimentos do sistema de comunicações da rede.
- Realizar o diagnóstico situacional na região, incluindo as capacidades atuais em termos de Segurança Cibernética e o relacionamento com as equipes de resposta nacionais.
- Propor um esquema metodológico para o desenvolvimento e implementação da política de Segurança Cibernética.
- Definir as capacidades desejáveis comuns de Segurança Cibernética na previsão, prevenção, detecção, dissuasão, resposta e recuperação.
- Propor uma terminologia e conceitos comuns na matéria entre os países membros.
- Propor um programa de educação em segurança informática e da informação.
- Avaliar a implementação de uma estrutura organizacional e níveis de capacitação padronizada para os integrantes da mesma.
- Propor mecanismos de ação ante incidentes cibernéticos de acordo ao nível de impacto.

- Propor mecanismos de gestão de pós-incidentes cibernéticos, para a geração de uma base de conhecimento e lições aprendidas.
- Considerar a viabilidade de desenvolver atividades de relacionamento e realizar exercícios multinacionais sobre incidentes cibernéticos com o objetivo de gerar confiança entre os países membros.
- Estudar a viabilidade de ampliar o alcance do Grupo de Trabalho ao âmbito da Segurança e Defesa do ciberespaço dos países membros da UNASUL.

Inicialmente, não há nada nesta listagem que pareça ser ofensivo ou danoso ao direito à liberdade de expressão para a região. São propostas importantes e adequadas para o estabelecimento de uma política regional de ciberdefesa e cibersegurança. Contudo, como será constatado, pouco do que foi planejado pelo GT tem sido executado.

Na segunda reunião do subgrupo, ocorrida nos dias 26 e 27 de setembro de 2013, foi elaborada uma “Proposta do Grupo de Trabalho para estabelecer uma política regional da UNASUL em matéria de cibersegurança e ciberdefesa”. A proposta estrutura-se em dois grandes objetivos:

1. Implementar e fomentar a coordenação de políticas públicas, para incrementar a consciência de segurança cibernética nos Estados-Membros e a região.
2. Impulsionar e fomentar capacidades humanas e tecnológicas assim como suas normativas para enfrentar as ameaças cibernéticas, que atentem contra a segurança e defesa.

Foram listadas diversas atividades a serem realizadas pelo subgrupo, tais como a realização de cursos, seminários, campanhas de sensibilização e capacitação sobre defesa cibernética; intercâmbios de políticas públicas sobre a matéria de defesa cibernética, entre diversas outros exercícios de capacitação, articulação e execução de atividades conjuntas em defesa cibernética. Novamente, nenhuma atividade listada pareceu em princípio ser prejudicial ao direito à liberdade de expressão e acesso à informação.

Ao final da atividade realizada no ano de 2014, o GT definiu temas prioritários para a condução dos seus trabalhos, constante em ata e, apesar da atividade constar no Plano de Ação do CDS dos anos de 2015 e 2016,

a última reunião ocorreu em 2014 e, atualmente, as atividades do GT estão paralisadas.”

Em resposta ao pedido (2), o MD enviou todas as atas do CDS de 2013 a 2014. Nessas atas, notou-se que as discussões sobre estratégias regionais sobre defesa cibernética não ultrapassam o grupo de trabalho devotado a essa função.

Já em resposta ao pedido (3), o MD foi categórico ao afirmar que nenhuma parceria privada sobre defesa cibernética foi estabelecida no âmbito da UNASUL.



Relações Multilaterais: OEA

A ARTIGO 19 enviou ao MRE um pedido de informação sobre a participação brasileira na OEA em questões de defesa cibernética. Ciente da existência de um programa regional de segurança cibernética, através do Comitê Interamericano Contra o Terrorismo (CICTE), foi perguntado ao órgão quais são as contribuições financeiras, tecnológicas, de experiências e de conteúdo brasileiras ao programa, quais órgãos públicos brasileiros participam deste programa regional além do MRE e em que este programa auxiliou o país em suas ações na área.

