UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

HENRIQUE RIBEIRO DA ROCHA

ESTRATÉGIAS DE DEFESA E SEGURANÇA CIBERNÉTICA DE ARGENTINA, BRASIL E URUGUAI: UMA ANÁLISE COMPARADA

FLORIANÓPOLIS
2019

HENRIQUE RIBEIRO DA ROCHA

ESTRATÉGIAS DE DEFESA E SEGURANÇA CIBERNÉTICA DE ARGENTINA, BRASIL E URUGUAI: UMA ANÁLISE COMPARADA

Trabalho de Conclusão do Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais.
Orientador: Prof. Dra. Graciela de Conti Pagliari

FLORIANÓPOLIS

2019

HENRIQUE RIBEIRO DA ROCHA

ESTRATÉGIAS DE DEFESA E SEGURANÇA CIBERNÉTICA DE ARGENTINA, BRASIL E URUGUAI: UMA ANÁLISE COMPARADA

A Banca Examinadora resolve atribuir a nota 8,5 ao acadêmico Henrique Ribeiro da Rocha pela apresentação do trabalho intitulado: Estratégias de Defesa e Segurança Cibernética na Argentina, Brasil e Uruguai: Uma Análise Comparada sendo este trabalho de conclusão de curso julgado adequado para obtenção do Título de Bacharel e aprovado em sua forma final pelo Curso de Relações Internacionais

Florianópolis, 10 de dezembro de 2019.

_____

Prof. Dra. Graciela de Conti Pagliari

Orientadora

Universidade Federal de Santa Catarina

_____

Prof. Dra. Danielle Jacon Ayres Pinto

Avaliadora

Universidade Federal de Santa Catarina

_____

M.ª Júlia Loose

Avaliadora

Universidade Federal de Santa Catarina

AGRADECIMENTOS

Para mim, só existe uma forma de começar esse agradecimento: agradecendo àqueles que realizaram tremendo esforço para que eu fosse a primeira pessoa de minha família a realizar o sonho de se formar em uma instituição superior de ensino público, gratuito e de qualidade. Então, aos meus pais, o meu mais sincero obrigado. Eu definitivamente não teria chegado até aqui se não fosse pelo esforço diário de vocês para me manter em outro estado do País focando em meus estudos. Vocês são o melhor exemplo que eu poderia ter. E lógico, também agradeço a minha irmã, que desde que me lembro por gente foi o meu grande suporte e inspiração de vida e que nunca hesitou em me ajudar quando precisei, obrigado.

Esse segundo semestre de 2019 teria, certamente, sido mais complicado caso eu não tivesse amigas como Adrielly Moroz e Ana Beatriz, que compartilharam os momentos bons e ruins do fim de graduação comigo, mas que certamente tornaram essa jornada mais leve, obrigado! Também agradeço ao Gustavo e a Victoria, que nestes últimos anos de graduação se tornaram a minha família em Florianópolis, definitivamente não teria sido o mesmo sem vocês comigo.

Não posso deixar de agradecer as/aos amigas/os e colegas que, ao longo da graduação, estiveram presentes comigo nos mais diversos âmbitos: seja no Centro Acadêmico de Relações Internacionais (CARI), seja na organização de eventos como a SemanaRI, o SiEM e o EERRI, ou nos grupos de pesquisa e extensão como o GESED e o GEPPIC, estes momentos foram extremamente enriquecedores para mim e para o meu crescimento pessoal e profissional.

Aos meus comparsas, Ana Beck e João Bosso, que não somente, mas principalmente ao longo de 2019, foram extremamente queridos e atenciosos comigo, sempre tentando me manter animado e focado, mesmo em momentos em que tudo parecia impossível, obrigado. As/aos diversas/os outras/os amigas/os que fiz ao longo da graduação e que tornaram a minha experiência na Universidade inesquecível: Arthur, Bonatto, Carolzinha, Davi, Duda, João Pedro, Júlia, Letícia, Leonardo, Maria Carolina, Martina, Milke, Monalisa, Sagaz, Telma, Vitória e todos àqueles outros que, de alguma forma, participaram destes 4 anos tão importantes de minha vida, obrigado!

Por fim, agradeço a Universidade Federal de Santa Catarina por ter me acolhido e ter sido a minha casa nos últimos 4 anos. As/aos incríveis professoras/es com quem tive a oportunidade de aprender e compartilhar a sala de aula, como as

professoras Danielle, Juliana, Patrícia, entre tantas outras e outros professores. A minha incrível orientadora, professora Graciela, que aceitou fazer parte deste trabalho comigo mesmo estando realizando suas pesquisas de campo na América do Norte no primeiro semestre de trabalho, e que sempre esteve disponível para me auxiliar no que fosse necessário, obrigado! Aos TAEs, em especial àqueles com quem tive a oportunidade de trabalhar na coordenadoria de cursos do CSE: Ana, Diogo, Filipe, Luci e Thaynara, vocês, e o incrível trabalho que vocês fazem por essa Universidade, são gigantes.

RESUMO

A presente monografia tem como objetivo geral realizar o mapeamento das estratégias de defesa e segurança cibernética de Argentina, Brasil e Uruguai a partir de uma pesquisa exploratória. Para alcançar este objetivo, foram utilizados documentos oficiais dos países como Livros Brancos de Defesa Nacional, Decretos, Leis, entre outros. Além disso, também se buscou compreender o que cada um dos Estados compreende por defesa cibernética e segurança cibernética, além de terem sido trabalhados os organismos responsáveis por cada uma dessas esferas nos três casos, como por exemplo comandos cibernéticos militares e centros de resposta a incidentes cibernéticos. O problema de pesquisa esteve centrado em entender qual o impacto das ameaças no ciberespaço para o estabelecimento de estratégias de defesa e segurança cibernética nos documentos oficiais dos Estados e foi possível verificar que, de fato, as ameaças presentes no ciberespaço influenciam no estabelecimento de estratégias voltadas para defesa e segurança cibernética.

Palavras-chave: Estratégias. Defesa Cibernética. Segurança Cibernética.

ABSTRACT

This study aims to map the cyberdefense and cybersecurity strategies of Argentina, Brazil and Uruguay from an exploratory research. In order to achieve this goal, official documents from the three countries such as National Defense White Papers, Decrees, Laws, among others were used. In addition, we also sought to understand what each state understands for cyberdefense and cybersecurity, as well as what are the bodies responsible for each of these spheres in the three states analysed, such as military cyber commands and cyber incident response centers. The research problem was centered on understanding the impact of cyberspace threats on the establishment of cyberdefense and cybersecurity strategies in the official documents of the states and it was made possible to verify that, in fact, the cyberspace threats influence the establishment of strategies aimed at cyberdefense and cybersecurity.

Keywords: Strategy. Cyberdefense. Cybersecurity.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE MAPAS

LISTA DE ABREVIAÇÕES

Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento - AGESIC

Banco Interamericano de Desenvolvimento - BID

Centro de Defesa Cibernética - CDCiber

Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores - CERT

Centro de Resposta a Incidentes de Segurança Cibernética do Ministério da Defesa uruguaio - DCSIRT

Comando de Defesa Cibernética brasileiro - ComDCiber

Comando Conjunto de Ciberdefesa - CCCD

Conselho Argentino de Relações Internacionais - CARI

Conselho de Defesa Sul-Americano - CDS

Denial of Service - DoS

Departamento de Segurança da Informação e Comunicações - DSIC

Diretiva de Política de Defesa Nacional - DPDN

Estratégia Nacional de Defesa - END

Estratégia Nacional de Segurança Cibernética - E-CIBER

Forças Armadas - FFAA

Infraestruturas Críticas - IFCs

Livro Branco de Defesa Nacional - LBDN

Livro Verde de Segurança Cibernética - LVSC

Ministério da Defesa - MD

Organização dos Estados Americanos - OEA

Política Nacional de Defesa - PND

Segurança da Informação - SI

Tecnologias da informação e comunicação - TICs

União de Nações Sul-Americanas - UNASUL

SUMÁRIO

INTRODUÇÃO

No campo das Relações Internacionais, principalmente a partir dos anos 1980 com o aumento do acesso à novas tecnologias, o espaço cibernético tem recebido enorme atenção por grande parte da população mundial, atingindo inclusive altos níveis de dependência do ciberespaço para serviços cotidianos como o serviço de bancos ou até mesmo o fornecimento de água ou energia: atualmente quase tudo funciona conectado a internet. Essa crescente ligação do mundo real com o mundo virtual passou, ao longo dos anos, a chamar a atenção dos Estados, pois o ciberespaço passou a ser categorizado como um novo território de atuação estatal e não-estatal, ao passo que ações realizadas no mesmo além de terem efeitos no próprio espaço cibernético, podem também ter efeito fora dele. Casos de ataques cibernéticos têm se tornado cada vez mais comuns, posto que para realizá-los e obter resultados não existe a necessidade de se possuir Forças Armadas, por exemplo, como tradicionalmente no campo de segurança e defesa militar. Atores com menos capacidades e/ou recursos financeiros, contanto que possuam o conhecimento necessário de códigos e sistemas computadorizados efetivos, podem realizar ações de ofensa cibernética que colocam em risco não apenas a segurança da sociedade e de empresas privadas, mas até mesmo a defesa nacional de Estados.

Exposto isso, neste trabalho serão utilizados teóricos tanto do campo de estudo das relações internacionais como teóricos de outros campos de atuação que estejam discutindo questões referentes ao espaço cibernético, de maneira a compreender o que levou a ascensão do ciberespaço como um novo campo de atuação internacional. Ascensão que deve ser vista como algo positivo, posto que nunca antes a população mundial tivera acesso tão facilitado a tanta informação. Contudo, neste cenário inovador também se fazem necessários métodos de segurança e defesa cibernética, para evitar que informações e dados disponíveis no ciberespaço sejam utilizados erroneamente, de maneira a evitar que Estados, empresas, Organizações Internacionais, Forças Armadas e pessoas comuns utilizando meios cibernéticos corram riscos de ter seus dados e informações comprometidas ou utilizados de forma negativa (GONZALES, 2017).

Nesse sentido, o cerne do presente trabalho se propõe a realizar um estudo exploratório sobre as capacidades de defesa e segurança cibernéticas de Argentina,

Brasil e Uruguai, assim como de suas estratégias de cibersegurança e ciberdefesa a partir dos documentos oficiais dos três Estados, como Livros Brancos, Decretos, Leis, entre outros. Os três Estados (e especialmente o Uruguai, apesar de não possuir muitos documentos oficiais que façam referência ao setor cibernético) foram escolhidos para esta análise pois são, de acordo com índices internacionais como o Índice Global de Cibersegurança, considerados os três países com o maior índice de cibersegurança na região da América do Sul, além de serem também os três mais poderosos no ciberespaço, ainda de acordo com o Índice. Visto que essa é uma área bastante nova e ainda pouco explorada, com o resultado se espera que seja possível um aprofundamento do tema em futuras pesquisas.

O presente estudo tem como principal objetivo o mapeamento das estratégias de Defesa e Segurança Cibernética de Argentina, Brasil e Uruguai, países que foram escolhidos para esta análise por serem os três maiores expoentes na região sul-americana em questões cibernéticas. Será trabalhado o entendimento de cada um dos três acerca do que eles compreendem por Defesa e Segurança cibernética e também como eles estão se preparando para responder às ameaças que surgem no espaço cibernético e colocam em risco as infraestruturas críticas nacionais [1]destes Estados. Entre os objetivos específicos estão compreender o que cada país entende por defesa e segurança cibernética, explorar quais são os órgãos responsáveis por questões de ciberdefesa e cibersegurança em cada um dos países e, por fim, explorar os documentos oficiais dos Estados para entender quais estratégias estão sendo elencadas por Argentina, Brasil e Uruguai para se prevenir e/ou combater ameaças e agressões no ciberespaço.

O que nos traz ao seguinte problema de pesquisa: como se dá o estabelecimento de estratégias de defesa e segurança cibernética em Argentina, Brasil e Uruguai?

A metodologia utilizada no trabalho é a de estudo exploratório dos documentos oficiais de governo - ou seja, fontes primárias - para em futuros trabalhos aprofundar e problematizar a pesquisa sobre a temática de defesa e segurança cibernética na

[1] Infraestruturas críticas são um conjunto de instalações físicas e/ou informatizadas que, se descontinuadas ou destruídas impactariam negativamente o funcionamento da sociedade de um Estado. São exemplos de IFCs os sistemas de informação, transporte e fornecimento de água. Ainda é necessário que haja melhor definição do termo, uma vez que a maior parte das IFCs estão na mão do setor privado, entretanto, ainda é responsabilidade do Estado protegê-las, o que talvez precise ser reformulado.

Argentina, Brasil e Uruguai. Serão utilizadas também análises comparativas para melhor elucidar os três casos, além de análises qualitativas.

1 SECURITIZIAÇÃO DO CIBERESPAÇO E REGULAMENTAÇÃO DO MESMO NA ARGENTINA, BRASIL E URUGUAI

Neste capítulo serão analisados, a partir dos documentos oficiais de Defesa de cada país e também da literatura já existente sobre o tema, quais são os entendimentos de Argentina, Brasil e Uruguai acerca do que é defesa cibernética e o que é segurança cibernética, bem como seus entendimentos acerca do espaço cibernético, para que no próximo capítulo sejam colocados em comparação os entendimentos dos três países acerca destas questões cibernéticas e, também, sejam analisados quais são os órgãos - em cada país - responsáveis por lidar com defesa e segurança cibernética.

Além disso, neste primeiro capítulo será trabalhada a necessidade que os Estados percebem para que haja maior securitização do espaço cibernético, bem como a priorização deste tema em suas agendas. Também serão ilustrados casos notórios de ciberataques para possibilitar melhor ilustração do tema, como o caso Stuxnet no Irã, que é considerado como um marco nos estudos sobre ciberdefesa tendo em vista que, a partir deste ataque, os Estados perceberam que era necessário voltar seus esforços para o setor cibernético uma vez que, enquanto não houver securitização do ciberespaço, as infraestruturas críticas e a soberania estatal estarão em perigo.

O espaço cibernético assume, principalmente a partir do século XXI, o caráter de uma nova esfera para a realização de relações internacionais, passando a ser considerado por inúmeros Estados, como é o caso de Brasil, Estados Unidos e Israel, países que já citam em seus documentos oficiais de Defesa o ciberespaço como uma nova dimensão de atividades estatais e não-estatais, da mesma maneira que o ar, mar, terra e o espaço sideral. Devido a isso, como apontam Medeiros et al. (2019), o espaço cibernético começa a passar por um processo de securitização por parte dos Estados, a fim de se protegerem das diversas ameaças que se tornam presentes nesta nova realidade[2].

Para maior compreensão da necessidade que os Estados percebem para que haja securitização do espaço cibernético, é importante frisar que neste espaço os mais

[2] "Vista do Uma análise sobre o processo de ... - EB Revistas.". Disponível em: <http://ebrevistas.eb.mil.br/index.php/RMM/article/view/1889/1763>. Acessado em 2 set. 2019.

diversos dados e informações civis, diplomáticos, militares e políticos, sigilosos ou não, trafegam e se interconectam, o que em determinado momento passou a chamar a atenção de diversos atores - sejam eles estatais ou não-estatais - para este espaço, tendo em vista que basicamente toda a informação existente no globo está disponível nele, inclusive as informações mais críticas dos Estados nacionais. (GONZALES; PORTELA, 2018).

1.1 CIBERATAQUES NOTÓRIOS E ESFORÇOS ESTATAIS VOLTADOS PARA O CIBERESPAÇO

O ciberespaço, para além de um meio de comunicação e de difusão de informações, tornou-se um canal pelo qual atores estatais e não-estatais comumente se enfrentam. Neste subtópico serão tratados alguns ciberataques de grande repercussão no cenário internacional, como o caso Stuxnet que foi selecionado por ser considerado um marco em questões de defesa e segurança cibernética no sistema internacional pois, a partir dele, muitos Estados passaram a perceber que sua soberania poderia ser colocada em risco por meio da utilização do ciberespaço, também será colocado em análise a necessidade que os Estados percebem para que os mesmos voltem esforços significativos para o setor cibernético.[3]

Como exemplo de um ciberataque pode se pensar o caso Stuxnet, descoberto em junho de 2010, ataque alegadamente realizado em conjunto pelos Estados Unidos e Israel, tendo como alvo as centrífugas iranianas que enriquecem urânio. Para a realização deste ataque foi injetado um malware por meio da inserção de cabos USB na rede do país, tendo como objetivo sabotar ou restringir o funcionamento das centrífugas do Irã, como apontou, Bestuzhev (2017) e o que, de fato, se concretizou. O impacto deste ciberataque foi tão grande que se estima que em decorrência dele o desenvolvimento do projeto nuclear iraniano sofreu um atraso de cerca de 10 anos. Um ponto central ao analisar o caso Stuxnet é ter em mente que este ciberataque provou que um vírus de computador pode ser tão ou mais nocivo que um ataque físico, uma vez que por meio da utilização de esforços cibernéticos foi possível destruir as

[3] Será utilizado o caso Stuxnet pois este é o ataque mais considerado pela literatura existente, entretanto, talvez o mais emblemático seja o caso da Estônia. Ainda é necessário que haja maior discussão acerca destes dois ataques para melhor entende-los e classifica-los, e isso será trabalhado em pesquisas futuras.

máquinas de enriquecimento de urânio do Irã, causando prejuízos gravíssimos ao país em questão.

Entretanto, é preciso levar em consideração que Estados Unidos e Israel não assumiram publicamente a responsabilidade pelo ataque, o então secretário de imprensa da Casa Branca, Josh Earnest, quando questionado por repórteres acerca do envolvimento estadunidense no ataque respondeu que "certas informações não devem ser divulgadas porque divulgá-las seria uma ameaça à segurança nacional".[4] O vírus em questão se encontrava presente em incontáveis computadores Windows, iOS, entre outros. Contudo, era inofensivo para estes, tendo em vista que o Stuxnet foi desenvolvido e aplicado para atingir e destruir as centrífugas de enriquecimento de urânio iranianas.

Entre as principais questões que levaram Estados nacionais a voltarem esforços significativos para o espaço cibernético, de maneira a garantir a segurança de suas diversas infraestruturas críticas e de seus cidadãos como um todo, está a facilidade de novos atores conduzirem ciberataques ou realizarem os mais diversos tipos de atividades ilegais neste ambiente. Tendo em vista que o custo para a realização de um ciberataque é, em comparação com ataques físicos e tradicionais, extremamente baixo e, da mesma maneira que os ataques convencionais, estes ciberataques podem causar impactos grandiosos mesmo que haja envolvimento de poucas pessoas na aplicação do ciberataque.