O órgão esclareceu, em sua primeira resposta, grande parte das indagações realizadas, excetuando as informações relativas às contribuições financeiras do Brasil ao CICTE. A resposta do órgão foi detalhada e descreveu todas as atividades realizadas pelo Brasil desde sua entrada no órgão em 2005, conforme pode-se observar:

“O Brasil vem colaborando com o Programa de Segurança Cibernética do Comitê Interamericano contra o Terrorismo (CICTE) desde 2005, mediante participação em iniciativas regionais baseadas no Programa, no âmbito das quais são intercambiadas experiências e assistência mútua no tema de segurança cibernética.

Essa troca de informações e boas práticas possibilita ao Brasil beneficiar-se da experiência dos demais países americanos participantes, ao mesmo tempo em que permite que prestemos nossa contribuição com vistas ao fortalecimento da segurança cibernética na região. Essa coope-

ração é central para o Programa e dela têm participado órgãos brasileiros como o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o Ministério da Defesa, o Ministério da Justiça, a Polícia Federal e o Ministério Público, além do Ministério das Relações Exteriores.

Em 2005, logo após o Programa ter se tornado operacional, o Brasil acolheu a 2ª Reunião do Grupo de Peritos Governamentais sobre Segurança Cibernética (São Paulo, 14-16/9/2005). Em abril de 2006, representantes do governo brasileiro participaram de um seminário nos EUA, cujo objetivo foi a capacitação de Membros da OEA para o cumprimento de requisitos para o combate a ameaças à segurança cibernética na região, conforme propostos pela Estratégia interamericana abrangente para o combate de ameaças à segurança cibernética (http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm).”

A colaboração entre o Brasil e a OEA no marco da segurança cibernética se aprofundou em 2007, quando o Brasil sediou, entre 25 e 29 de junho, em Brasília, um Curso de Fundamentos para Implementação de Centros de Tratamento de Incidentes de Redes de Computadores de Governo.

Tratou-se do primeiro curso dessa natureza no âmbito da OEA, tendo por objeto as condições para a criação e o gerenciamento de Equipes de Resposta a Incidentes de Redes de Computadores (Computer Security Incident Response Teams - CSIRTs), com o intuito de prevenir, neutralizar e mitigar efeitos de atos contra infraestruturas cibernéticas críticas. Ainda em 2007, peritos brasileiros participaram, nos EUA, do 2º Seminário sobre Segurança e Crimes Cibernéticos, que tratou de tópicos no nível técnico e de políticas para a intensificação da colaboração e de parcerias estratégicas entre os Membros da OEA, corporações privadas e academia, com o propósito de melhor proteger infraestruturas críticas de ameaças cibernéticas.

Em 2008, representantes do governo brasileiro participaram do primeiro encontro da Rede Hemisférica de CSIRTs nacionais. O Brasil havia sido um dos cinco países participantes do projeto-piloto para desenvolvimento da referida rede interamericana, hoje em funcionamento, consistente na comunidade online de CSIRTs capazes de disseminar rapidamente informação sobre cibersegurança e oferecimento de assistência técnica e apoio na eventualidade de um incidente cibernético. Em 2009, o Brasil participou da Conferência conjunta entre Conselho da Europa e OEA sobre terrorismo e segurança cibernética, realizada em abril, em Madri.

Em novembro de 2009, o Brasil sediou, no Rio de Janeiro, seminário hemisférico de alto nível sobre segurança cibernética da OEA, envolvendo a Reunião de Ministros da Justiça das Américas (REMJA), a Comissão Interamericana de Telecomunicações (CITEL) e o CICTE, do qual resultaram recomendações para os esforços no âmbito daqueles foros para o fortalecimento da segurança cibernética.

Em 2010, técnicos de segurança cibernética brasileiros participaram, no Panamá, em Washington e em Montevideú, de cursos e seminários, sob os auspícios da OEA, sobre gerenciamento de CSIRTs e trocas de experiências e de boas práticas sobre respostas a incidentes cibernéticos.

Em 2011, o Brasil participou do seminário hemisférico sobre segurança cibernética e crime cibernético, em Miami, que congregou, em 5 dias, 102 representantes de 31 Estados Membros da OEA. As atividades de cooperação prosseguiram em 2012, com a participação brasileira no seminário sobre boas práticas em segurança cibernética e crimes cibernéticos, em Montevideú, e em debate para “cyber security policymakers”, em Ottawa. No mesmo ano, em São José da Costa Rica, técnicos brasileiros participaram de simpósio sobre segurança cibernética que permitiu a troca de informações sobre tendências e ameaças de hacking e de crimes cibernéticos.

Em 2013, representantes do governo brasileiro participaram, em Washington, de exercício simulado regional de gerenciamento de crise em segurança cibernética com vistas a avaliar a capacidade dos países de comunicação e cooperação internacional para o combate a ataque cibernético transnacional organizado capaz de comprometer infraestruturas críticas nacionais e regionais. O exercício serviu para testar mecanismos de resposta a incidentes, troca de informações e comunicações. O tema da resposta a ameaças a infraestruturas críticas foi também tratado em simpósios regionais sobre desafios à segurança cibernética para Estados e o papel de organizações internacionais, em Buenos Aires e em Montevideú.

Em outro evento, coordenado em conjunto entre a OEA e o Banco Interamericano de Desenvolvimento, em 2014, participantes brasileiros puderam beneficiar-se da troca de informações sobre práticas sobre o desenvolvimento de políticas nacionais sobre segurança cibernética em países da América Latina e do Caribe.

Em 2015, a OEA reuniu chefes de unidades de combate a crimes cibernéticos das Américas para debater a situação da criminalidade cibernética na região. Em setembro e outubro de 2015, representante do governo brasileiro participou, da sede da OEA, do OAS-FIRST Cybersecurity Technical Colloquium e do lançamento oficial do “Cybersecurity Awareness Month”. Em novembro, representante de Programa de Segurança Cibernética da OEA participou de Fórum de Governança da Internet, em João Pessoa. Também em novembro, representante brasileiro participou de seminário sobre segurança cibernética na proteção de infraestruturas críticas e sistemas de controle industrial, em Assunção.


Em março de 2016, o Programa de Segurança Cibernética promoveu, em Belo Horizonte, o seminário “Desafios de segurança cibernética no Brasil”, em parceria com o Ministério Público de Minas Gerais, que debateu o ponto de situação atual a respeito dos instrumentos disponíveis no Brasil para a investigação e combate a ameaças à segurança cibernética no Brasil.

Também em 2016, técnicos brasileiros participaram de treinamento da OEA sobre preservação de provas digitais em crimes cibernéticos, nos EUA. Outra iniciativa com a presença de participantes brasileiros, entre 200 peritos, realizada em Washington, debateu o futuro da governança da internet, segurança cibernética e liberdade de expressão na rede nas Américas, que promoveu a melhor compreensão das relações entre privacidade, proteção de dados e segurança cibernética.

No recurso de primeira instância, que pediu o montante das contribuições brasileiras ao CICTE, foi informado que o país não contribuiu desde 2005, sendo que os únicos registros de aporte financeiros vindos do Brasil são os seguintes:

Dezembro/2001: US \$20.000,00
Dezembro/2002: US \$15.000,00
Março/2004: US\$ 20.000,00
Janeiro/2005: US\$ 10.000,00
Total: US\$ 65.000,00

De acordo com a resposta ao primeiro pedido, notou-se que a OEA é o fórum multilateral com maior número de atividades estabelecidas sobre segurança e defesa cibernética, demonstrando sua importância e relevância na região.