No discurso de Estados para o estabelecimento da securitização do espaço cibernético estão atreladas principalmente questões envolvendo o ciberterrorismo, espionagem e ciberataques direcionados às infraestruturas críticas nacionais, situação que gera preocupação enorme também ao Brasil, levando em conta a catástrofe que poderia ser desencadeada caso fosse tomado o controle de hidrelétricas brasileiras por meios cibernéticos, por exemplo. Para elucidar a preocupação com ciberespionagem, se pode pensar o caso sofrido pela ex-presidenta Dilma Rousseff, que foi trazido à tona no ano de 2013 por Edward Snowden, a partir da divulgação de diversos documentos governamentais secretos dos Estados Unidos que comprovaram que o país, por meio de suas agências de inteligência, estava

[4] "Stuxnet was work of U.S. and Israeli experts, officials say - The ...." 2 jun. 2012, Disponível em: <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>.Acessado em 22 out. 2019

espionando e monitorando telefones, e-mails e ações da ex-presidenta, assim como de outras autoridades e organizações latino-americanas. Na época, Dilma Rousseff chegou a adiar uma viagem que estava programada aos Estados Unidos.

Para pensarmos a diferença entre um ataque tradicional e um ciberataque como foi o caso Stuxnet citado anteriormente, podemos analisar o recente ocorrido entre o Estado de Israel e o Hamas: o movimento palestino Hamas possuía, até maio de 2019, um prédio denominado “Hamas Cyber Headquarters”[5], local em que o grupo, de acordo com autoridades israelenses, realizava ciberataques direcionados à infraestruturas críticas[6] de Israel. O que ocorreu em maio deste ano foi que Israel, utilizando-se de um ataque tradicional-físico, bombardeou o prédio onde o grupo se localizava, impossibilitando, pelo menos por algum tempo, que o grupo pudesse realizar ações ofensivas contra Israel por meio do espaço cibernético.

No espaço cibernético, possuindo a capacidade mínima de recursos necessários - como por exemplo o acesso à internet e a componentes eletrônicos tais quais computadores, tablets, celulares -, qualquer pessoa, Estado, grupo ou Organização pode realizar atividades a partir de qualquer ponto do globo mesmo que o seu alvo esteja em um ponto completamente oposto ao seu. Por exemplo**,** o caso ocorrido em 2013, no qual a Target, que é a segunda maior cadeia de varejo dos Estados Unidos, sofreu um ataque cibernético de larga escala, onde os dados de cerca de 110 milhões de clientes da rede foram sequestrados no período de 27 de novembro a 15 de dezembro do mesmo ano. Entre os dados estavam informações bancárias e dados pessoais, como endereços de e-mail e números de telefone. Interessante frisar que não foi a própria Target que percebeu o ataque, e sim o serviço secreto dos Estados Unidos, que uma vez tendo percebido a realização de movimentações bancárias suspeitas levou isso até a marca. De acordo com os serviços de segurança estadunidenses, o grupo de hackers responsável localizava-se na Europa Oriental e instalou um malware[7] no sistema das caixas registradoras da

[5] O que o ataque de Israel a hackers do Hamas significa para o futuro ...." 8 mai. 2019, Disponível em: <https://epocanegocios.globo.com/Mundo/noticia/2019/05/o-que-o-ataque-de-israel-hackers-do-hamas-significa-para-o-futuro-da-guerra-cibernetica.html>. Acessado em 2 set. 2019.
[6] Infraestrutura crítica é um termo utilizado para designar os ativos que são necessários para manter o funcionamento da sociedade, como por exemplo a produção e distribuição de energia.
[7] "Aprenda as diferenças entre vírus, trojans, spywares e outros ...." 31 out. 2008, Disponível em: <https://www.tecmundo.com.br/phishing/853-aprenda-as-diferencas-entre-virus-trojans-spywares-e-outros.htm>. Acessado em 23 ago. 2019.

marca para, assim, ter acesso às informações de cartões de crédito que ali fossem utilizadas.

Diante do cenário de possíveis ciberataques a qualquer momento sem grandes - ou quaisquer - avisos prévios, os Estados percebem-se na obrigação de elaborar estratégias de defesa e segurança cibernética a fim de proteger seus setores estratégicos, suas informações críticas e sigilosas, bem como proteger a sua população de possíveis ataques. Em um contexto em que cada vez mais o ciberespaço se destaca como uma das principais esferas de interação internacional seja entre Estados, seja entre atores não-estatais, os Estados estão se articulando para combater e neutralizar as ameaças realizadas neste território (AYRES PINTO, 2017).

1.2 DEFINIÇÕES DOS TERMOS POR CADA ESTADO EM ANÁLISE

Existem distinções entre o que diferentes Estados consideram como defesa cibernética e segurança cibernética e outros termos envolvendo questões cibernéticas, nesta seção serão expostas as definições de Argenta, Brasil e Uruguai acerca do que estes países definem por cibersegurança, ciberdefesa, segurança da informação para que, no próximo capítulo, seja possível analisar comparativamente estes termos e, também, explorar definições de outros termos mais específicos.

Posto isso, a definição do governo brasileiro é de que Defesa cibernética, como aponta o IPEA (2013), remete a ações defensivas, exploratórias e ofensivas, a partir do delineamento militar a fim de proteger os sistemas de informação, bem como as próprias informações críticas nacionais, também visa a obtenção de dados para produção de inteligência e para acarretar danos aos sistemas de informação do inimigo (BRASIL, 2011). Já a segurança cibernética, na visão do Brasil, tem relação à proteção e garantia da utilização de ativos de informação estratégicos, em especial os que são relacionados a exercer controle sobre as infraestruturas críticas nacionais.[8] O governo também destaca que a cibersegurança abrange a interação com os órgãos públicos e privados que estão envolvidos em atividades das infraestruturas críticas nacionais (BRASIL, 2011).

[8] "TD 1850 - A Segurança e Defesa Cibernética no Brasil e uma Revisão ...." Disponível em: <http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=19183>. Acessado em 23 ago. 2019.

O Estado argentino traz a definição de Segurança da Informação, que envolve “investigações e desenvolvimentos relativos a detenção, classificação e identificação de intrusos, honeypots, redes virtuais privadas e firewalls” (ARGENTINA, 2010). Já a respeito do termo Defesa Cibernética, a Argentina destaca que este não trata apenas de garantir a segurança dos sistemas de informação em casos de espionagem, mas também de buscar autonomia no assunto de Defesa Cibernética e avançar em ações para proteger seu ciberespaço frente à ameaças externas que possam “ser perpetradas contra os interesses vitais e estratégicos do País e de sua população” (ARGENTINA, 2015).

A respeito do espaço cibernético a Argentina traz as seguintes considerações em sua Diretiva de Política de Defesa Nacional do ano de 2018:

> O desenvolvimento de novas tecnologias da informação e comunicação, juntamente com a extensão global da conectividade, fizeram do ciberespaço uma área na qual os Estados implementam operações de agressão e influência sobre nações adversárias. A tendência para uma maior competição estratégica internacional no ciberespaço levou vários países a desenvolver capacidades cibernéticas de ponta, a fim de garantir a segurança de sua infraestrutura crítica ou estratégica de computadores. A república Argentina deve adaptar suas organizações militares ao impacto que emerge desses novos riscos. A política de defesa cibernética deve se concentrar na redução gradual de vulnerabilidades que emergem da informatização de ativos estratégicos de interesse da Defesa Nacional (DPDN, 2018, tradução própria).

A partir da interpretação deste trecho que discorre a respeito do espaço cibernético, é possível identificar que existe uma grande preocupação do Estado argentino quanto ao ciberespaço e suas utilizações, uma vez que o país elucida que Estados implementam operações de agressão e influência sobre outras nações por meio deste território, bem como quando é destacado que a Argentina precisa adaptar suas organizações militares de forma a concentrar sua Defesa cibernética na atuação para reduzir gradualmente as vulnerabilidades advindas do ciberespaço e que põem em risco os ativos estratégicos argentinos.

Ainda pensando as definições brasileiras: como destaca o Ministério da Defesa (2014), a partir de 2008, ano em que foi lançada a Estratégia Nacional de Defesa (END), surgem duas distinções de termos, sendo elas: “a Segurança Cibernética, que estaria a cargo da Presidência da República, e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas” (MD, 2014). Diante disso, é

necessário distinguir os termos, ainda de acordo com o Ministério da Defesa (2014), a Defesa Cibernética seria:

> um conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (MD, 2014).

Já a Segurança cibernética é definida pelo Ministério da Defesa (2014) como a "arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (MD, 2014). A partir dessas definições, é possível analisar que, ao passo que a Defesa Cibernética está mais relacionada à ações operacionais para deter as diversas ameaças que surgem no ciberespaço, a Segurança Cibernética está mais ligada aos cuidados para evitar que ditos ataques ocorram e venham a corromper os sistemas de informação e as infraestruturas críticas do país.

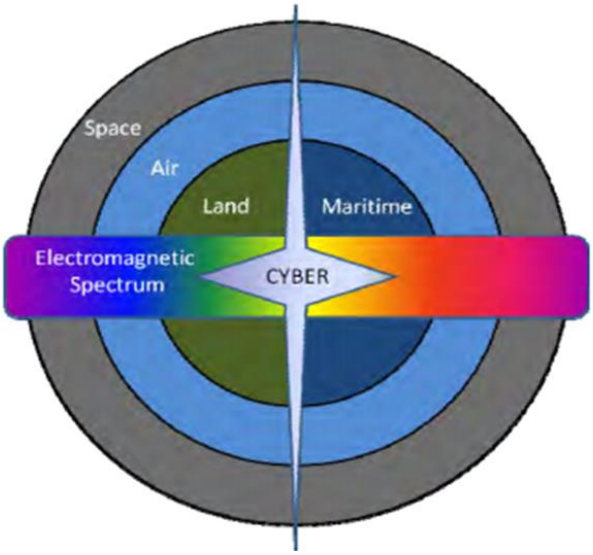
O Brasil ainda não possui em seus documentos oficiais de Defesa uma definição brasileira do que se considera como espaço cibernético, entretanto, no Livro Verde: Segurança Cibernética no Brasil, é trazido a conceituação feita por Pierre Levy, que é a seguinte:

> O que seria o espaço cibernético? O espaço cibernético é um terreno onde está funcionando a humanidade, hoje (...) é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores. Atualmente, temos cada vez mais conservados, sob forma numérica e registrados na memória do computador, textos, imagens e músicas produzidos por computador. Então, a esfera da comunicação e da informação está se transformando numa esfera informatizada. (...) Com o espaço cibernético temos uma ferramenta de comunicação muito diferente da mídia clássica, porque é nesse espaço que todas as mensagens se tornam interativas, ganham uma plasticidade e têm uma possibilidade de metamorfose imediata. E aí, a partir do momento que se tem o acesso a isso, cada pessoa pode se tornar uma emissora, o que obviamente não é o caso de uma mídia como a imprensa ou a televisão. (...) Do interior do espaço cibernético encontramos uma variedade de ferramentas, de dispositivos, de tecnologias intelectuais. Por exemplo, um aspecto que se desenvolve cada vez mais, nesse momento, é a inteligência artificial. Há também os hipertextos, os multimídias interativos, simulações, mundos virtuais, dispositivos de tele-presença. (...) O importante é que a informação esteja sob a forma de rede e não tanto a mensagem, porque esta já existia numa enciclopédia ou dicionário". (BRASIL, 2010, p.18 *apud* LEVY, 1994, n.p)

O Marco de Cibersegurança uruguaio de 2018 elaborado pela Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento (AGESIC), define o “ciclo de vida” da cibersegurança, sendo este: identificar, proteger, detectar, responder e recuperar. O documento também define cada parte do ciclo: a identificação está vinculada ao entendimento do contexto da organização, assim como aos ativos que dão suporte aos processos críticos das operações e aos riscos que podem estar envolvidos. Este entendimento serve para que os recursos e investimentos sejam definidos de acordo com a estratégia de gerenciamento de riscos e seus objetivos. A proteção está ligada à aplicação de medidas para proteger os ativos e os processos da organização em questão. Já a detecção está relacionada a execução de atividades para identificar o mais rápido possível os incidentes de segurança, por meio do monitoramento contínuo e processos de detecção. O ciclo de resposta diz respeito a definição e execução de atividades de resposta aos incidentes, com o objetivo de reduzir o impacto. Por último, o documento define a recuperação como a execução de atividades destinadas a gerenciar “planos e atividades para restaurar processos e serviços devido a um incidente de segurança”, tendo como objetivo último a resistência dos sistemas e instalações e, caso haja de fato incidentes, possa apoiar a recuperação das operações (AGESIC, 2018).

De acordo com Gonzales (2019), é preciso ter em mente que o espaço cibernético é, assim como as dimensões de terra, ar, mar e o espaço sideral, um espaço de apropriação e de uso, o qual contém inúmeros recursos para os mais diversos aproveitamentos e, a partir destes recursos e da estabilização de quem são aqueles que os detém, são firmadas relações de poder. Além disso, a partir da estabilização do espaço cibernético, todos os domínios se encontram interconectados, como se pode perceber na imagem abaixo:

Figura 1 – Diagrama das Relações de Domínio Operacional de Combate



Fonte: EUA, Air Force, apud Convertino, Sebastian, Flying and Fighting in Cyberspace, July 2007, Air University, p. 11

A figura anterior torna clara a relevância do espaço cibernético e a dimensão do poder detido por aqueles que possuem o controle deste domínio - poder que, de acordo com Nye (2011), se torna extremamente difuso no século XXI, podendo este se encontrar tanto na mão de atores estatais como de atores não-estatais - posto isso, a partir do ciberespaço é possível realizar ações ofensivas que podem se estender e afetar a todos os outros domínios, sendo estes: ar, mar, terra, e até mesmo o espaço sideral.

Como apontam Lobato e Kenkel[9] (2015), o aumento de ataques cibernéticos e também a publicação do Manual de Tallinn mostram que a comunidade internacional como um todo possui riscos bastante altos quando o assunto é tecnologias de informação e comunicação, uma vez que há um crescimento enorme no acesso e publicação de informações no ciberespaço principalmente a partir do início do século XXI, o que coloca em cheque a segurança da informação e, devido a isso, os Estados percebem que a securitização do ciberespaço precisa ser priorizada e colocada no topo da agenda. Antes dos anos 1990, questões que envolviam cibersegurança eram bastante restritas àqueles que eram experts em computação, contudo, a partir do desenvolvimento da tecnologia que presenciamos pelo menos nos últimos 30 anos,

[9] "Discourses of cyberspace securitization in Brazil and in the ... - SciELO." Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292015000200023>. Acessado em 2 set. 2019.

ameaças virtuais agora afetam a sociedade em geral, especialmente devido a crescente globalização da cibernética (HANSEN; NISSENBAUM, 2009).

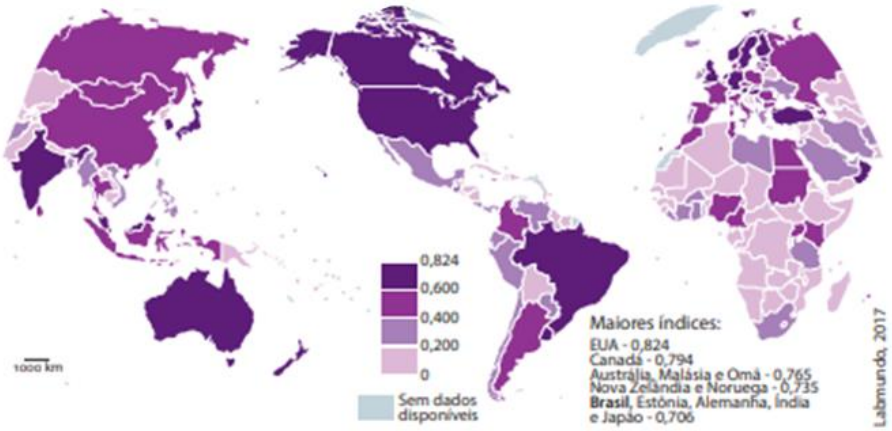
Como supracitado, as estratégias de Segurança e Defesa cibernética alavancaram sua posição na agenda política e militar dos países ao redor do globo nas últimas décadas, posto a dimensão de importância que o ciberespaço vem desempenhando no cenário internacional contemporâneo - bem como o expoente aumento de interações realizadas no mesmo - nas esferas econômica, política e social, como postula Choucri (2012). Diante disso, nesta pesquisa serão tratados especificamente os casos de Argentina, Brasil e Uruguai neste novo cenário, de maneira a compreender o desempenho dos três países sul-americanos de maior relevância do espaço cibernético bem como de buscar compreender como estes três países vêm se articulando frente às diversas ameaças que estão presentes nesse novo território de projeção de poder.

1.3 REGULAMENTAÇÃO SOBRE O CIBERESPAÇO

Nesta seção será trabalhado o poder cibernético dos três países em análise em perspectiva global e regional, além da relevância do Brasil quando o assunto tratado é ataques cibernéticos a nível global. Nas subseções, serão tratadas as regulamentações que estão sendo desenvolvidas por Argentina, Brasil e Uruguai acerca da temática de cibersegurança e ciberdefesa.

De acordo com o Atlas da Política Brasileira de Defesa (2017), no ano de 2015, Brasil, Uruguai, Colômbia e Argentina representavam os quatro países da América do Sul com maior poder no espaço cibernético, como se pode perceber na imagem abaixo:

Mapa 1 – Índice Global de Cibersegurança, por país, em 2015



Fonte: ITU, 2015

A partir da análise do índice global de cibersegurança por país no ano de 2015 trazida pelo Atlas de 2017 é possível inferir que, na América do Sul, Brasil, Uruguai, Argentina e Colômbia, respectivamente, são os países com o maior índice de cibersegurança na região. É interessante destacar que o Brasil apresenta o mesmo índice (0,706) que alguns países centrais, como Alemanha e Japão, estando também bastante próximo do índice dos Estados Unidos (0,824). O índice foi produzido com base no relatório Medindo a Sociedade da Informação (MIS), que apresenta uma visão global dos últimos desenvolvimentos em tecnologia da informação e comunicação, se baseando em dados comparáveis internacionalmente e metodologias acordadas.

O Brasil é o maior país da região, e também o país onde há o maior número de usuários de internet na América do Sul, posto isso, é o único Estado da região que configura entre o top 10 de países que mais realizam e/ou recebem ciberataques a nível mundial. De acordo com o Relatório de Ameaças à Segurança na Internet de 2019, produzido pela Symantec, o Brasil configurou a terceira posição entre os países que mais realizaram ciberataques no ano de 2018 (9,8% do total mundial), ficando atrás apenas de China (24%) e Estados Unidos (10.1%). É necessário frisar, mais uma vez, que estes ciberataques podem ter sido realizados por qualquer grupo, instituição ou indivíduo em território brasileiro, não é necessário nenhum vínculo com o Estado brasileiro para ser categorizado com um ataque advindo do Brasil.

A partir da securitização e fronteirização do espaço cibernético, como apontam Demchak e Dombrowski (2011), os Estados passam a perceber a necessidade de estabelecer regulamentações e legislações acerca do ciberespaço, bem como comandos de Defesa Cibernética para garantir a soberania de seus Estados e a

segurança de sua população, posto isso, em seguida será exposto o que vem sendo desenvolvido a respeito desta temática por Argentina, Brasil e Uruguai, para que, no próximo capítulo seja possível realizar uma análise comparativa entre os entendimentos dos países assim como serão analisados os órgãos responsáveis em lidar com as questões de defesa e segurança cibernética em cada um dos três países, como por exemplo o Comando de Defesa Cibernética brasileiro (ComDCiber).

1.3.1 Argentina

Entre as principais legislações envolvendo questões cibernéticas propostas pelo Estado argentino está a Lei 26.388, denominada de Delitos Informáticos (2008). A Lei 26.388 “apresenta uma modificação/adição no Código Penal argentino, incorporando a este Código delitos cometidos por meios informáticos (delitos contra a integridade sexual, como pornografia infantil; violação de segredos e de privacidade; acesso ao sistema informático; acesso ao banco de dados; publicação de comunicação eletrônica; fraudes e danos informáticos)” (ARGENTINA, 2008).

A Argentina também possui a Lei 25.520, intitulada como Lei de Inteligência Nacional, do ano de 2001, que define em seu artigo segundo cinco pontos regulados pela mesma, são eles:

Quadro 1 – Aspectos Regulados pela Lei de Inteligência Nacional Argentina

Inteligência Nacional	É a atividade que consiste em obter, reunir, sistematizar e analisar as informações específicas referentes aos fatos, ameaças, riscos e conflitos que afetam a segurança nacional e externa da nação.
Contrainteligência	É a atividade do campo de inteligência que é realizada com o objetivo de evitar atividades de inteligência de atores que representam ameaças ou riscos à segurança do Estado Nacional argentino.

Inteligência Criminal	Faz parte da Inteligência referente às atividades criminosas específicas que, por sua natureza, magnitude, consequências previsíveis, perigo ou modalidades, afetam a liberdade, a vida, o patrimônio dos habitantes, seus direitos e garantias e as instituições do sistema representativo, republicano e federal estabelecido pela Constituição Nacional.
Inteligência Estratégica Militar	Faz parte da Inteligência referente ao conhecimento das capacidades e fraquezas do potencial militar dos países que interessam do ponto de vista da Defesa nacional, bem como do ambiente geográfico das áreas operacionais estratégicas determinadas pelo planejamento estratégico militar.
Sistema de Inteligência Nacional	É o conjunto de relações funcionais das agências de inteligência do Estado Nacional, dirigido pela Secretaria de Inteligência, a fim de contribuir para a tomada de decisões em questões de segurança externa e interna da Nação.

Fonte: ARGENTINA. Ley 25.520. 3 dez. 2001. Tradução própria.

A partir de análise da Lei 25.520, referente à inteligência nacional, é possível inferir a preocupação do Estado argentino em estabelecer meios para se proteger no espaço cibernético datando do começo do século XXI, uma vez que o país define e regulamenta estes cinco pontos supracitados com o intuito de defender a nação.

1.3.2 Brasil

A Política Nacional de Defesa (PND) é o documento de mais alto nível voltado para o planejamento de Defesa, tendo prioritariamente o foco contra ameaças externas. De acordo com o Ministério da Defesa (2012), a Política Nacional de Defesa “estabelece objetivos e diretrizes para o preparo e o emprego da capacitação nacional, com o envolvimento dos setores militar e civil, em todas as esferas do Poder Nacional.”

Já a Estratégia de Defesa Nacional (END) foi desenvolvida para atender às necessidades dos comandos militares, de maneira a reorganizar a indústria de defesa para que as tecnologias mais avançadas estejam sob domínio nacional, este documento também estabelece quais diretrizes são adequadas para a melhor preparação e capacitação das três Forças (Força Aérea, Exército e Marinha), de maneira a garantir a segurança do país tanto em tempos de paz como em tempos de crise (MD, 2012). De acordo com o Ministério da Defesa:

> O documento institui ações estratégicas de médio e longo prazo e objetiva a modernização da estrutura nacional de defesa. Também trata das questões político-institucionais que garantam os meios para fazer com que o governo e sociedade se engajem decisivamente na “grande estratégia” de segurança da nação (MD, 2012).

Entre todos os documentos da defesa brasileira o Livro Branco de Defesa Nacional (LBDN) é considerado o mais completo e abrangente a respeito das atividades de Defesa brasileiras. O objetivo do Livro Branco é esclarecer para com a sociedade brasileira e também à comunidade internacional, quais são as políticas e ações que norteiam os procedimentos de segurança e proteção da soberania brasileira. Um ponto bastante importante a ser levantado quanto ao Livro Branco de Defesa Nacional é que ele é elaborado pelo Ministério da Defesa, entretanto, por meio de audiências públicas, é aberto espaço para que a sociedade civil, o setor empresarial e a academia possam fazer possíveis contribuições para a elaboração de políticas acerca das temáticas de Defesa nacional, que podem ou não ser acatadas, mas que é extremamente importante para que a população brasileira tome conhecimento maior a respeito de temas militares e de Defesa e também para que o engajamento da sociedade brasileira nessa temática tão delicada seja cada vez maior nestas discussões que afetam a Nação como um todo (MD, 2012). O Ministério da Defesa ainda estabelece que o LBDN:

> Além de aportar transparência quanto à atuação das Forças Armadas, prestando contas sobre a adequação da estrutura de defesa disponível no país, serve de instrumento para estimular o debate sobre esse tema no âmbito do Congresso Nacional, da burocracia federal, da Academia e da sociedade em geral.
> Para fora do país, tem o objetivo de compartilhar as motivações e finalidades do instrumento militar junto à comunidade internacional para, assim, constituir mecanismo de construção de confiança mútua entre o Brasil e as nações amigas, especialmente as vizinhas (MD, 2012).

Diante disso, o Ministério da Defesa (2012) frisa que o LBDN é um meio de fortalecer a cooperação, principalmente entre os países da América do Sul, tendo em vista que o documento estimula a organização de uma comunidade de paz e segurança no entorno estratégico do Brasil, frisando a opção por soluções pacíficas e eliminando a possibilidade de conflitos na região.

Assim como o Estado argentino possui a Lei de Inteligência Nacional, o Brasil possui a Política Nacional de Inteligência (PNI), de maneira a "definir os parâmetros e limites de atuação da atividade de Inteligência e de seus executores e estabelece seus pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (SISBIN)" (ABIN, 2016). O documento define os termos da seguinte forma:

Quadro 2 – Definições segundo a Política Nacional de Inteligência Brasileira

Inteligência	Atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado.
Contrainteligência	Atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado.

Fonte: BRASIL. Política Nacional de Inteligência. 2016

1.3.3 Uruguai

O Uruguai possui dois decretos e uma lei que envolvem, principalmente, questões de segurança da informação, são eles: o Decreto Nº 451/009, o Decreto Nº 92/014 e a Lei Nº 18331. O Decreto Nº 451/009 prevê em seu artigo primeiro que "a Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), por meio do Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), protegerá os sistemas de computadores que suportam ativos de informações críticas do Estado, assim como os sistemas que os cercam" (URUGUAI, 2009).

O Decreto N° 92/014, de 2014, é intitulado Política de Segurança da Informação para Organizações da Administração Pública e tem como objetivo desenvolver, implementar, manter e melhorar continuamente o sistema de gerenciamento de segurança da informação uruguaio (URUGUAI, 2014). Por fim, a Lei Nº 18331 diz respeito aos direitos à proteção de dados que é inerente a todos os cidadãos uruguaios, respaldado pela Constituição uruguaia no Artigo 72.

1.4 CONSIDERAÇÕES FINAIS

Por fim, neste capítulo foram trabalhados casos notórios de ciberataques, como o Stuxnet no Irã que prejudicou o projeto nuclear do país de maneira significativa, o que serviu como um marco para os estudos de segurança e defesa cibernética, uma vez que, a partir do caso Stuxnet, os Estados perceberam a necessidade de investir no setor cibernético de maneira a garantir a segurança de suas infraestruturas críticas bem como sua soberania estatal e a segurança de sua população, assim como foram trabalhadas as definições de termos envolvendo questões cibernéticas para os três países em análise como Defesa Cibernética e Segurança Cibernética e, por fim, foi trabalhada a regulamentação do espaço cibernético que está sendo feita por Argentina, Brasil e Uruguai, para que, no próximo capítulo, seja possível colocar em comparação os entendimentos dos três países acerca destas questões cibernéticas e, também, seja possível analisar quais são os órgãos - em cada país - responsáveis por lidar com defesa e segurança cibernética.

2 ANÁLISE DA CIBERDEFESA E CIBERSEGURANÇA EM ARGENTINA, BRASIL E URUGUAI E ESPECIFIDADES DOS ORGANISMOS RESPOSÁVEIS PELA ÁREA

A partir do trabalho realizado no capítulo anterior, no qual foram trabalhados alguns casos específicos sobre ataques cibernéticos e também expostos alguns conceitos centrais acerca da temática de defesa e segurança cibernética, além de regulações que vem sendo desenvolvidas neste setor pelos países em análise, no presente capítulo serão trabalhados e aprofundados, comparativamente, os entendimentos de Argentina, Brasil e Uruguai acerca de Defesa e Segurança cibernética a partir de documentos oficiais dos Estados, como a Direção Nacional de Infraestruturas Críticas de Informação e de Cibersegurança da Argentina, do Comando Conjunto de Ciberdefesa argentino (CCCD), da Doutrina Militar feita no âmbito do Ministério da Defesa brasileiro e de palestras de oficiais das Forças Armadas de Argentina e Brasil que ocorreram em julho de 2019 no Rio de Janeiro, durante o XXI Ciclo de Estudos Estratégicos, do qual tive a oportunidade de participar. Para entender a ciberdefesa e cibersegurança uruguaias, foi utilizado o livro Segurança Nacional: Situação da ciberdefesa. Neste capítulo também será trabalhada a definição de outros termos da área, como segurança da informação e o próprio conceito de ciberespaço, bem como as diferentes abordagens acerca do mesmo.

Posteriormente, serão explorados os organismos responsáveis por questões de ciberdefesa e cibersegurança nos três países, como os Comandos Cibernéticos de Argentina e Brasil e para a análise específica do Uruguai serão utilizadas informações da Agência de Governo Eletrônico e Sociedade da Informação (AGESIC), do Centro Nacional de Respostas a Incidentes de Segurança Informática (CERTuy) e do Centro de Resposta a Incidentes de Segurança Cibernética do Ministério da Defesa uruguaio (DCSIRT).

2.1 ABORDAGENS SOBRE O CIBERESPAÇO

O ciberespaço, especialmente a partir do século XXI, adquire grande relevância no cenário internacional, passando a ser interpretado por diversos autores - e também por Estados - como um quinto domínio, assim como o ar, espaço exterior, o mar e a terra. Posto isso, uma vez que o ciberespaço pode ser visto como um novo domínio,

é possível inferir que os Estados irão, assim como o fazem nos outros domínios, estar presentes militarmente. De acordo com o Gen. Larry Welch da Força Áerea dos Estados Unidos (2011), os objetivos militares essenciais no ciberespaço são bastante parecidos com os objetivos das Forças Armadas nos outros quatro domínios, sendo estes: a liberdade para desenhar ações militares desejáveis e a habilidade de negar essa liberdade à adversários em momentos e locais de escolha do País em questão.

A partir da visão trazida pelo general Larry Welch se torna clara a intenção de utilização do ciberespaço por alguns Estados, também, como meio para ações militarizadas e, possivelmente, torna possível o desencadeamento de uma ciberguerra. É importante destacar que o ciberespaço perpassa todos os outros quatro domínios, e que as operações nestes domínios estão cada vez mais dependentes do espaço cibernético, posto isso, é possível desencadear resultados nos domínios ar, espaço exterior, mar ou terra por meio do ciberespaço, como por exemplo tornar um satélite inoperante ou até mesmo corromper os sistemas de instalações petrolíferas em alto mar de maneira a interromper o seu funcionamento.

O Manual de Tallinn, desenvolvido no âmbito da OTAN, é um dos principais referenciais nos estudos acerca de conflitos no espaço cibernético. Neste documento, o ciberespaço é definido como:

> o ambiente formado por componentes físicos e não físicos, caracterizado pelo uso de computadores e pelo espectro eletromagnético para armazenar, modificar e trocar dados usando redes de computadores (OTAN, 2013, p.211, tradução própria).

Uma percepção interessante, a partir da análise do conceito trazido pela OTAN, é a questão de componentes físicos fazerem parte do ciberespaço, é necessário percebermos que existe uma interligação entre componentes físicos e não físicos, que é o que possibilita o funcionamento do espaço cibernético. Novamente, é de suma importância lembrar que, diferentemente dos outros domínios, o ciberespaço foi e continua sendo constantemente construído por seres humanos.

O conceito elaborado no Manual de Tallinn é bastante parecido com o conceito de ciberespaço feito por Kuehl (2009), o qual entende o ciberespaço como:

> um domínio global dentro do ambiente de informações, cujo caráter distinto e único é enquadrado pelo uso de eletrônicos e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas, usando tecnologias de comunicação e de informação (KUEHL, 2009, p.2, tradução própria).

Como apontam Maziero e Ayres Pinto (2019), a definição de Kuehl possui pontos merecedores de destaque. Primeiramente, quanto ao nível operacional, é possível inferir que por meio da tecnologia disponível no ciberespaço, se torna viável que atores criem efeitos que não se limitam ao mesmo, podendo estes adentrar os outros domínios. Em segundo lugar, uma diferenciação dos outros domínios que é perceptível nesta conceituação é a possibilidade de, por meios eletrônicos, não apenas fazer parte do ciberespaço, mas também se possibilita criá-lo. Por fim, um ponto extremamente relevante que é trazido por Kuehl em sua definição do ciberespaço, é a questão do processo de troca de informações, que ocorre por meio de redes que são interdependentes e interconectadas, processo que se dá a partir da utilização de tecnologias de comunicação e de informação.

De acordo com Ventre (2011), o ciberespaço é composto por três camadas: a camada inferior, que é material e diz respeito à infraestrutura (hardware); a camada do meio, que é a camada dos sistemas de informação e do processamento de dados (software); e, por último, da camada superior (cognitiva) que diz respeito ao caráter humano do ciberespaço. Como apontam Guedes et al (2017, p.22), a conceituação de Ventre traz o caráter humano pois, sem ele, não haveria ciberespaço. Uma vez que, diferentemente dos outros domínios, o ciberespaço não existiria caso os seres humanos não o tivessem produzido.

Como foi exposto no capítulo anterior, os diferentes Estados conceituam os termos a respeito do ciberespaço de acordo com os seus entendimentos e suas necessidades internas. Diferentemente de Brasil e Uruguai, que apesar de discorrerem bastante sobre o espaço cibernético e suas utilizações em seus documentos oficiais de Defesa não possuem uma definição própria do termo espaço cibernético, a Argentina traz em seu Libro Blanco de la Defensa (2015) a seguinte conceituação:

> O espaço cibernético não é um âmbito militar operacional específico, mas sim uma dimensão operacional transversal aos ambientes operacionais tradicionais - ar, mar, terra e espaço exterior - na qual podem acontecer operações de natureza militar, o que requer um planejamento militar conjunto (ARGENTINA, 2015, tradução própria).

A partir da definição elaborada pela Argentina, é possível percebermos que, ainda que o país não enxergue o espaço cibernético como um âmbito militar operacional específico, ele prevê que neste espaço podem ocorrer operações de

natureza militar. O Estado argentino também destaca o fato de o ciberespaço ser transversal a todos os outros domínios - ar, mar, terra e espaço exterior - o que, em última instância, possibilita a atuação estatal militarizada nestes quatro domínios por meio do ciberespaço.

O Brasil ainda não apresentou em seus documentos oficiais de defesa uma definição de ciberespaço feita pelo país. Como tratado no capítulo anterior, o país utiliza em seu Livro Verde de Defesa Cibernética a definição feita por Levy, entretanto, no mesmo livro, quando o Estado discorre sobre cibersegurança, aponta que “chama atenção que o chamado espaço cibernético, não tem suas fronteiras ainda claramente definidas, impacta o dia a dia de todos os dirigentes governamentais, de empreendimentos e dos próprios cidadãos” (BRASIL, p.13, 2010). A partir disso, fica claro que o governo brasileiro está, de fato, preocupado com a fronteirização do espaço cibernético, o que pode servir para amenizar ameaças e/ou ataques no ciberespaço. Ademais, o Estado brasileiro ao caracterizar a falta de fronteiras definidas, também se demonstra preocupado com ameaças advindas do ciberespaço que tenham como alvo seja o governo, seja o setor privado ou a sociedade brasileira como um todo (BRASIL, 2010, p.13).

2.2 ANÁLISE COMPARATIVA SOBRE DEFESA E SEGURANÇA CIBERNÉTICA

É importante se ter em mente que não existem conceitos únicos definidos acerca do que é cibersegurança e o que é ciberdefesa, os termos podem ter significados distintos de acordo com o que àquele que os define deseja abarcar. Diante disso, uma possível conceituação trazida por Galinec et al. (2017), é a de que a defesa cibernética foca na prevenção, na detecção rápida e no fornecimento de respostas que sejam efetivas a ataques ou ameaças, de forma a evitar que qualquer infraestrutura ou informação venha a ser violada. Ademais, os autores destacam que com o aumento tanto em números de ataques como na complexidade dos mesmos, a defesa cibernética se faz essencial para as entidades, de forma a proteger informações confidenciais e ativos estratégicos.

A partir dessa definição, se pode perceber um caráter que volta a defesa cibernética mais para o lado estatal (assim como a defesa nacional), uma vez que esta se preocupa principalmente em proteger as infraestruturas críticas dos Estados de possíveis ameaças ou ataques, bem como proteger informações confidenciais, ou

seja, informações de um Estado - ou de seus governantes - que, se trazidas a público, podem causar problemas para o país em questão. A visão elucidada por Goldsmith (2010), demonstra claramente a crescente militarização do ciberespaço, o autor indica que a melhor defesa cibernética para proteger sistemas críticos computadorizados pode, na verdade, ser uma boa ofensa, ou seja, sua capacidade de atacar.