Relações Multilaterais: Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas

No período de 9 a 20 de maio de 2016, o Centro de Instrução de Guerra Eletrônica (CIGE) realizou o 1º Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas. Em pedido de informação ao Ministério da Defesa, a ARTIGO 19 requisitou cópia do programa deste estágio, assim como da lista de participantes do mesmo, com seus respectivos países de origem.

O Ministério da Defesa enviou, após recursos em primeira e segunda instância, o programa e a lista de países que participaram do Estágio. No total, foram participantes de outros 12 países, sendo eles: Alemanha, Angola, Argentina, Chile, Colômbia, Nigéria, Peru, Senegal, Sri Lanka, Paraguai, Uruguai e República Dominicana. É notável a presença de países vizinhos e da região latino-americana. Percebe-se também que o Brasil está se tornando um exportador de conhecimento na área. Disponibilizamos, a seguir, o programa do Estágio recebido após pedido de informação pública:

Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas

Data	Hora	Local	UNIF	Disciplina / Assunto
09 Maio (Seg)	09:00 - 09:20	CDCiber	9º B2	Boas Vindas e Medidas Administrativas
	09:20 - 10:00			Aula Inaugural
	10:10 - 10:40			Doutrina Militar de Defesa Cibernética
	11:00 - 11:30			Visitação ao CDCiber
	11:30 - 12:00	-		Deslocamento para o CCOMGEX
	13:30 - 15:30	CIGE Laboratório Cibernética		Emprego do Simulador de Operações Cibernéticas (SIMOC)
	15:40 - 17:30	Lab Ciber		<i>Hardening</i> de Servidores
10 Maio (Ter)	08:30 - 10:30	Lab Ciber	9º B2	<i>Hardening</i> de Servidores
	10:30 - 12:30	Lab Ciber		Criptografia
	13:30 - 15:30	Lab Ciber		Criptografia
	15:30 - 17:30	Lab Ciber		<i>Information Gathering</i>
11 Maio (Qua)	08:30 - 10:30	Lab Ciber	9º B2	<i>Information Gathering</i>
	10:30 - 17:30	Lab Ciber		Vulnerabilidades em Sistemas Linux
12 Maio (Qui)	08:30 - 10:30	Lab Ciber	9º B2	Vulnerabilidades em Sistemas Linux
	10:30 - 17:30	Lab Ciber		Vulnerabilidades em Sistemas Windows
13 Maio (Sex)	08:30 - 12:30	Lab Ciber	9º B2	Vulnerabilidades em Sistemas Windows
	13:30 - 17:30	Lab Ciber		Vulnerabilidades em Redes sem Fio


Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas

Data	Hora	Local	UNIF	Disciplina Assunto
16 Maio (Seg)	08:30 - 17:30	Lab Ciber	9º B2	Vulnerabilidades em Páginas Web
17 Maio (Ter)	08:30 - 17:30	Lab Ciber		Técnicas de Forense em Windows
18 Maio (Qua)	08:30 - 17:30	Lab Ciber		Técnicas de Forense em Linux
19 Maio (Qui)	08:30 - 17:30	Saguão Piso Superior		Exercício prático
20 Maio (Sex)	08:30 - 10:30	Lab Ciber		Análise Pós-ação do Exército
	10:30 - 12:30	Saguão Piso Superior		Encerramento do Estágio

A partir da análise dos conteúdos oferecidos pelas Forças Armadas Brasileiras durante o Estágio, conforme ilustrado pela programação, não é possível afirmar que as técnicas utilizadas comprometem diretamente a privacidade ou o direito à liberdade de expressão dos usuários de internet na região. O hardening de servidores, por exemplo, é uma técnica usada para mapear ameaças e depois executar possíveis correções nos sistemas, preparando-os para determinadas tentativas de ataques ou violação na segurança da informação.”³⁰ Já o information gathering, ou seja, a técnica de acúmulo, ou ajuntamento de informações online, não necessariamente é uma técnica violadora de direitos, desde que seja realizada de maneira ética e responsável. Entretanto, há exemplos notórios da prática de técnicas de vigilância utilizadas por forças militares no Brasil, especialmente em momentos de intensas manifestações sociais, nas quais violou-se uma série de direitos constituídos.³¹