Ainda sobre ofensa cibernética, inúmeros autores a consideram mais efetiva do que a própria defesa cibernética, uma vez que realizar ofensas ainda é relativamente fácil e possui baixo custo - importante retomar aqui o argumento de Demchack e Dombrowski (2011) de que, a partir da fronteirização do espaço cibernético por parte dos Estados se tornaria mais difícil adentrar o ciberespaço de uma nação, uma vez que os custos para realizar tais ações seriam mais altos e os atacantes precisariam deslocar esforços maiores - além do enorme dano que é possível de se desencadear a partir de atos ofensivos por meio do ciberespaço, tanto mirando em alvos estratégicos de Estados como na sociedade. Lieber (2014), ainda destaca que ataques - ou seja, a ofensa cibernética -, precisam ter como alvo apenas alguma vulnerabilidade para obter sucesso, ao passo que a defesa cibernética envolve inúmeros fatores de segurança para evitar que o atacante obtenha informações secretas e/ou explore os sistemas do atacado.

Gonzales e Portela (2018) utilizam a definição de segurança cibernética elaborada por Medeiros Filho (2014), na qual a segurança cibernética é associada a dimensão da segurança pública. Para Medeiros Filho (2014), ao passo que defesa cibernética é relacionada com noções ligadas à guerra, a segurança cibernética é relacionada com questões de ilegalidade. Ou seja, a partir das conceituações feitas pelo autor, as definições de defesa e segurança cibernética estão diretamente ligadas ao que está sendo enfrentado. Portanto, uma das formas de enxergar a ciberdefesa estaria diretamente relacionada a ações ofensivas (de guerra) contra o Estado, enquanto a cibersegurança serviria para lidar com ilegalidades no ciberespaço, como por exemplo o roubo/sequestro de dados.

Como tratado no capítulo anterior, existem similaridades e distinções quanto ao que cada um dos três Estados em análise - Argentina, Brasil e Uruguai - compreendem por defesa e segurança cibernética. Diante disso, esta subseção busca analisar, comparativamente, as definições trazidas por estes países em seus documentos oficiais de defesa. Abaixo, foi elaborada uma tabela para melhor

esclarecer as definições de defesa e segurança cibernética da Argentina, Brasil e Uruguai.

Quadro 3 – Defesa e Segurança Cibernética para a Argentina, Brasil e Uruguai

	ARGENTINA	**BRASIL**	**URUGUAI**
Defesa Cibernética	Medidas e ações, desenvolvidas pelo Estamento Militar, com a finalidade de resguardar as IFCs.	Conjunto de ações ofensivas, defensivas e exploratórias com a finalidade de proteger os sistemas de informação de interesse da Defesa, obter dados para produzir inteligência e comprometer o inimigo.	Conjunto de ações de defesa ativa, passiva, pró-ativa, preventiva e reativa para garantir o uso adequado do ciberespaço e negá-lo ao inimigo ou a outras inteligências opostas.
Segurança Cibernética	Situação de segurança das IFCs, liberdade de funcionamento da IFC em questão.	Capacidade de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas IFCs.	Conjunto de ações preventivas que visam garantir o uso de redes próprias e negá-lo a terceiros.

Fonte: Elaboração Própria com base na Doutrina Militar de Defesa Cibernética (MD, 2014), no website do CCCD (ARGENTINA, 2019) e do livro Situación de La Ciberdefensa (URUGUAI, 2017).

A partir da análise das tabelas acima, formuladas a partir da palestra de major argentino no Rio de Janeiro (que teve como base os entendimentos do CCCD)[10] e documentos do Ministério da Defesa brasileiro, é possível inferir que os entendimentos

[10] "Comando Conjunto de Ciberdefensa - Estado Mayor ...." Disponível em: <http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx>. Acessado em 22 nov.. 2019.

dos três Estados em matéria de Defesa Cibernética são bastante similares. Para a Argentina, o termo diz respeito às atividades desenvolvidas pelo setor militar que possuam o intuito de resguardar a segurança cibernética das infraestruturas críticas do sistema nacional argentino assim como das infraestruturas necessárias para preservar o mesmo, independente da origem da agressão, ou seja, essa instância poderá lidar com atores estatais ou não-estatais advindos tanto de território argentino como de outras partes do globo.

O Brasil traz uma definição mais estreita do termo Defesa Cibernética. De acordo com o MD (2014), o termo significa um conjunto de ações que podem ser ofensivas, defensivas e/ou exploratórias, realizadas no ciberespaço com um planejamento nacional de nível estratégico que é coordenado pelo Ministério da Defesa a fim de proteger os sistemas de informação de interesse da Defesa brasileira, obter dados que sirvam para produzir inteligência nacional e, por fim, comprometer os sistemas do oponente. Posto isso, é possível compreender que Argentina e Brasil preveem que as instâncias responsáveis por lidar com a Defesa Cibernética de seus respectivos países poderão realizar ações ofensivas contra àquele que os atacou, o que não fica claro é se os países responderão por meio do espaço cibernético ou se ataques físicos poderão ser utilizados como resposta à ataques advindos do ciberespaço.

O caso uruguaio é bastante distinto, pois, diferentemente de Argentina e Brasil, que especificam os termos de defesa cibernética e segurança cibernética elaborados pelos seus respectivos órgãos responsáveis, o Uruguai não o faz. Na verdade, em Segurança Nacional: Situação da ciberdefesa (URUGUAI, 2017)[11], o Uruguai traz as definições de ciberdefesa e cibersegurança elaboradas pelo Conselho Argentino de Relações Internacionais, sendo a defesa cibernética caracterizada como um “conjunto de ações de defesa ativa, passiva, pró-ativa, preventiva e reativa para garantir o uso adequado do ciberespaço e negá-lo ao inimigo ou a outras inteligências opostas” (CARI, p.2, 2013)[12]. Em contrapartida, a definição respectiva a cibersegurança diz que esta é um “conjunto de ações preventivas que visam garantir o uso de redes próprias

[11] "situación de la ciberdefensa - Centro Militar." Disponívem em: <http://www.centromilitar.org.uy/Servicios/RevistaElSoldado/RevistaElSoldado192.pdf>. Acessado em 22 nov.. 2019.
[12] "Ciberdefensa-Ciberseguridad Riesgos y Amenazas." Disponível em: <http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf>. Acessado em 22 nov.. 2019.

e negá-lo a terceiros” (CARI, p.2, 2013). Posto isso, é possível identificarmos que o Uruguai entende a ciberdefesa e cibersegurança de maneira parecida aos entendimentos de Argentina e Brasil, ao passo que enquanto a defesa cibernética está diretamente ligada a ações de defesa quanto à utilização de seu ciberespaço por inimigos bem como a elaboração de respostas para lidar com possíveis invasões, a segurança cibernética é entendida como as ações que servirão para prevenir possíveis invasões de ocorrer.

2.3 ÓRGÃOS RESPONSÁVEIS POR DEFESA E SEGURANÇA CIBERNÉTICA POR ESTADO

Nesta seção serão trabalhados quais são os organismos responsáveis por questões de defesa e segurança cibernética em cada um dos Estados em análise - Argentina, Brasil e Uruguai -, de forma a buscar compreender se estes setores estão vinculados às Forças Armadas dos respectivos países ou a outros setores governamentais.

2.3.1 Argentina

O caso da Argentina é bastante significativo na América do Sul, o país é o único país no qual as Forças Armadas são, constitucionalmente, encarregadas de lidar exclusivamente com ameaças estrangeiras. Isso decorre, substancialmente, como um reflexo da ditadura militar no país, o que levou a essa definição, não permitindo que as Forças Armadas argentinas atuassem em questões de segurança pública dentro do país.

Posto isso, como visto anteriormente, a dimensão da cibersegurança está mais voltada para o âmbito de segurança pública, uma vez que está diretamente relacionada a proteção da sociedade civil como um todo no ciberespaço. Diante disso, se busca entender como a Argentina lida com a questão de segurança cibernética e qual é o organismo encarregado de lidar com isso, uma vez que não serão as Forças Armadas.

De acordo com a OEA, a Argentina é notável por ter sido um dos primeiros países a estabelecer um *Computer Security Incident Response Team* (CSIRTs) no ano de 1994, já demonstrando, então, sua preocupação com o desenvolvimento das

tecnologias da informação e com sua segurança no ciberespaço. Desde 2011, o organismo funciona no âmbito do ICIC, que é o Programa Nacional de Proteção de Infraestruturas Críticas e Informação e Cibersegurança (ICIC-CERT). O CERT argentino é responsável pelo registro de eventos que envolvam cibersegurança e ameaças/agressões, assim como o CERT.br e o CERT.uy.

No ano de 2016, por meio do Ministério da Modernização criado no governo Macri, foi aprovada a estrutura organizacional que estabelece as funções da Direção Nacional de Infraestruturas Críticas de Informação e de Cibersegurança, tendo como responsabilidade principal “auxiliar em todos os aspectos relacionados à cibersegurança e a proteção de infraestruturas críticas, incluindo a geração de recursos de detecção, defesa, resposta e recuperação em caso de incidentes do setor público nacional” (ARGENTINA, 2016). A partir da criação dessa Direção e da definição de sua responsabilidade principal por meio desta, se torna clara a preocupação do Estado argentino quanto a segurança pública nacional no ciberespaço. Um ponto merecedor de destaque é a recuperação em caso de acidentes do setor público nacional, pois isso demonstra a preocupação do país com o desenvolvimento de sua resiliência no ciberespaço, ou seja, a sua capacidade de recuperar o controle de seus sistemas de informação e cibersegurança o mais rápido possível quando estes sofrerem ataques, evitando que grandes danos ocorram, isso é importante pois a Argentina assume que nem sempre será possível evitar que o país seja atacado (e de fato, muitas vezes não é possível evitar o ataque), contudo, o país busca desenvolver meios para, quando o atacante obter sucesso, o país possa retomar esse controle o quanto antes.

Dentro da estrutura organizacional também são estabelecidas quatorze ações que serão realizadas pela Direção Nacional de Infraestruturas Críticas de Informação e de Cibersegurança, sendo elas as seguintes:

> 1. Auxiliar e supervisionar tudo relacionado à segurança e privacidade de informações digitalizadas e eletrônicas no âmbito de sua competência;
>
> 2. Desenvolver e propor normas e padrões destinados a elevar os limites de segurança de recursos e sistemas relacionados a tecnologias de computador no âmbito de sua competência
>
> 3. Propor e desenhar a política de segurança do modelo de informação;

> 4. Desenvolver, em coordenação com o setor privado, políticas para proteger a segurança digital com atualização constante, com foco específico nas infraestruturas críticas;
>
> 5. Estabelecer prioridades e planos estratégicos para lidar com a cibersegurança;
>
> 6. Investigar e incorporar novas tecnologias e ferramentas no campo da segurança de computadores para minimizar vulnerabilidades da infraestrutura digital do setor público nacional;
>
> 7. Monitorar os serviços que o Setor Público Nacional fornece por meio da rede da Internet e os que são identificados como infraestrutura crítica para a prevenção de possíveis falhas de segurança;
>
> 8. Alerta em casos de tentativas de violação da infraestrutura crítica, bem como das vulnerabilidades encontradas;
>
> 9. Compreender o planejamento e a implementação de exercícios de resposta a incidentes cibernéticos do setor público nacional;
>
> 10. Aconselhar aos diversos organismos sobre ferramentas, técnicas de proteção e defesa de seus sistemas de informação;
>
> 11. Aconselhar, tecnicamente, em caso de incidentes de segurança em sistemas de computadores relatados pelas agências do setor público nacional;
>
> 12. Coordenar ações entre as unidades de administração de redes de computadores do Setor Público Nacional, para prevenção, detecção, gerenciamento e coleta de informações sobre incidentes de segurança;
>
> 13. Coordenar as ações da equipe de resposta a emergências de computadores em nível nacional, gerenciando todas as informações sobre os relatórios de incidentes de segurança no setor público nacional e canalizando suas possíveis soluções de maneira organizada e unificada;
>
> 14. Atuar como repositório de todas as informações sobre incidentes de segurança, ferramentas, técnicas de proteção e defesa, padrões e boas práticas (ARGENTINA, 2016, tradução própria).

Entre as quatorze ações definidas em questões de cibersegurança pela Argentina, algumas chamam bastante a atenção. A primeira ação, por exemplo, diz respeito a supervisão de ‘tudo relacionado à segurança e privacidade de informações digitalizadas e eletrônicas no âmbito de sua competência’, entretanto, em nenhum momento o documento deixa claro qual é a sua competência, o que pode infringir em problemas de abuso da privacidade de sua própria população, por não haver um direcionamento claro do que é ou não permitido ser supervisionado. A quarta ação também chama bastante a atenção, pois trata a respeito da cooperação com atores não-estatais para o desenvolvimento de segurança cibernética. Nesta ação, o governo argentino estabelece que deve ser desenvolvido, em coordenação com o setor

privado, políticas que sirvam para proteger a segurança digital, focando nas infraestruturas críticas, foco este que é comum aos três países analisados neste trabalho. Além disso, algumas ações estabelecidas pela Argentina também dizendo respeito ao constante aprimoramento da sua segurança cibernética, o aconselhamento aos diversos organismos da nação (tanto públicos como privados) de forma que estes possam obter o conhecimento necessário para que sua cibersegurança seja boa, a coordenação das cabíveis respostas aos incidentes ocorridos, entre outros. Contudo, uma crítica que deve ser feita é que, apesar de serem elencadas essas quatorze importantes ações, em nenhum momento o país busca esclarecer em seus documentos como essas ações serão, de fato, efetivadas. Por exemplo quando se fala das respostas aos ataques, não é elaborado que tipo de respostas serão dadas.

Em 2014, o Ministério da Defesa da República Argentina, por meio da Resolução Ministerial nº 343, criou o Comando Conjunto de Ciberdefesa (CCCD), com dependência organizacional, funcional e operacional do Estado-Maior Conjunto das Forças Armadas.

Entre as funções listadas para o CCCD, está a coordenação de suas ações com todos os Centros de Ciberdefesa das Forças Armadas argentinas, bem como o estabelecimento de critérios orientadores, ao nível do Estamento Militar, para determinar quais infraestruturas críticas devem ser protegidas; o CCCD também deve participar da elaboração, revisão e experimentação da Doutrina de Ciberdefesa. Além disso, quando a pedido do Ministério da Defesa, o CCCD deve atuar em apoio a outras organizações, assim como na conscientização das Forças Armadas em matéria de ciberdefesa e, também, na determinação e supervisão de padrões de segurança e certificação de protocolos que estejam relacionados às Forças Armadas (ARGENTINA, 2019). Assim como no caso da Direção Nacional de Infraestruturas Críticas de Informação e de Cibersegurança, não existem especificações divulgadas por parte do CCCD a respeito de quais serão as infraestruturas críticas a serem protegidas (apesar do órgão explicitar que essa determinação existe), por exemplo.

A Argentina também possui uma Diretoria de Ciberdefesa do Exército Argentino, a qual tem como função:

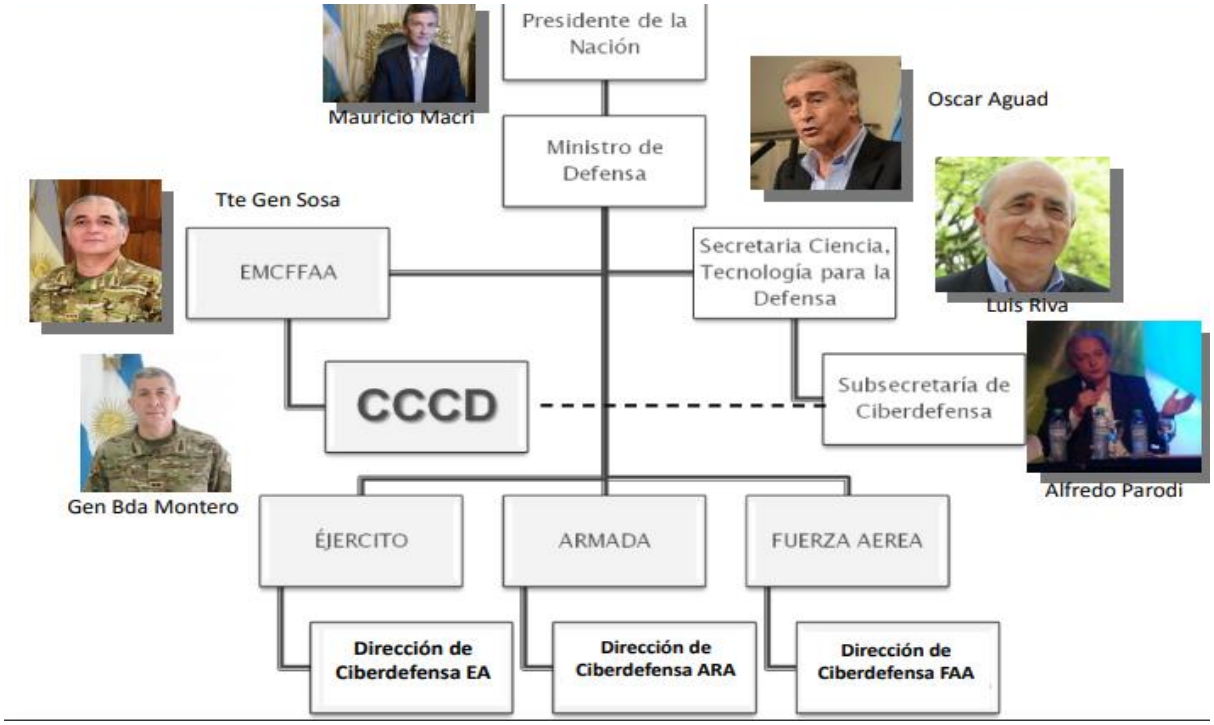
> Executar as ações necessárias para prevenir e preservar, a todo momento, o uso eficiente dos recursos, das redes, sistemas de informação ou outros a fim de assegurar o livre acesso ao espaço cibernético de interesse militar e

> oferecer uma resposta adequada ante ameaças e agressões que possam afetar a Infraestrutura Crítica da Força, a fim de contribuir sistematicamente com a missão do CCCD (GÓMEZ, 2019).

A partir da Decisão Administrativa 15/2015, foi criada a Direção Geral de Ciberdefesa, que entre suas missões intervir na orientação, direcionamento e na supervisão das ações de ciberdefesa executadas pelos militares, promover políticas de convocação, recrutamento, incentivo e treinamento de recursos humanos para defesa cibernética, com o objetivo de formar uma equipe adequada para lidar com a ciberdefesa argentina, além de ter como objetivo buscar cooperação e intercâmbio de informações com organizações públicas e privadas (CARI, 2015)[13]. Posto isso, é possível identificarmos que a Direção Geral de Ciberdefesa possui funções bastante relevantes, como por exemplo o recrutamento e treinamento de recursos humanos, fator central para consolidar uma defesa cibernética bem estruturada.

Abaixo, ilustração da organização do setor de Defesa Cibernética na Argentina

Figura 2 – Organização do Setor de Defesa Cibernética na Argentina



Fonte: Palestra Políticas Públicas de Defesa Cibernética em perspectiva comparada de Mariano Oscar Gómez, Rio de Janeiro, julho de 2019.

[13] "/ CARI / - Consejo Argentino para las Relaciones Internacionales." Disponível em: <http://www.cari.org.ar/pdf/boletin61.pdf>. Acessado em 22 nov. 2019

2.3.2 Brasil

No Brasil, as ações operacionais de segurança cibernética são realizadas pelo Departamento de Segurança da Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional (DSI), da Presidência da República (PR), ou seja, a segurança cibernética está a cargo da Presidência da República. Em 2015, foi lançado pela então presidenta Dilma Rousseff, a Estratégia que guiaria a segurança cibernética no período de 2015-2018. A estratégia prevê o fortalecimento da política e do planejamento de segurança da informação e comunicações e de segurança cibernética na Administração Pública Federal, de forma a garantir e defender os interesses do Brasil e da sociedade brasileira, preservando a soberania nacional. Abaixo, os princípios norteadores da estratégia:

Figura 3 – Princípios Norteadores da Estratégia no Brasil

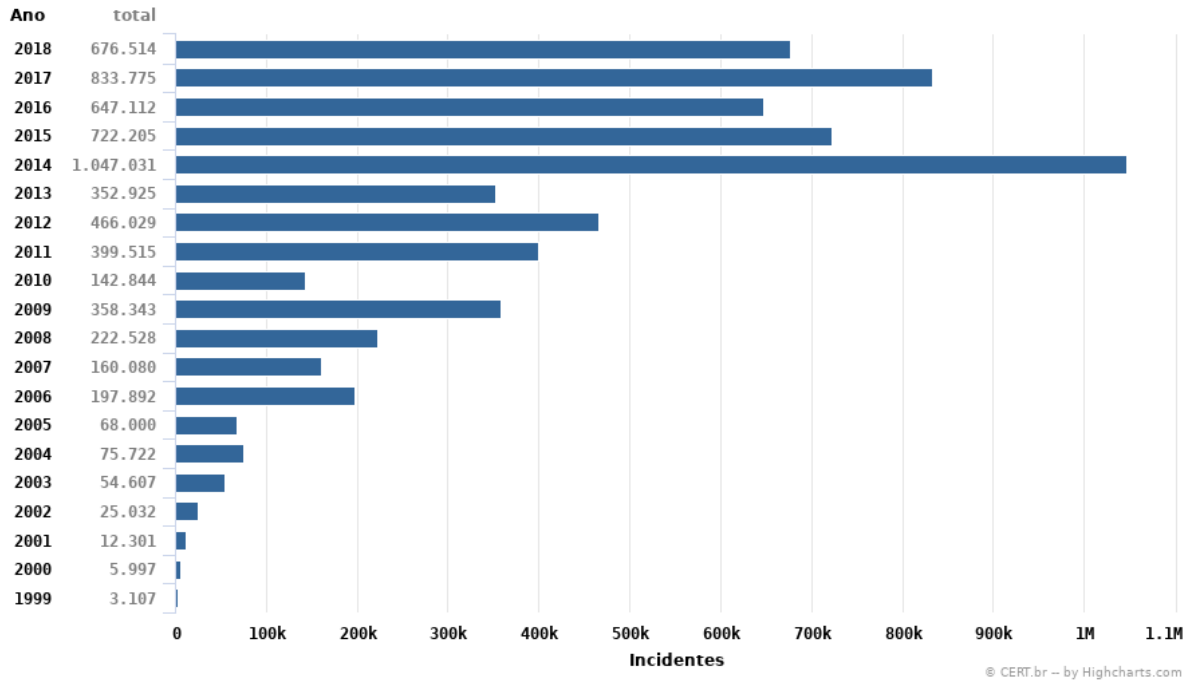
Órgão Central: contribuir com o estabelecimento de um órgão central e de um sistema nacional, objetivando a coordenação executiva, o acompanhamento e a avaliação da implantação e execução da Política Nacional de SIC e SegCiber.
Governança: contribuir com a definição de um modelo de governança sistêmica de SIC e de SegCiber, de amplo alcance e cobertura para uma conexão forte entre os múltiplos atores, em nível nacional.
Política Nacional: contribuir com a formulação da Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética.
Capacidade de posicionamento e de respostas da Nação: contribuir com a criação de uma robusta capacidade de posicionamento e de respostas da Nação frente às potenciais quebras de segurança e ameaças cibernéticas, fortalecendo a alocação de recursos financeiros, tecnológicos e humanos.
Comprometimento da Alta Administração: envolver a Alta Administração dos órgãos e entidades da Administração Pública Federal em relação às diretrizes e ações de SIC e de SegCiber no âmbito de suas atuações.
Marcos Legais: colaborar para o aprimoramento e atualização dos marcos legais em SIC e SegCiber.
Articulação e Parcerias: garantir que a SIC e a SegCiber estejam contempladas em termos, acordos, contratos e instrumentos firmados entre a APF e setores públicos ou privados, nacionais ou internacionais.
Soberania Nacional: reconhecer as áreas de SIC e de SegCiber como estratégicas para a soberania nacional, garantindo recursos contínuos e adequados.
Cooperação: promover a cooperação nacional e internacional, visando trocas de experiências e o fortalecimento dos temas de SIC e de SegCiber no âmbito da APF e com setor produtivo e academia.
Integração: fomentar e fortalecer ações conjuntas visando à integração entre as áreas de SIC e de SegCiber com outras áreas que atuam no espaço cibernético.
Resiliência: contribuir com o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas.

Fonte: BRASIL, 2015.

A partir dos princípios norteadores da estratégia, dois objetivos se destacam: os mesmos que se destacaram no caso argentino. Primeiro, assim como o primeiro país analisado, o Brasil também ressalta a importância de atores não-estatais no processo de desenvolvimento de segurança cibernética quando incentiva que se faça cooperação não somente com setores públicos e mas também privados e, o documento vai além disso: também incentiva a cooperação com a academia. Entretanto, apesar de ser necessário valorizar este discurso, é preciso salientar que, até o momento (2019), não há divulgação de parcerias entre o governo federal e a academia em questões que envolvam o desenvolvimento de segurança cibernética. Em segundo lugar, o governo também dá enfoque na questão da resiliência, de forma a garantir que, quando houver um ataque que afete as infraestruturas críticas nacionais, seja possível retomar o controle dos sistemas o quanto antes, evitando que grandes perdas sejam efetuadas (BRASIL, 2015). Resiliência é um ponto extremamente central ao se tratar de defesa e segurança cibernética, pois ao ser tratado pelos países, é admitido que nem sempre será possível evitar que ciberataques e invasões ocorram, entretanto o país se demonstra disposto a desenvolver meios para recuperar o controle de seus sistemas de forma a garantir que o mínimo de dano possível seja causado.

O caso brasileiro é bastante distinto: existem diversos CERTs no país. Como por exemplo o CERT-RS, CERT.Bahia, CSIRT BB, CSIRT TIM, entre outros, alguns são responsabilidade de órgãos governamentais e outros do setor privado ou até mesmo acadêmicos. O Brasil também possui o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), assim como o Uruguai possui o CERTuy e a Argentina o ICIC-CERT. Este organismo, no Brasil, possui uma base de dados extremamente importante datando a partir de 1999 a respeito da quantidade e dos tipos específicos de incidentes cibernéticos realizados no ciberespaço brasileiro. Abaixo, a quantidade de incidentes reportados ao CERT.br no período de 1999 a 2018:

Figura 4 – Incidentes cibernéticos reportados ao CERT.br no período de 1999 a 2018



FONTE: CERT.br

Diferentemente do caso uruguaio que será trabalhado posteriormente, o caso brasileiro é extremamente alarmante. O número de incidentes reportados cresceu muito ao longo dos anos, atingindo mais de um milhão de incidentes no ano de 2014 - apenas de incidentes reportados, o que indica que o número real pode ter sido ainda maior. Estes incidentes colocam em risco a segurança e a soberania do país e, devido a isso, o país percebe a necessidade de fortalecer seus organismos responsáveis por questões de segurança e defesa cibernética, como é o caso do ComDCiber, ativado em abril de 2016. Referente aos tipos de incidentes reportados ao CERT.br no ano de 2018, dois se destacam, são eles scan (58,77%) que o próprio organismo define como notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador e DoS (23,42%) definido como "notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede" (CERT.br, 2019).

O Brasil possui um comando cibernético militar especificamente para lidar com a defesa cibernética, chamado Comando de Defesa Cibernética (ComDCiber), o órgão tem como missão principal

> Planejar, orientar, coordenar, integrar e executar atividades relacionadas ao desenvolvimento e aplicação das capacidades cibernéticas, como órgão central e no âmbito do Sistema Militar de Defesa Cibernética, a fim de contribuir para o uso efetivo do espaço cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional (AMIN, 2019).

Tendo em vista a definição acima, a defesa cibernética brasileira, comandada pelo ComDCiber, tem como objetivo principal evitar que aqueles atacantes externos que tenham como intuito ferir os interesses da Defesa Nacional, sejam eles atores estatais ou não-estatais, adentrem o ciberespaço brasileiro e, quando não for possível evitar que estes atacantes não tenham sucesso, a defesa cibernética irá dificultar a entrada desses atores de maneira a organizar sua capacidade de resiliência, para que possa retomar o controle dos sistemas que, eventualmente, tenham sido atacados e/ou corrompidos.

Além disso, como foi exposto pelo comandante do ComDCiber, General Amin (2019), em palestra no Rio de Janeiro, o objetivo futuro do ComDCiber é de que o órgão consiga atingir sua capacidade operacional plena, atuando “como comando operacional conjunto, permanentemente ativado e com a capacidade de atuação interagências”. É importante destacar que nesta mesma palestra, o General salientou que o investimento anual atual em defesa cibernética é de cerca de R$7 milhões e que, para de fato atingir a sua capacidade operacional plena, o órgão precisaria de cerca de R$120 milhões anuais (AMIN, 2019).

No ano de 2018, o então comandante do ComDCiber, Gen. Okamura, quando questionado em entrevista explicou o funcionamento do Comando de Defesa Cibernético:

> é um Comando Operacional Conjunto dentro da estrutura regimental do Exército Brasileiro. Está organizado da seguinte maneira: Estado-Maior Conjunto, chefiado por um Contra-Almirante; Departamento de Gestão e Estratégia, chefiado por um Brigadeiro; e Centro de Defesa Cibernética, chefiado por um General de Brigada. O Comandante de Defesa Cibernética é um General de Divisão. O efetivo total, incluindo a Escola Nacional de Defesa Cibernética, deverá chegar a 300 militares, atuando nas atividades

> operacionais, doutrinárias, de ciência e tecnologia, de inteligência e de capacitação (OKAMURA, 2018).[14]

A partir da resposta do então comandante, uma informação de extrema relevância surge: o efetivo total do ComDCiber (incluindo os militares presentes na Escola Nacional de Defesa Cibernética, que foi inaugurada em 2019). Esse dado não se encontra disponível em nenhum site e/ou documento oficial de governo, mas o Gen. Okamura afirma que o efetivo do ComDCiber deve chegar em 300 militares, o que em primeira mão pode parecer pouco, mas é preciso levar em consideração que todos eles terão seu treinamento e capacitação focados especificamente para lidar com a defesa cibernética brasileira.

Já a respeito das contribuições realizadas pelo ComDCiber, o Gen. Okamura afirma que desde a sua criação tanto o Ministério da Defesa como as Forças Armadas passaram a possuir maior capacidade para atuar no ciberespaço. Além de destacar que a sua criação serviu também para aumentar as capacidades científico-tecnológicas e industriais brasileira, bem como aumentar a capacidade de dissuasão das Forças Armadas, colaborando para a transformação das Forças “da era industrial para a era do conhecimento” (OKAMURA, 2018).

2.3.3 Uruguai

No Uruguai se tem a Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), como responsável pela segurança da informação. A agência foi criada em 2005 (artigo 72 da Lei nº17.930) e seu funcionamento foi regulamentado no ano seguinte, 2006. A missão da AGESIC é liderar a estratégia de implementação de um Governo Eletrônico no país, com base em um Estado eficiente e centrado no cidadão, além de ter como objetivo impulsionar a sociedade da informação e do conhecimento como uma nova forma de cidadania, promovendo a inclusão e a apropriação por meio do bom uso da tecnologia da informação e das comunicações (LASSERE, 2016, p.271).

A definição trazida pela própria Agência em seu website é de que:

> a Agência para o Desenvolvimento do Governo Eletrônico visa garantir a melhoria dos serviços prestados aos cidadãos, utilizando as possibilidades oferecidas pelas tecnologias da informação e comunicação (TIC). Da mesma

[14] "General de Divisão Angelo Kawakami Okamura, comandante ...." 24 abr.. 2018, Disponível em: <https://www.defesaaereanaval.com.br/aviacao/general-de-divisao-angelo-kawakami-okamura-comandante-do-comdciber-fala-sobre-as-forcas-armadas-no-brazil-cyber-defense>. Acessado em 22 nov.. 2019.

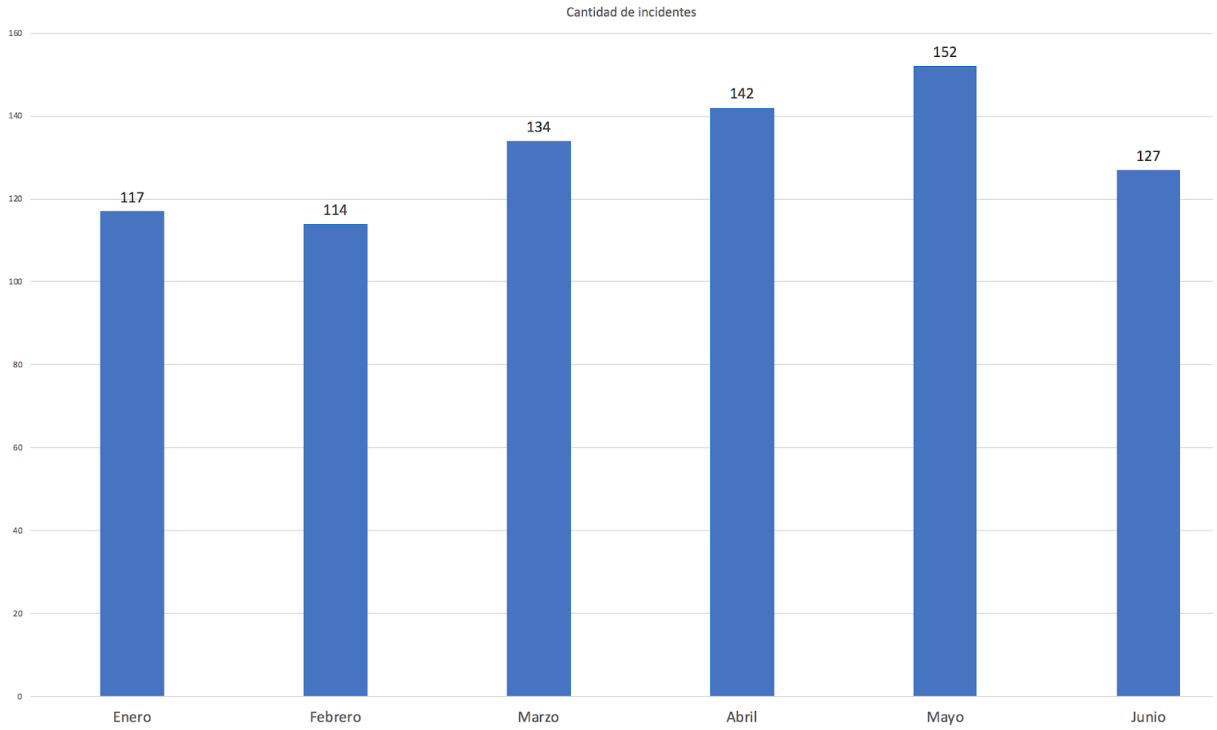
> forma, promoverá o desenvolvimento da Sociedade da Informação no Uruguai, com ênfase na inclusão da prática digital de seus habitantes e no fortalecimento das habilidades da sociedade no uso de tecnologias (AGESIC, 2006).

Diferentemente dos casos anteriores - Argentina e Brasil -, aqui não se percebe exatamente a questão da segurança cibernética, ou qualquer menção a proteção de infraestruturas críticas e/ou de proteção da sociedade, mas sim um incentivo para o aprendizado da população uruguaia de como se utilizar a internet de forma a se ter menos riscos.

Entretanto, pouco tempo depois (e vinculado a AGESIC), foi criado o CERTuy, Centro Nacional de Respuesta a Incidentes de Seguridad Informática, por meio da Lei 18.362, no ano de 2008. Primeiramente, foi definido que o CERTuy seria responsável por “disseminar as melhores práticas sobre o assunto, centralizar e coordenar a resposta a incidentes com computador, bem como executar as tarefas preventivas correspondentes”. A partir de então, já se torna possível perceber certa preocupação envolvendo segurança cibernética por parte do Uruguai, bem como o desenvolvimento de sistemas que possibilitem respostas a possíveis ataques. No ano de 2009, por meio do Decreto nº 451, foi estabelecido que o CERTuy viria a proteger, também, os sistemas de computadores que suportam ativos críticos de informação do Estado, bem como os sistemas que o cercam. Aqui fica claro que o Uruguai percebe que existem riscos no ciberespaço, riscos estes que podem implicar em situações delicadas para as infraestruturas críticas nacionais e, por isso, o país estabelece tais diretrizes (LASSERE, 2016).

O CERTuy faz um trabalho extremamente importante: o organismo, além de trabalhar diariamente na detecção e monitoramento de incidentes, possui uma plataforma para receber relatos de acidentes cibernéticos no país e, a partir disso, desenvolve estatísticas sobre a quantidade e o tipo de acidentes realizados no ciberespaço uruguaio. Abaixo, as estatísticas referentes a quantidade de acidentes registrados no primeiro semestre de 2018:

Figura 5 – Quantidade de Acidentes Cibernéticos detectados no Ciberespaço Uruguaio



Fonte: CERTuy, 2019.