30 André Luiz Facina. Algumas técnicas de Hardening no OpenBSD. Disponível em: http://www.dicas-l.com.br/arquivo/algumas_tecnicas_de_hardening_no_openbsd.php#.WgmQsmdm-1E

31 Para mais informações sobre atividades precedentes, acesse: <http://protestos.artigo19.org/violacoes.php>, ou leia, ainda: <http://artigo19.org/blog/2016/09/30/exercito-conclui-ate-novembro-caso-do-capitao-apontado-como-infiltrado-entre-manifestantes/>



Pedidos de Informação no Paraguai e Argentina

A título de comparação, parceiros da ARTIGO 19 no Paraguai (TEDIC) e na Argentina (ADC) submeteram em seus países os pedidos de informações com pequenas adaptações por conta do contexto de cada nação.

Paraguai

No caso do trabalho feito pelo TEDIC no Paraguai, as Forças Armadas ofereceram respostas, positivas ou negativas, a todos os pedidos endereçados. De maneira geral, as respostas foram superficiais ou, então, redirecionadas a outros órgãos, que seriam, na visão das Forças Armadas paraguaias, responsáveis por fornecer as informações solicitadas.

Nas respostas, foi negada a existência de qualquer iniciativa relativa à defesa cibernética do MERCOSUL e disponibilizou as informações referentes às atividades no Conselho de Defesa Sul-Americano, fornecendo suas atas de reunião e apontando que a delegação peruana no órgão internacional é responsável por desenvolver as atividades do Grupo de Trabalho sem maior detalhamento. Reforçou que não há nenhuma parceria com entidades privadas nas atividades da UNASUL.

A nível nacional, o Ministério da Defesa Paraguuaio participou de um evento para discutir a implementação de um centro de segurança e defesa cibernética, organizado pela empresa de consultoria Argentina GL/GROUP, que apresentou sua expertise em termos de metodologia e processo para implementação desse tipo de iniciativas. O Ministério da Defesa paraguaio negou qualquer acordo financeiro ou político com a empresa em questão, mas sua participação demonstra o interesse do mesmo no tema.

Argentina

A investigação realizada pela ADC sobre a situação na Argentina foi dificultada pela reticência do Estado nacional em fornecer as informações referentes às atividades desenvolvidas na área de ciberdefesa. O percurso que as diversas tentativas de obter informações de caráter público denotam é o de um Estado que ainda não incorporou plenamente critérios de transparência e publicidade.

O primeiro pedido de informação foi realizado no dia 20 de julho de 2016 para o Ministério das Relações Exteriores. Ali, buscou-se indagar as atividades desenvolvidas pelo Estado argentino no marco da relação bilateral com o Estado brasileiro, o Conselho de Defesa da União de Nações Sul-Americanas (UNASUL) e a Organização dos Estados Americanos (OEA). Frente a tal pedido, a reação do Ministério foi solicitar um adiamento do prazo de resposta estabelecido pela normativa de 10 dias. A justificativa dada foi a quantidade e complexidade da informação solicitada. Então, o Ministério encaminhou a consulta aos Ministérios da Defesa e da Modernização.