De acordo com o órgão, no primeiro semestre de 2018 foram contabilizados 786 incidentes relacionados a segurança informática, o que caracterizou um aumento de 78% se posto em comparação com o mesmo período no ano anterior. Algo muito importante que deve ser destacado, todavia, é que estes dados são referentes apenas aos incidentes que foram detectados pelos organismos ou reportados ao CERTuy, portanto, os números reais de incidentes podem ser ainda maiores. Com relação aos tipos de incidentes, três se destacaram: spam/phishing (37%) que diz respeito ao acesso indevido a dados como senhas e informações de acesso para variados tipos de serviços, o comprometimento de sistemas (30%) e a indisponibilidade de sistemas (20%), que é referente a tirar em sua totalidade os sistemas atacados do ar.

No quesito de Segurança Cibernética, no ano de 2015 foi criado o Centro de Resposta a Incidentes de Segurança Cibernética (DCSIRT), no âmbito do Ministério da Defesa Nacional. A sua criação é importante pois, como postula Lassere (2016), foi a primeira organização no campo específico de Defesa Nacional responsável por abordar questões de defesa cibernética. Entre o alvo pelo qual este órgão é responsável está o próprio Ministério da Defesa e aqueles organismos que são dependentes deste, como por exemplo as Forças Armadas. É importante salientar que, além de ações para tentar recuperar os sistemas uma vez que o ataque tenha se

materializado (desenvolvimento de sua resiliência), o Centro busca estabelecer medidas preventivas que sirvam para minimizar o impacto dos ataques. A respeito deste centro, algo interessante - e diferente dos outros dois casos trabalhos, Argentina e Brasil - é que, no caso uruguaio, a defesa e a segurança cibernética se misturam, uma vez que o Centro é intitulado como Centro de Resposta a Incidentes de Segurança Cibernética mas as ações feitas pelo mesmo são, também, ações de defesa cibernética, que buscam proteger as infraestruturas críticas do país de ataques inimigos assim como proteger os organismos dependentes do Ministério da Defesa.

Quadro 4 - Órgãos Responsáveis por Ciberdefesa e Cibsersegurança

	ARGENTINA	**BRASIL**	**URUGUAI**
Órgãos responsáveis por Defesa Cibernética	Comando Conjunto de Ciberdefesa (CCCD), com a função de conduzir as operações de ciberdefesa a fim de garantir a operacionalidade da Defesa Nacional.	ComDCiber: missão de contribuir para o uso efetivo do ciberespaço, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional.	DCSIRT, responsável pela segurança cibernética do Ministério da Defesa e dos organismos dependentes dele (como as FFAA).
Órgãos responsáveis por Segurança Cibernética	O ICIC-CERT argentino é responsável pelo registro de eventos que envolvam cibersegurança e ameaças/agressões.	No Brasil, as ações operacionais de cibersegurança são realizadas pelo Departamento de Segurança da Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional (DSI), da Presidência da República (PR).	O CERTuy é responsável por disseminar as melhores práticas sobre o assunto, centralizar e coordenar a resposta a incidentes com computador, bem como executar as tarefas preventivas correspondentes.

Fonte: elaboração própria com base nos websites oficiais de cada órgão.

A partir da tabela acima pode-se perceber que existe similaridade entre os três Estados tanto nos entendimentos acerca do que cabe aos organismos de defesa como quanto aos de segurança cibernética. Ao passo que claramente se pode perceber o caráter mais militarizado dos organismos de defesa cibernética (por lidarem com inimigos e ameaças externas), a segurança cibernética fica a cargo de organismos compostos por civis.

2.4 CONSIDERAÇÕES FINAIS

Neste capítulo foram trabalhadas diferentes abordagens acerca do espaço cibernético a partir do século XXI, como por exemplo as visões de autores que passam a incluir o espaço cibernético como um novo domínio, assim como o aéreo, marítimo, terrestre e o domínio espacial. Ademais, também foram expostas as conceituações dos países em análise sobre o ciberespaço - quando disponível -.

Em seguida foi realizada uma análise comparativa sobre os conceitos de Defesa e Segurança cibernética, que possuem diferentes significados para diferentes autores, mas que na maioria dos casos tem a defesa cibernética voltada pro caráter de defesa nacional, ou seja, de defesa quanto a inimigos externos e a segurança cibernética na maior parte das vezes é conceitualizada como a esfera que busca cuidar da segurança pública, dentro dos países. Também foi analisado para os três países em questão: Argentina, Brasil e Uruguai - quando disponível - quais eram os entendimentos de cada um dos países acerca dessas temáticas.

Por fim, foram trabalhados os organismos responsáveis por lidar com questões de Defesa e Segurança cibernética nos três casos analisados, onde foi possível perceber que existe uma grande similaridade entre os órgãos de Argentina e Brasil e uma certa diferenciação nos órgãos responsáveis por essas esferas no Uruguai.

3 ESTRATÉGIAS DE DEFESA E SEGURANÇA CIBERNÉTICA DE ARGENTINA, BRASIL E URUGUAI

Neste capítulo serão trabalhadas as estratégias de defesa e segurança cibernética de Argentina, Brasil e Uruguai, de acordo com seus documentos oficiais de Defesa, bem como com base nos documentos elaborados pelos órgãos responsáveis pelos setores de defesa e segurança cibernética analisados nos capítulos anteriores, como por exemplo o ComDCiber. Também ficará claro a partir deste mapeamento, que foi possível perceber que as ameaças presentes no ciberespaço, de fato, impactam no estabelecimento de estratégias de defesa e segurança cibernética nos documentos oficiais dos Estados em análise, tendo em vista que os países têm buscado se proteger neste novo domínio. Além disso, será feito um mapeamento, a partir das estratégias elaboradas pelos Estados, com o intuito de demonstrar como os três países em análise estão se articulando para responder e/ou se proteger das ameaças e ataques presentes no espaço cibernético. Por fim, serão trabalhadas as similaridades e diferenças entre as estratégias de defesa e segurança cibernética elaboradas por Argentina, Brasil e Uruguai.

Para o mapeamento da Argentina foram utilizados os Livros Brancos dos anos de 2010 e 2015, além de Resoluções e Decretos elaborados no âmbito do Ministério da Defesa argentino e, também a Diretiva de Política de Defesa Nacional, aprovada no ano de 2018.

O caso brasileiro é bastante notório, pois o país possui uma boa quantidade de documentos específicos acerca da temática cibernética, sendo eles: o Livro Verde de Segurança Cibernética do ano de 2010, a Estratégia de Defesa Nacional que foi lançada em 2008 e atualizada em 2012 a qual coloca o setor cibernético como um setor estratégico, assim como o setor nuclear e espacial e, também, a Estratégia Nacional de Segurança Cibernética, lançada no ano de 2019, além dos Livros Brancos de Defesa Nacional de 2012 e 2017 que também tratam sobre o tema.

Já o mapeamento uruguaio se deu principalmente pelo livro Segurança Nacional: situação da ciberdefesa e também pela Política Nacional de Defesa uruguaia, além do seu Livro de Defesa Nacional do ano de 2005.

3.1 ESTRATÉGIAS DE DEFESA E SEGURANÇA CIBERNÉTICA: CASO ARGENTINO

A Argentina não possui um documento oficial de Estado específico para tratar das estratégias nacionais de defesa do país, como é o caso do Brasil com o END. Entretanto, a partir da análise de documentos e decretos elaborados no âmbito do Ministério da Defesa argentino - além de seu Livro Branco de Defesa Nacional de 2010 e sua atualização de 2015 -, é possível identificar certos caminhos que estão sendo traçados pela Argentina no que tange ao setor de defesa cibernética.

No ano de 2010, com o lançamento seu Livro Branco de Defesa Nacional, a Argentina passou a dar maior destaque ao setor cibernético. Neste documento, o país discorre sobre como a sua política de Defesa está interconectada à sua estratégia nacional de desenvolvimento e, nesse sentido, traz a relevância do fortalecimento de sua indústria de defesa, inclusive por meio de cooperação em tecnologia e inovação.

A Argentina considera o avanço em pesquisa, desenvolvimento e aplicação de tecnologias relacionadas ao ciberespaço como estratégico, destacando que essas tecnologias são contribuições críticas para que se torne possível viabilizar os efeitos pretendidos pelo Estado argentino no âmbito de sua estratégia defensiva. Além disso, no Livro Branco de 2010 também é enfatizado que as inovações relacionadas ao setor cibernético são extremamente essenciais para que se tenha um alerta estratégico e antecipado de possíveis agressões militares advindas de atores externos, bem como para desenvolver de maneira efetiva as operações militares necessárias para se proteger dessas agressões e, por fim, também é destacado a capacidade de exercer o controle efetivo dos espaços terrestres, marítimos e aeroespacial da nação argentina por meio das tecnologias do setor cibernético (ARGENTINA, 2010).

Dentre as estratégias adotadas pelo Estado argentino no Livro Branco de Defesa Nacional de 2010 quanto as suas capacidades cibernéticas, são notáveis o desenvolvimento de dispositivos militares, capacidades, organizações e recursos humanos que irão servir para garantir que o uso e o controle do ciberespaço argentino continuem sob a guarda dos Sistemas Nacionais de Defesa (ARGENTINA, 2010). A ênfase dada aos recursos humanos é um fator importante na análise pois, apesar do ciberespaço ser majoritariamente eletrônico, as ações realizadas no mesmo são, no fim, feitas por seres humanos, portanto garantir o treinamento daqueles que irão operar em questões que envolvem defesa cibernética é extremamente necessário.

Os anos de 2014 e 2015 foram de extrema importância para a Defesa Nacional argentina como um todo, mas, especialmente, para o setor cibernético. Nestes dois anos, além de ter sido lançado um novo Livro Branco de Defesa Nacional em 2015 - o qual daria ainda maior ênfase ao ciberespaço e ao setor cibernético do que o de 2010 -, 2014 foi o ano em que o Comando Conjunto de Ciberdefesa argentino (CCCD) se tornou operante.

Neste Livro Branco, a Argentina destaca a crescente importância do espaço cibernético para o desenvolvimento de operações militares, especialmente pelo seu caráter artificial e que não necessita de localização física específica para funcionar ao mesmo tempo em que transpassa por todos os outros domínios, como destaca a Argentina:

> Outro aspecto associado ao novo paradigma científico-tecnológico e as tecnologias da informação é a importância que o ciberespaço tem adquirido para o desenvolvimento de operações militares. Este âmbito artificial e sem localização física precisa... possui meios, capacidades e regras próprias que o fazem atravessar os espaços terrestres, marítmos e aeroespaciais (ARGENTINA, 2015, tradução própria).

O Estado argentino deixa claro, então, a importância das ciências tecnológicas e das tecnologias da informação voltadas também para um caráter mais militarizado: o desenvolvimento de operações militares no ciberespaço, podendo atingir os demais domínios.

Também se destaca o fato das ações de ciberguerra, originadas e desenvolvidas no ciberespaço, terem a capacidade de desencadear efeitos cinéticos sobre o mundo real, de forma a poder afetar o controle de infraestruturas críticas, como por exemplo o controle sobre o abastecimento de água ou do setor de energia, nesse sentido a Argentina destaca que:

> Embora as ações de uma guerra cibernética tenham sua origem e desenvolvimento no campo virtual de redes de comunicação e nos sistemas de computadores, elas podem desencadear efeitos cinéticos específicos no mundo real e afetar o controle de infraestruturas críticas, como o suprimento de energia e abastecimento de água potável, tráfego aéreo e terrestre e, entre outros aspectos, a segurança de informações estratégicas (ARGENTINA, 2015, tradução própria).

Diante deste cenário que está cada vez mais difundido, o Estado argentino percebe que os desafios existentes no ciberespaço demandam que haja uma rápida

adaptação dos sistemas de defesa do país e o desenvolvimento de capacidades específicas que possam lidar com esse âmbito operacional.

Um ponto levantado no Livro Branco de 2015 da Argentina e que merece devida atenção, são os feitos a respeito do setor de defesa cibernética realizados no âmbito da Unasul, principalmente os que ocorreram por meio do Conselho de Defesa Sul-Americano (CDS). Durante o tempo em que o Conselho estava em operação, existiram enormes incentivos para a cooperação em Defesa entre os Estados-membros, de maneira que se tornasse possível, cooperativamente, criar mecanismos de defesa para lidar com ameaças extrarregionais. O documento também ressalta a importância da consolidação desse espaço regional caracterizado por ações de cooperação em defesa e de como isso serviu para constituir um processo de superação sobre as relações entre os Estados durante o século XX, principalmente no que diz respeito a assuntos militares. Apesar de países como Argentina[15] e Brasil terem anunciado suas respectivas saídas da Unasul, é notável que, no âmbito da organização, foi desenvolvido certo nível de confiança entre os países, portanto, é possível que - apesar de não ser mais viável que haja cooperação em defesa cibernética por meio da Unasul - a cooperação em defesa cibernética se dê por vias bilaterais ou por meio de outros organismos regionais.

Algo muito importante e que é destacado pela Argentina em seu Livro Branco de 2015 é a tendência em se consolidar um espaço regional que tenha como característica a cooperação em defesa na América do Sul, o que, sem dúvidas, supera a maneira como as questões relacionadas a defesa e ao setor militar como um todo eram lidadas no século passado nesta região. Diante disso, o Estado argentino incentiva o debate sobre a “reforma e adaptação das organizações regionais de defesa, com base nas atuais condições e princípios estratégicos regionais do Estado de Direito que governa os países da região” (ARGENTINA, 2015).

Especificamente sobre matéria de defesa cibernética, o Estado argentino salienta que, por meio da Unasul, se deve não apenas procurar garantir a segurança dos sistemas e das redes de informação dos países da região, mas também se deve focar em avanços para proteger o ciberespaço de cada Estado-membro contra

[15] "Argentina anuncia saída da Unasul devido ao 'alto ... - O Globo." 12 abr.. 2019, Disponível em: <https://oglobo.globo.com/mundo/argentina-anuncia-saida-da-unasul-devido-ao-alto-conteudo-ideologico-do-bloco-1-23596595>. Acessado em 14 nov.. 2019.

interferências externas que atentem contra os interesses dos Estados e/ou ataques aos seus setores estratégias e suas respectivas populações (ARGENTINA, 2014). Diante disso, se percebe claramente a importância dos organismos da região para a possibilidade de haver cooperação em defesa, o que foi feito no âmbito da Unasul entre os Estados sul-americanos de forma destacável no cenário internacional.

O Ministério da Defesa argentino definiu pontos da política nacional sobre ciberdefesa e cibersegurança em duas dimensões simultâneas:

1. Criação do Programa Nacional de Infraestruturas Críticas da Informação e Cibersegurança (Resolución JGM 580/2011), tendo como objetivo alcançar os padrões mínimos de segurança da informação necessários para a jurisdição e seus organismos descentralizados (ARGENTINA, 2011).

2. Coordenação das diferentes capacidades e unidades especializadas geradas no Ministério da Defesa, no Estado Maior Conjunto e nas Forças Armadas, a fim de elaborar uma política abrangente, uma proposta orgânico-institucional e desenvolver mecanismos de resposta integrados.

Diante disso, por meio da Resolução Ministerial 385 se cria a Unidade de Coordenação de Ciberdefesa, junto ao Gabinete do Ministro da Defesa. Tendo como função principal coordenador a política e o desempenho de atores vinculados a defesa cibernética. Posto isso, o Ministério da Defesa Argentino focou seus esforços para desenvolver um plano de trabalho para os anos de 2014-2015, tendo um plano de atividades que apreciava os seguintes objetivos prioritários:

1. Melhorar os níveis da infraestrutura e segurança, inclusive a padronização e aspectos técnicos;

2. Gerar estratégias de difusão por meio de ferramentas de treinamento e conscientização dentro e fora do Ministério da Defesa;

3. Desenvolver vínculos de intercâmbio e cooperação com os órgãos acadêmicos, científicos, empresariais e outros órgãos estatais;

4. Promover relações específicas acerca da temática de ciber, tanto a nível CDS-Unasul quanto bilateralmente, com os países que o compõem, assim como com a OEA e com os países-membros da União Europeia.

Diante dessas quatro estratégias trazidas no Livro Branco da Argentina de 2015, que foram encabeçadas pelo Ministério da Defesa, se torna perceptível que o Estado Argentino está disposto a cooperar para conseguir obter os níveis de segurança cibernética que almeja, inclusive explicitando que irá cooperar com universidades, cientistas da área e com o setor privado, que é um ator extremamente relevante quando o assunto é segurança cibernética, posto que grande parte das capacidades de segurança cibernética são geradas em empresas privadas. Além disso, a Argentina também destaca que irá cooperar com Estados da região seja por meios multilaterais (Unasul e OEA) ou bilateralmente com Estados-membros destes órgãos, além de prever cooperações com países da União Europeia.

Como exemplo dessa cooperação trazida pelo Estado argentino se pode pensar o caso ocorrido em 2016, resultado de um acordo feito pelo então ministro Celso Amorim em Buenos Aires, o qual previa a cooperação entre Argentina e Brasil em matéria de defesa cibernética. O Brasil recebeu em 2016, no seu curso de ciberguerra (promovido pelas Forças Armadas) e que é a principal atividade das forças de defesa brasileiras para preparar os militares para conflitos no espaço cibernético, o primeiro estrangeiro: um oficial argentino. Em contrapartida, um oficial brasileiro foi a Argentina para realizar capacitação em segurança de redes e criptografia (GOMES, 2014).

No ano de 2014 foi criado o Comando Conjunto de Ciberdefesa argentino, resultado da Resolução Ministerial 344/2014, sendo este dependente orgânica, funcional e operacionalmente do Estado Maior Conjunto das Forças Armadas. As principais atividades desenvolvidas por este Comando são focadas na determinação de necessidade de equipamentos, comunicações e redes; no levantamento das capacidades de cada uma das Forças; na análise de projetos de pesquisa e desenvolvimento e na coordenação de cursos de treinamento. O objetivo principal do Comando é gerar a capacidade de impedir e repelir ataques cibernéticos contra as infraestruturas críticas de informação bem como ativos do Sistema Nacional de Defesa e seu instrumento militar (ARGENTINA, 2014).

Em 2015, por meio da Decisão Administrativa 15/2015, se cria a Dirección General de Ciberdefensa, dentro da estrutura do Ministério da Defesa. Tendo como responsabilidade principal a intervenção no planejamento, formulação, direcionamento, supervisão e avaliação das políticas de ciberdefesa e sua respectiva jurisdição e para o instrumento militar. Dentro de suas funções estão a coordenação com outros organismos e autoridades estatais e também a promoção de intercâmbio e cooperação com os setores acadêmicos, científicos e empresariais, assim como na Resolução 385 tratada anteriormente (ARGENTINA, 2015). Os dois órgãos, o Comando Conjunto de Ciberdefesa e a Direção General de Ciberdefesa, funcionam de maneira integrada e têm como sede principal o Centro de Ciberdefesa.