O Ministério da Defesa solicitou outro adiamento para responder o pedido, mas, mesmo ao fim do prazo do adiamento, não foi dada nenhuma resposta. Por sua vez, o Ministério da Modernização respondeu de maneira curta, referindo-se unicamente à participação da Argentina no Comitê Interamericano contra o Terrorismo (CICTE) da OEA. Ali, explicaram que a participação no dito programa não implicava em nenhuma contribuição econômica ou tecnológica por parte do Estado nacional. Igualmente, informaram que os órgãos públicos que participam do CICTE são: o Ministério das Relações Exteriores, através da

Representação Especial para Assunto de Terrorismo e Outros Delitos Conexos (RETOD), e o Ministério da Modernização, através da Direção Nacional de Infraestruturas Críticas de Informação e Cibersegurança. A respeito do restante dos temas, eximiram-se de qualquer resposta com base na justificativa de que não tinham a competência para responder.

Ante a resposta pouco favorável às intenções propostas, foi enviado um novo pedido de informação ao Ministério da Defesa em 1 de novembro de 2016. Nessa ocasião, houve uma reunião com a Direção de Transparência Institucional do Ministério da Defesa, na qual afirmaram sua predisposição em colaborar com os pedidos de informação. Entretanto, o novo pedido tampouco foi respondido, apesar da tentativa por parte do Ministério em coordenar uma reunião com a Subsecretaria de Ciberdefesa. Quando chegou o momento de articular esse encontro, não houve contato.

Finalmente, em 5 de maio de 2017, apresentou-se outro pedido de acesso à informação ao Ministério da Defesa. Neste caso, houve uma resposta por parte da instituição. Contudo, esta se limitou unicamente a explicar as razões pelas quais – a seu critério – não poderiam nos oferecer a informação solicitada. Sobre o pedido de receber os registros das reuniões realizadas pelo grupo bilateral, afirmou-se que primeiro deveriam consultar o governo brasileiro e receber sua autorização para responder a solicitação.

A respeito das atividades realizadas no marco da UNASUL, a resposta foi que tal informação deveria ser requerida à própria organização internacional.

Por último, o Ministério afirmou não ter informações sobre a participação argentina na atividade de formação em defesa cibernética para oficiais de nações amigas organizada pelo Ministério de Defesa brasileiro em maio de 2016.³²

■ 32 Em vista de toda a reticência a entregar as informações requeridas, a ADC decidiu levar o caso à justiça, já que consideramos que essa situação afeta o direito a acesso à informação pública. Atualmente, o processo judicial está em trâmite e ainda não se emitiu uma resolução.



Considerações finais

Em 2013 e 2014, Brasil e Argentina protagonizaram um movimento de estreitamento de cooperação em ciberdefesa e ambos os países também demonstram interesse e ações concretas para levar esses tipos de ações a foros multilaterais, como a UNASUL e o MERCOSUL.

Contudo, a conclusão chegada é a de que, apesar da reação forte e articulada nos ambientes institucionais internacionais após as denúncias de 2013, essas atividades não se mantiveram nos anos seguintes. O GT criado no âmbito do Conselho de Defesa da UNASUL não realizou atividades nos anos de 2015 e 2016. O MERCOSUL, ao menos institucionalmente, demonstrou não ter levado a cabo os nove objetivos enunciados e apresentados na “Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da América nos Países da Região”. Logo, resta concluir que as ações conjuntas nessa área não estão ocorrendo nesses espaços atualmente.

Entretanto, o Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas é um indicativo de que o interesse de influência regional por parte do Estado brasileiro permanece – ainda que seja uma iniciativa liderada unilateralmente pelo Brasil.

Se as informações obtidas não são suficientes para identificar *a priori* práticas vigilanistas, por outro lado, tampouco demonstram comprometimento com o respeito e a promoção dos direitos humanos, nomeadamente a liberdade de expressão e a privacidade. As respostas aos pedidos de informação nos mostraram que os direitos humanos ainda não são parte do discurso oficial quando se refere a medidas de ciberdefesa e cibersegurança

Para que haja controle social sobre o que acontece no desenvolvimento dessas capacidades, é necessário que o governo seja transparente com relação às informações de protocolos, procedimentos, operações e poderio. O acesso à informação é um dos passos imprescindíveis para observância do respeito a direitos fundamentais, em especial a liberdade de expressão e a privacidade.

Durante todo o processo de requisição de informações públicas, houve entraves das instituições no fornecimento de informações e documentos. Dos oito pedidos de informação realizados pela ARTIGO 19, somente em um não foi necessário entrar com um recurso para mais informações. Em dois deles, a informação solicitada foi negada e os cinco restantes necessitaram de um ou dois recursos para que a autoridade responsável fornecesse uma resposta adequada.

A ARTIGO 19 acredita que é necessário ampliar o controle social sobre as atividades desenvolvidas e práticas estabelecidas no setor da defesa cibernética. Não se deve aceitar a justificativa de segurança nacional para a negação dos pedidos de informações, já que não se buscam detalhamentos de eventuais operações, mas sim números, informações históricas e protocolares que permitam à sociedade avaliar a capacidade de defesa e segurança cibernética do país.

São nossas recomendações, portanto:

A. Que o aparato de segurança não seja usado contra a própria população. Respeito à privacidade.

O desenvolvimento de um sistema de defesa e segurança cibernética não pode desconsiderar seus impactos na vida dos milhões de usuários de Internet no país. A utilização de técnicas de vigilância foi intensa em momentos de agita-

ção social nos últimos anos. A defesa cibernética trata-se de outra modalidade de atividade, contudo, não deve se pautar em ferramentas danosas ao livre fluxo de informações na rede de computadores a nível nacional nem ameaçar direitos estabelecidos dos cidadãos brasileiros.

B. Aperfeiçoamento dos sistemas de transparência ativa e passiva no âmbito da segurança da Internet.

As atividades de defesa e segurança cibernética que foram objetos dos pedidos de informação neste estudo deveriam estar em acesso público sem a necessidade de requisições. A ARTIGO 19 acredita que se deve buscar a implementação de um sistema de transparência nos órgãos responsáveis pelo estabelecimento da defesa e segurança cibernética nacional, que, não comprometendo informações sigilosas, forneçam à população a possibilidade de fiscalizar e, mais do que isso, participar dos rumos das políticas públicas da área, ampliando o rol de atores sociais participantes em um assunto ainda tratado com demasiado sigilo.





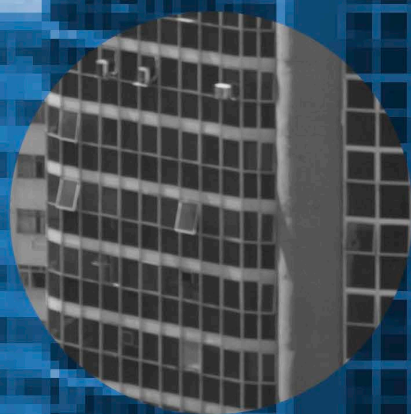
Sobre a ARTIGO 19

A ARTIGO 19 é uma organização não governamental de direitos humanos nascida em 1987, em Londres, com a missão de defender e promover o direito à liberdade de expressão e de acesso à informação em todo o mundo. Seu nome tem origem no 19º artigo da Declaração Universal dos Direitos Humanos da ONU.

Com escritórios em nove países, a ARTIGO 19 está no Brasil desde 2007 e tem se destacado por impulsionar diferentes pautas relacionadas à liberdade de expressão e informação, dentre as quais estão o combate às violações ao direito de protesto, a descriminalização dos crimes contra a honra, a elaboração e a implementação da Lei de Acesso à Informação e a construção e defesa do Marco Civil da Internet.

Contando com especialistas de diferentes campos, a organização atualmente se divide em quatro áreas: Acesso à Informação, Centro de Referência Legal, Direitos Digitais e Proteção e Segurança.

Se você quiser entrar em contato para discutir esta análise, por favor, envie um e-mail para comunicacao@artigo19.org.br.



ARTICLE 19