Além da realização permanente de defesa cibernética para garantir as operações militares argentinas e a proteção de suas infraestruturas críticas, o Comando Conjunto de Ciberdefesa possui, do ponto de vista do planejamento, a responsabilidade de preparar o Plano de Emprego da Defesa Cibernética, seguindo as diretrizes estabelecidas pelo Estado Maior Conjunto.

Assim como os anos de 2014 e 2015, o ano de 2018 foi um ano bastante importante para o setor cibernético argentino. Pois, em 2018, foi aprovada a Diretiva de Política de Defesa Nacional, por meio do Decreto 703/2018, no âmbito do Ministério da Defesa. Neste decreto, é salientado que as ameaças cibernéticas mais sofisticadas são provenientes de organizações militares e agências de inteligência de outros Estados. Também é destacado que, apesar de países tecnologicamente avançados possuírem vantagens comparativas em relação aos outros países no setor cibernético, países menores também possuem a capacidade de implementar operações disruptivas no espaço cibernético. Diante disso, a Argentina percebe que é necessário que a Defesa Nacional passe a adotar medidas e ações para resguardar a segurança cibernética de suas infraestruturas críticas do Sistema de Defesa Nacional e daquelas que são designadas para a preservação das mesmas, independente da origem da agressão (ARGENTINA, 2018).

Neste Decreto, o Estado argentino prevê a utilização do espaço cibernético para fins militares, ao declarar que o ciberespaço como um ambiente militar configura ameaça de interesse estratégico para a Defesa Nacional, uma vez que por meio do ciberespaço inimigos argentinos podem tanto atacar setores estratégicos e infraestruturas críticas como corromper sistemas de defesa argentinos. Também é

destacado que o desenvolvimento de novas tecnologias da informação e de comunicação, interligados a extensão global da conectividade, tem tornado o ciberespaço em um âmbito no qual os Estados implementam operações de agressão e/ou influência sobre nações adversárias.

Além disso, é enfatizado no Decreto que a República Argentina deve adaptar suas organizações militares de maneira a possibilitar que se lide com o impacto dos riscos que emergem no espaço cibernético - o que já começou a ser feito desde a inauguração do Comando Conjunto de Ciberdefesa argentino (CCCD) em 2014 e também na capacitação das Forças em questões de defesa cibernético -, além disso, é destacado que a política de defesa cibernética precisa focar na redução gradual das vulnerabilidades que emergem da informatização de ativos estratégicos de interesse da Defesa Nacional (ARGENTINA, 2018).

Para tornar essas ações possíveis, são estabelecidos alguns pontos importantes no Decreto, como por exemplo a cooperação com outras áreas do Estado que tenham responsabilidade em matéria da política nacional de segurança cibernética. Também é estabelecido que o Ministério da Defesa tem o dever de fortalecer as capacidades de vigilância e controle no ciberespaço, possibilitando que se antecipe e previna ataques e/ou exploração cibernética de redes nacionais que possam vir a afetar o Sistema Nacional de Defesa argentino, assim como as ações direcionadas às infraestruturas críticas e/ou que permitam o acesso a ativos digitais estratégicos atribuídos as mesmas (ARGENTINA, 2018).

De acordo com a OEA e o Banco Interamericano de Desenvolvimento (2016), as Forças Armadas argentinas conduzem, anualmente, exercícios de resposta a ciber incidentes para compartilhar melhores práticas e revisar funções de comando e controle, entretanto, de acordo com as organizações, o Estado argentino possui capacidades limitadas de resiliência cibernética, ou seja, quando o país sofre um ciberataque, sua capacidade de recuperação ainda não alcançou os níveis desejados. Entretanto, assim como os documentos oficiais argentinos, a OEA e o BID não especificam nada a respeito dos exercícios que as Forças Armadas fazem.

Por fim, apesar da Argentina destacar em seus documentos algumas estratégias referentes a defesa cibernética, como por exemplo o objetivo de melhorar a segurança de suas infraestruturas críticas e gerar estratégias de difusão de conhecimento sobre cibernética tanto no âmbito do Ministério da Defesa como fora

dele, além de salientar que o país está desenvolvendo capacidades militares para se proteger de agressões no ciberespaço, os documentos não são transparentes a respeito de quais são as respostas previstas para lidar com os ataques e agressões no espaço cibernético, o que, em certa medida, pode ser interpretado como uma forma de proteção também, pois ao não divulgar quais são seus dispositivos e elementos específicos de defesa cibernética, o Estado argentino não abre brechas para atacantes externos adequarem seus ataques para lidar com a defesa argentina e, ao mesmo tempo, não limita a sua atuação no ciberespaço, podendo adequá-la ao que achar necessário em diferentes momentos.

3.1.1 Caso Brasileiro

Passando para a análise do Brasil, é importante ressaltar que, entre os países analisados, o Brasil é o que possui a maior quantidade de documentos acerca de defesa e segurança cibernética ou documentos que tratam sobre o tema apesar de não serem específicos da área de cibernética, como é o caso dos Livros Brancos de Defesa Nacional.

A Estratégia Nacional de Defesa (END) de 2008 é um marco de extrema importância para o setor cibernético no Brasil, pois, a partir da END, o setor cibernético passa a ser um setor estratégico para o Brasil, junto aos setores espacial e nuclear. De acordo com o documento, as capacidades cibernéticas terão as seguintes atribuições:

> se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar (BRASIL, 2008).

A partir de então, se torna perceptível a importância atribuída ao setor cibernético pelo governo brasileiro, além de também se demonstrar claro o caráter militar e securitário do ciberespaço, de forma a atribuir a capacitação do setor cibernético às Forças Armadas, de maneira a aperfeiçoar os dispositivos e procedimentos de segurança com o intuito de reduzir a vulnerabilidade dos sistemas

interligados a Defesa Nacional, fortalecendo o país contra possíveis ataques cibernéticos (BRASIL, 2008).

A atualização da Estratégia Nacional de Defesa (END) lançada no ano de 2012 é ainda mais específica sobre a temática cibernética, passando a elencar algumas estratégias necessárias para a evolução na área, são elas:

> (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;
>
> (b) Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;
>
> (c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;
>
> (d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;
>
> (e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;
>
> (f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;
>
> (g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas;
>
> (h) Estruturar a produção de conhecimento oriundo da fonte cibernética. (BRASIL, 2012)

A primeira estratégia, referente a evolução do Centro de Defesa Cibernética para um Comando de Defesa Cibernética (ComDCiber), se efetuou alguns anos após o lançamento da END (em 2016), contudo, o Centro não deixou de existir. Por meio da lista acima, fica claro que existe muito trabalho a ser feito quanto ao setor cibernético no Brasil, apesar de alguns pontos já estarem em pleno funcionamento, ainda é necessário que haja melhor distribuição do investimento em Defesa direcionado ao setor cibernético para que se alcance todos os objetivos almejados.

O primeiro documento oficial brasileiro a tratar especificamente sobre cibernética foi o Livro Verde: Segurança Cibernética no Brasil, lançado no ano de 2010. Neste documento o país demonstra seus desejos e suas preocupações com relação ao espaço cibernético e a sua segurança no mesmo. Logo na introdução do livro a segurança cibernética já é caracterizada como uma função estratégica do Estado no século XXI, além de ser destacada a sua essencialidade para garantir "a manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras" (BRASIL, p.13, 2010).

Assim como visto anteriormente no caso argentino, no Livro Verde brasileiro o país também se demonstra disposto a realizar parcerias e ações de cooperação entre países na matéria de segurança cibernética, uma vez que entende os impactos possíveis por causa da interdependência existente no ciberespaço. O governo brasileiro destaca que, para que a cooperação seja efetiva, é necessário que exista uma forma de governança bem estabelecida e que seja baseada em modelos efetivos e eficazes com colaborações de governo, setor privado e também a academia, ponto também similar ao que é trazido pelo governo argentino em seus documentos. Os governos estão cada vez mais percebendo que é extremamente difícil - e talvez até perigoso - tentar monopolizar a segurança do espaço cibernético e estão se colocando na mesa de diálogo junto a atores-chave no setor cibernético, como por exemplo o setor privado (que em grande medida é quem oferece serviços de segurança cibernética, inclusive para Estados) e também com a academia, que está constantemente produzindo conhecimentos valiosos sobre o ciberespaço e suas possíveis utilizações e riscos.

O Livro Verde traz oito pontos a nível político-estratégico que devem ser estabelecidos em matéria de segurança cibernética para se alcançar o que o Brasil almeja no ciberespaço, são eles:

1. Caracterizar a segurança cibernética como alta prioridade e de extrema urgência para o país, no curto prazo, implementando uma robusta estratégia nacional de segurança cibernética;

2. Valorizar e ampliar as competências nos diversos temas que perpassam a temática da segurança cibernética, e temas correlatos, como o de segurança das infraestruturas críticas da informação, no curto e médio prazo;

3. Lançar, no curto prazo, a Política Nacional de Segurança Cibernética;

4. Criar órgão central para macrocoordenação da Política Nacional de Segurança Cibernética, no curto prazo;

5. Estabelecer programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, no curto, médio e longo prazo;

6. Desenvolver arcabouço conceitual da segurança cibernética para o Estado brasileiro, no curto prazo;

7. Estender a capacidade da Defesa do País para proteção da nação no espaço cibernético;

8. Incrementar a capacidade dissuasória da Defesa do País para fazer frente a ameaça cibernética (BRASIL, 2010).

Logo no primeiro ponto estratégico se percebe a urgência em criar uma estratégia nacional específica para segurança cibernética o que, de fato, se concretizou neste ano de 2019 com o lançamento da Estratégia Nacional de Segurança Cibernética (E-ciber), que será analisada em seguida. Assim como a Argentina (e a maioria dos Estados) o Brasil também se demonstra bastante preocupado com a segurança das infraestruturas críticas da informação no ciberespaço, visto que qualquer vazamento e/ou ato de espionagem pode ter consequências graves. O ponto cinco, novamente, traz a questão da cooperação, tanto entre governos como com atores não-estatais, como por exemplo empresas de segurança cibernética (cooperação que, de acordo com o documento, será realizada tanto a nível doméstico como internacional). Por fim, os pontos sete e oito - referentes à Defesa do Brasil no ciberespaço e também a capacidade dissuasória da Defesa frente às ameaças no espaço cibernético -, são estratégias que já vêm sendo implementadas, por meio do ComDciber, órgão responsável pela defesa cibernética no Brasil.

O documento também levanta algumas preocupações e desafios para o setor cibernético no Brasil. Como por exemplo a falta de clareza acerca da real dimensão e importância da segurança cibernética como um tema de Estado, a quantidade de atores de governo envolvidos - o que pode levar a superposição de missões institucionais e dificultar a governança no espaço cibernético -, e outro ponto destacado no Livro Verde e que merece devida atenção é a falta de senso comum e de arcabouço conceitual sobre a segurança cibernética no Brasil, essa falta de consenso acerca da temática da cibernética e dos diversos conceitos que surgem desta pode ser problemática, pois um mesmo conceito pode ser interpretado de

diversas formas por atores distintos, podendo dificultar ações e interações no ciberespaço (BRASIL, 2010).

No que diz respeito a cooperação internacional, o Livro Verde destaca que o Brasil irá promover a cooperação bilateral e multilateral - em nível regional e global - de forma a trocar experiências, para que se fortaleça a estratégia nacional de segurança cibernética brasileira, além de participar da articulação de acordos de cooperação técnica de segurança cibernética, participação internacional que de certa maneira vai de encontro com a vontade do Brasil de ser um dos grandes jogadores do ciberespaço no futuro, como foi explicitado no próprio documento (BRASIL, 2010).

Já o Livro Branco de Defesa Nacional de 2017 coloca a cibernética entre os temas que apresentam implicações para a proteção da soberania brasileira e, devido a isso, a defesa cibernética deve ser vista como prioridade. Também é salientado no Livro que a possibilidade de guerras cibernéticas no século XXI se mostra como um grande desafio para a capacidade brasileira de defesa e para o mantimento da paz e segurança internacionais (BRASIL, 2017). Um importante passo para lidar com essas implicações foi a criação do Centro de Defesa Cibernética (ComDCiber) no ano de 2016, que tem como missão

> planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética, sendo seu órgão central, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas brasileiras e impedir ou dificultar sua utilização contra interesses da Defesa Nacional (BRASIL, 2017).

O ano de 2019 foi um ano bastante importante para o setor cibernético no Brasil. Neste ano foi lançada a Estratégia Nacional de Segurança Cibernética (E-Ciber), que contou com a participação de mais de 40 órgãos e entidades do governo, e também com instituições privadas e do setor acadêmico. Um ponto salientado na estratégia é o papel do cidadão brasileiro e suas responsabilidades no ciberespaço, de acordo com o documento é necessário que as/os brasileiras/os elevem sua participação no espaço cibernético, de forma a não apenas utilizar as tecnologias disponíveis mas, essencialmente, reportar por meio dos canais disponíveis para denúncias (como o canal de denúncias do CERT.br trabalhado no capítulo anterior, por exemplo) todas as ações maliciosas e crimes que se perceber e/ou for vítima no ciberespaço (BRASIL, 2019).

O documento considera como de extrema importância que seja criado um ambiente colaborativo no qual participem a administração pública, o setor privado e a sociedade civil, no qual sejam compartilhadas informações e aprendizados pois no ciberespaço é possível que as ameaças e crimes sofridos pelas organizações sejam parecidos e/ou os mesmos, portanto uma rede na qual sejam compartilhadas as lições aprendidas deve ser criada.

Como exemplo de ação colaborativa de sucesso o documento elucida o “Guardião Cibernético”, exercício organizado todos os anos pelo Comando de Defesa Cibernética (ComDCiber) em parceria com o Gabinete de Segurança Institucional da Presidência da República, com participantes dos Ministério da Defesa, da Justiça e das Relações Exteriores; do Gabinete de Segurança Institucional da Presidência da República; das Forças Armadas; órgãos do Governo Federal; Banco Central do Brasil, bancos públicos e privados; empresas dos setores nuclear, elétrico e de telecomunicações, além de acadêmicos, todos agindo cooperativamente para atingir seus objetivos, tanto em nível decisório (gestão de crises) como em nível técnico (resposta a incidentes), ambos de grande impacto para as organizações envolvidas. De acordo com o documento, o Brasil ainda carece de ações de capacitação que alcancem as diferentes esferas de governo, ao mesmo tempo em que ainda é necessário dedicar atenção especial à proteção das infraestruturas críticas nacionais, portanto é preciso realizar ações que protejam as estruturas relacionadas a internet como os grandes servidores, os pontos de troca de tráfego e os *datacenters*, que mantém o funcionamento dos setores críticos da rede (BRASIL, 2019).

A E-Ciber destaca que os principais tipos de ameaças contra as infraestruturas críticas são os ataques de phishing - que servem para obter dados de forma ilegal -, negação de serviços em larga escala - o que é um grande problema pois pode afetar o fornecimento de água ou energia elétrica da população, por exemplo -, vazamento de informações privadas ou institucionais, espionagem cibernética e a interrupção de serviços. Diante desse cenário, a estratégia ressalta que para realizar a proteção das infraestruturas críticas contra ameaças cibernética é preciso que haja uma abordagem ampla de segurança cibernética, avaliando riscos, realizando planejamentos calculados e coordenando e desenvolvendo ações de cibersegurança, além de destacar que deve haver ação conjunta entre governo e os operadores das

infraestruturas críticas, pois é a forma mais provável de garantir de proteger as IFCs no espaço cibernético (BRASIL, 2019).

A estratégia destaca claramente seus objetivos em matéria de segurança cibernética, sendo eles: tornar o Brasil mais próspero e confiável no espaço cibernético, aumentar a resiliência brasileira frente às ameaças cibernéticas - resiliência tem a ver com a capacidade do Estado de se recuperar de ataques e retomar o controle daquilo que foi atingido, por exemplo -, e, por fim, fortalecer a atuação do Brasil em segurança cibernética no cenário internacional, novamente trazendo a vontade do Brasil em se tornar um dos grandes jogadores em matéria de cibernética (BRASIL, 2019).

Por fim, a Estratégia Nacional de Segurança Cibernética estabelece dez ações estratégicas para tornar possível aprimorar a segurança cibernética brasileira, as ações serão expostas na imagem abaixo e trabalhadas a seguir:

Figura 6 – Ações Estratégicas do Governo Brasileiro

Fonte: BRASIL, 2019

A primeira ação diz respeito ao fortalecimento das ações de governança cibernética, trabalhando junto com os setores público e privado, com atividades relacionadas à gestão de pessoas, atendimento aos requisitos de cibersegurança e também à gestão dos ativos da informação, o documento estabelece ações que podem ser adotadas para para alcançar este objetivo, como por exemplo a realização de foros de governança, importação de programas e projetos sobre governança cibernética e a adoção de padrões internacionais pela indústria de segurança cibernética. Essa ação possui dois pontos bastante interessante, o primeiro é a gestão de pessoas, fator chave ao se tratar do espaço cibernético pois apesar de se tratar de um domínio majoritariamente digital, as ações realizadas no ciberespaço são feitas por seres humanos, portanto, àqueles que trabalham com cibersegurança precisam ser devidamente preparados para tal. O segundo ponto é a questão a respeito da adoção de padrões internacionais pela indústria de segurança cibernética brasileira, o que em primeira mão parece bastante interessante, mas é preciso buscar entender de que padrões se trata, pois ainda não existe uma padronização internacional acerca de segurança cibernética, diferentes práticas são adotadas por diferentes Estados e por diferentes empresas (BRASIL, 2019).

A segunda ação estratégica diz respeito ao estabelecimento de um modelo centralizado de governança no âmbito nacional, o que ocorrerá por meio da criação de um Sistema Nacional de Segurança Cibernética e que deverá ter as seguintes atribuições iniciais: a promoção da coordenação dos inúmeros atores envolvidos na segurança cibernética, realização de análises conjuntas sobre os desafios enfrentados no ciberespaço, a governança também servirá para auxiliar na formulação de políticas públicas relacionadas à segurança cibernética. Fica perceptível a necessidade atribuída pelo governo brasileiro acerca da governança cibernética, envolvendo setores público e privado, uma vez que duas das dez ações estratégicas estabelecidas na E-Ciber dizem respeito a isso. Por fim, o documento estabelece que essa governança de cibersegurança deverá ser coordenada pelo Gabinete de Segurança Institucional da Presidência da República, entretanto, destaca também que será necessária a cooperação e participação da Defesa Cibernética, que está a cargo do Ministério da Defesa por meio do ComDCiber (BRASIL, 2019).

A terceira ação estratégica discorre a respeito da promoção de um ambiente que seja colaborativo, participado, confiável e seguro, de maneira a envolver os setores público e privado, além da sociedade como um todo. Como exemplo para tornar essa ação factível são elencados o compartilhamento de informações privadas sobre incidentes e vulnerabilidades cibernético, realização de exercícios cibernéticos com a participação de múltiplos atores (que pode ter como inspiração o exercício Guardião Cibernético, realizado anualmente pelo ComDCiber), e também na maior utilização de recursos criptografados, entre outros (BRASIL, 2019).

Já a quarta ação estratégica fala sobre como é necessário elevar o nível de proteção do governo, o que pode ser feito por meio de ações no ciberespaço como por exemplo incluindo requisitos mínimos de segurança cibernética nos contratos de órgãos e entidades governamentais, no aperfeiçoamento e incentivo do uso de dispositivos de comunicação segura do governo, o que se mostrou necessário no governo de Jair Bolsonaro, a partir do momento em que vazamentos de diálogos do próprio Presidente da República e de seus ministros vieram a tona pois os membros do governo não utilizavam dispositivos criptografados. [16]

A quinta ação estratégica é um ponto comum em todos os documentos analisados: trata-se de elevar o nível de proteção das Infraestruturas Críticas Nacionais, o que deve ser feito por meio do aumento da resiliência, possibilitando uma contínua prestação de serviços essenciais, como por exemplo fornecimento de água e energia. Para tal, é preciso promover a interação entre as agências responsáveis pelas IFCs para aprender e aprimorar os conhecimentos sobre cibersegurança, além de estimular a adoção de ações de segurança cibernética pelas IFCs e incentivar a implementação de políticas de segurança cibernética, como também incentivar a participação dos responsáveis pelas IFCs a participarem de exercícios cibernéticos, como àquele realizado pelo ComDCiber (BRASIL, 2019).

Em seguida, na sexta ação estratégica, se trata sobre o aprimoramento do arcabouço legal sobre cibersegurança, a necessidade de revisar, atualizar, abordar novos temas e elaborar novos instrumentos. Para alcançar esse objetivo, a E-Ciber destaca que é necessário identificar e abordar os temas que não estão presentes na

[16] "GSI alertou Bolsonaro e ministros sobre riscos de ... - O Globo." 25 jul.. 2019, Disponível em: <https://oglobo.globo.com/brasil/gsi-alertou-bolsonaro-ministros-sobre-riscos-de-comunicacao-em-celulares-nao-criptografados-23831668>. Acessado em 17 nov.. 2019.

legislação vigente, consolidar a legislação que trata sobre crimes cibernéticos, criar políticas de incentivo para contratação de mão de obra que seja especializada em segurança cibernética, o que é extremamente vital para se construir um ciberespaço seguro.

A sétima ação discorre sobre o incentivo a concepção de soluções inovadores em segurança cibernética, por meio do incentivo à pesquisa e desenvolvimento que possam trazer inovação ao setor cibernético brasileiro, inclusive incentivando projetos acadêmicos que abordem as necessidades da área. A E-Ciber salienta que a inclusão da cibersegurança nos programas de fomento à pesquisa, no incentivo à criação de centros de pesquisa focados no desenvolvimento de cibersegurança e também na viabilização de investimentos tanto por meio de fundos públicos e privados, além do incentivo a criação de startups de segurança cibernética, algo que é comum nos países líderes em questões de segurança cibernética, como é o caso de Israel.[17]

Ampliação da cooperação internacional em matéria de segurança cibernética é a oitava ação estratégica estabelecida pela E-Ciber, aqui o Brasil sinaliza buscar a cooperação com o maior número possível de países - de maneira transparente -, buscando reforçar a possível brasileira na busca pela paz e segurança internacionais. Para alcançar tal objetivo, a E-Ciber destaca que são necessários o estímulo a cooperação internacional em matéria de cibersegurança, maior incentivo a discussões que envolvam o tema nos órgãos internacionais e em fóruns dos quais o Brasil faz parte, além de destacar a necessidade de uma aproximação com os países da região em matéria de cooperação cibernética, o que, em certa medida, acontecia por meio da Unasul e agora pode continuar sendo feito pela OEA (onde também já ocorria, entretanto num escopo regional com mais atores). O que pode se tornar um problema nessa ação estratégica estabelecida pelo Brasil é quanto ao endossamento da cooperação internacional em matéria de segurança cibernética, pois, apesar dos Estados buscarem cooperação para aprimorar sua própria segurança, a probabilidade de alguns Estados abrirem mão de participar de ditas cooperações por não terem vontade de compartilhar suas estratégias de segurança cibernética por questões de segurança é grande.

[17] "Israeli Startups Shine In The $92 Billion Cybersecurity Market." 26 fev.. 2019, Disponível em: <https://www.forbes.com/sites/gilpress/2019/02/26/israeli-startups-shine-in-the-92-billion-cybersecurity-market/>. Acessado em 17 nov.. 2019.

A nona ação estratégica é sobre a parceria entre setor público, privado, academia e sociedade civil, algo que foi bastante trabalhado ao longo do documento para enfatizar a importância de todos os atores no ciberespaço. Essa cooperação entre todos os setores da sociedade buscará elevar a maturidade da cibersegurança, podendo ocorrer por meio de incentivos financeiros e materiais, além da implementação de programas, projetos e ações sobre cibersegurança, que alcancem toda a sociedade brasileira (BRASIL, 2019). É interessante notar a importância dessa estratégia, entretanto, também é preciso ter em mente que no ano de 2019, cerca de 30% da população brasileira ainda não possui acesso a internet, o que torna essa ação inviável, pelo menos no presente momento.[18]

A décima e última ação estratégica trazida pela E-Ciber fala sobre a necessidade de elevar o nível de maturidade da sociedade em questões que envolvem a segurança cibernética. Para tal, se identifica que é necessário incentivar órgãos públicos e empresas privadas a realizar campanhas de conscientização internas, também se percebe necessário realizar ações de conscientização da população e criar políticas públicas que promovam essa conscientização sobre a importância da segurança cibernética. A conscientização precisa ser abrangente, e devido a isso, o documento destaca que é necessário incluir a segurança cibernética nos níveis de ensino infantil, fundamental e médio, além da estimulação a criação de cursos de nível superior focados em segurança cibernética. Já existem alguns cursos superiores e técnicos (majoritariamente privados) com foco em segurança cibernética, como é o caso da Escola Superior de Redes[19], entretanto, para oferecer o ensino de segurança cibernética em escolas públicas de nível infantil a médio, seria necessário um investimento e preparação de profissionais enorme, visto que não existem profissionais suficientes da área ainda para abarcar tal demanda, posto isso, a estratégia é extremamente necessária para aumentar a maturidade brasileira em questões de segurança cibernética, contudo, é preciso se pensar melhor em como efetivar isso de fato.

---

[18] "Uso da internet no Brasil cresce, e 70% da população ... - G1." 28 ago.. 2019, Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml>. Acessado em 17 nov.. 2019.

[19] "Escola Superior de Redes - RNP." Disponível em: <https://esr.rnp.br/> .Acessado em 17 nov.. 2019.

O caso dos documentos brasileiros é bastante parecido com o Argentino: o governo salienta e exemplifica algumas de suas estratégias voltadas para a defesa cibernética e para a segurança cibernética, como por exemplo a necessidade de incrementar a capacidade dissuasório da Defesa brasileira frente à ameaças cibernéticas, desenvolver capacitação de pessoal na área cibernética, desenvolver sistemas computacionais de alto padrão para efetivar a defesa cibernética, entre inúmeras outras estratégias.

Contudo, assim como o governo argentino, o governo brasileiro em nenhum momento esclarece nos documentos por quais meios essas estratégias serão de fato efetivadas, quais recursos serão utilizados e como, de fato, o Brasil irá lidar com as ameaças e agressões cibernéticas. Postura que, como dito anteriormente, pode ser uma própria forma de defesa do País, para não deixar o inimigo saber quais são os arcabouços disponíveis no Brasil para lidar com ameaças cibernéticas, ou, por outro lado, essa não especificação pode ocorrer pelo fato de que, dessa maneira, o governo não restringe sua atuação no ciberespaço, podendo atuar em diferentes momentos de distintas formas, como melhor achar adequado. É importante destacar também, que, como destacado por Gonzales e Portela (2018), Argentina e Brasil possuem uma formação híbrida nos setores de defesa e segurança cibernética: órgãos militares estão a cargo do primeiro e civis do segundo, o que de maneira alguma impede que exista cooperação entre as esferas de segurança e defesa cibernética quando necessário.

3.1.2 Caso Uruguaio

Em seu Livro de Defesa Nacional lançado em 2005 e, principalmente, no anexo documental do mesmo, o Uruguai já se demonstrava preocupado com a sua segurança cibernética. No anexo documental o país afirmou que irá trabalhar para desenvolver uma cultura de cibersegurança nas Américas por meio da adoção de medidas eficazes de prevenção que servirão para antecipar, tratar e responder a ataques cibernéticos, independente de qual seja a origem do ataque (o que abre margem para a Defesa lidar com atores internos), além de destacar que o país irá combater ameaças cibernéticas e crimes cibernéticos, de forma a tipificar os ataques que possuem seu ciberespaço como alvo, além disso o país também salienta a

proteção das infraestruturas críticas e a garantia do sistema de redes como prioritário (URUGUAI, 2005).[20]

O organismo uruguaio responsável pela resposta a incidentes de segurança informática no país (CERTuy), estabelecido no ano de 2008, coordena conjuntamente a outros órgãos regionais e internacionais as respostas para como lidar com acidentes e como respondê-los. Além disso, o CERTuy fornece registros estatísticos sobre ataques cibernéticos - como foi trabalhado no capítulo anterior - e emite alertas sobre possíveis riscos iminentes. Ao passo que o CERTuy está mais ligado a acidentes e ataques que coloquem em risco a segurança informática, a Política Nacional de Defesa incorpora as medidas de defesa cibernética (URUGUAI, 2017).[21]

Um ponto muito importante trazido por Guedes et al. (2017) é que o Uruguai, além de possuir o CERTuy que lida com a segurança cibernética na administração pública uruguaia, o países também possui um CERT Militar: o DCSIRT, que tem como missão prevenir e minimizar incidentes e agressões que tenham como alvo as Forças Armadas do Uruguai. Ademais, os autores também destacam que o DCSIRT, além de ser responsável por essas questões citadas, também lida com emergências cibernéticas, controle de tráfego fronteiriço, aéreo e marítimo.

A Política Nacional de Defesa uruguaia, por sua vez, estabelece algumas estratégias prioritárias quanto à questões relacionados ao espaço cibernético, são elas: a proteção do Estado, do governo e da população uruguaia de todas as formas de espionagem, de forma a reafirmar a soberania nacional e o direito à privacidade e segurança das comunicações internas e internacionais do país, além de proteger o Uruguai de ataques cibernéticos e preservar seus dados que são produto das gestões estatais e de empresas privadas, tanto a nível nacional como regional, de acordo com o que se perceber necessário e, por fim, o Uruguai destaca que irá incentivar o uso de software livro no país, o que deve ser entendido como um software que respeita a liberdade e o senso de comunidade dos usuários, não cometendo crimes e delitos no ciberespaço, por exemplo (URUGUAI, 2014). Percebe-se na PND uruguaia que o país estabelece quais são seus objetivos de proteção no ciberespaço, entretanto, o

[20] "anexo documental - Resdal.". Disponível em: <https://www.resdal.org/Archivo/uru-defensa-anexo.pdf>. Acessado em 17 nov.. 2019.
[21] "situación de la ciberdefensa - Centro Militar." Disponível em: <http://www.centromilitar.org.uy/Servicios/RevistaElSoldado/RevistaElSoldado192.pdf>. Acessado em 17 nov.. 2019.

documento deixa a desejar no quesito de quais instrumentos serão utilizados para de fato efetivar as ações de defesa cibernética do país.

O Uruguai admite que ainda possui um longo caminho a ser percorrido para ter sua estratégia completa de defesa e segurança cibernética, assim como estruturas conjuntas e integradas para enfrentar os ciberataques, contudo, o país já consegue delinear certos esforços para lidar com questões de ciberdefesa e cibersegurança. No que diz respeito a estratégia de uso do ciberespaço, o país afirma que esta irá cumprir os preceitos estabelecidos pela legislação uruguaia e a respeito do direito à legítima defesa, consagrado na Carta das Nações Unidas, irá se reservar o direito ao uso da força em caso de agressões militares externas, posto isso, o país assume que só haveria um ataque cibernético do Estado uruguaio caso ocorresse uma agressão externa nesta área. Assim como foi feito na Argentina e no Brasil, o Uruguai entende que as estruturas militares de defesa cibernética deverão ser enquadradas no âmbito do Estado Maior da Defesa, dependente do Ministério da Defesa e que será responsável tanto pela elaboração da doutrina cibernética como do planejamento e comando das operações realizadas pelas Forças Armadas uruguaias (URUGUAI, 2017).

A OEA (2016) destaca que, apesar do Uruguai não possuir uma estratégia nacional de cibersegurança, o país é líder regional no desenvolvimento de sofwares de segurança e um mercado em ascensão para tecnologias e seguros contra crimes cibernéticos. O organismo também destaca que o CERTuy, que foi estabelecido em 2008, coordena frequentemente atividades com outros CERTs regionais e além de produzir respostas aos incidentes e agressões cibernéticos, o CERTuy também disponibiliza estatísticas sobre os ciberataques direcionados ao Uruguai, como já trabalhado no capítulo anterior. Outra iniciativa criada pelo CERTuy foi a campanha Se Conecte de Forma Segura e Seu Data Tem Valor, campanha de conscientização nacional para tentar melhorar a segurança da sociedade uruguaia no ciberespaço.

Por fim, apesar do Uruguai ainda não possuir uma estratégia de defesa e segurança cibernética, o país tem modernizado sua estrutura legal e também tem incluído as ameaças relativas ao ciberespaço junto àquelas que podem afetar o dia-a-dia de sua população e que precisam ser lidadas pelo Estado, sendo objetivo da Defesa Nacional. Como exemplo disso pode-se pensar na criação dos já trabalhados

CERTuy e na AGESIC, responsável pela elaboração do Marco de Cibersegurança também utilizado neste trabalho.

3.2 ANÁLISE COMPARATIVA DOS CASOS

A partir do trabalho realizado neste capítulo, se torna claro que os casos argentino e brasileiro são bastante semelhantes, talvez por ambos os países já terem seus Comandos cibernéticos militares estruturados para lidar com questões de defesa cibernética, o que muitos países ainda não conseguiram fazer, como é o caso do Uruguai, que está trabalhando fortemente para alcançar este objetivo. Além disso, outro ponto comum entre Argentina e Brasil é que, apesar dos Estados elencarem em seus documentos oficiais de defesa as suas estratégias referentes a segurança e defesa cibernética, eles não são transparentes sobre como irão, de fato, implementar essas estratégias. Por exemplo, quando a Argentina fala que está desenvolvendo capacidades para lidar com agressões externas, o país não discorre sobre quais são essas capacidades, ou como elas funcionariam. O que pode ter diferentes motivos para ocorrer, como a real vontade de não explicitar nenhuma característica específica de suas estratégias para garantir que seus inimigos externos não tenham conhecimentos avançados sobre a defesa de Argentina ou Brasil e possam explorar isso a seu próprio benefício, entretanto, outra possibilidade é que os países podem simplesmente escolher não divulgar como irão efetivar suas estratégias de defesa cibernética pois, dessa maneira, podem agir no ciberespaço sem grandes represálias, já que não está definido como eles devem agir.

O Uruguai, por sua vez, é considerado um líder regional em segurança cibernética, status que recebe devido ao seu avançado desenvolvimento de softwares de segurança e o crescente mercado do mesmo, existem diversas parcerias entre governo e setor privado na área. Entretanto, o país ainda não possui um Comando militar cibernético (apesar de afirmar estar o criando), também não possui documentos específicos sobre defesa cibernética, como Argentina e Brasil.

Um ponto comum entre os três casos é a preocupação dos Estados com suas infraestruturas críticas nacionais, seja em maior, seja em menor nível, a segurança e defesa das infraestruturas críticas nacionais é algo que sempre está presente no discurso dos países, os três países afirmam que estão constantemente desenvolvendo capacidades para lidar com ataques/agressões externas a suas IFCs,

novamente, apesar de demonstrarem tamanha preocupação e afirmarem possuir capacidades para lidar com tais atos, os Estados não divulgam em seus documentos oficiais como irão implementar tais estratégias de defesa e segurança cibernética.

3.3 CONSIDERAÇÕES FINAIS

Neste capítulo foram exploradas, majoritariamente, as estratégias de defesa e segurança cibernética de Argentina, Brasil e Uruguai, com o objetivo de mapear as estratégias desse campo novo nas relações internacionais que é a segurança e defesa cibernética para que, em futuros trabalhos, seja possível realizar pesquisas mais aprofundadas do tema, já existindo esse mapeamento levantado. Existem pontos semelhantes e distintos merecedores de análise nos três casos: entre os principais pontos percebidos nos três casos está a necessidade de criar mecanismos para proteger as infraestruturas críticas nacionais dos países, o que é algo bastante natural visto que o fornecimento de serviços básicos corre o risco de ser interrompido caso haja um ciberataque direcionado às infraestruturas críticas, como por exemplo um ataque de negação de serviços, no qual se obtido sucesso, o fornecimento de água ou energia elétrica poderia ser totalmente cortado para uma região ou até mesmo para um país inteiro dependendo da dimensão do ataque. Outro ponto bastante trabalhado tanto pelos documentos argentinos como brasileiros é a questão da cooperação nos mais diversos níveis: tanto a nível doméstico, entre o setor público, privado e a academia, como no nível internacional.

De maneira a responder especificamente ao problema de pesquisa “como se dá o estabelecimento de estratégias de defesa e segurança cibernética em Argentina, Brasil e Uruguai?”, se pode perceber que o estabelecimento de estratégias de defesa e segurança cibernética nesses três Estados vem ocorrendo por meio da institucionalização dessas estratégias nos documentos oficiais desses países, bem como em documentos específicos para tratar sobre a questão cibernética. O que ocorre, claramente, devido a crescente importância dada a temática por esses Estados, que buscam criar os dispositivos necessários para se proteger no ciberespaço.

Como foi possível visualizar ao longo do capítulo, ao passo que Argentina e Brasil já possuem inúmeras estratégias de defesa e segurança cibernética bem estabelecidas, o caso do Uruguai é bastante diferente. O Uruguai possui organismos

responsáveis por lidar com as questões de defesa e segurança cibernética, como foi explicitado por meio da análise da PND uruguaia e do CERTuy e a AGESIC, entretanto, o país está trabalhando para lançar sua estratégia nacional de defesa cibernética, contudo, o país já deixou claro que, assim como nos casos de Argentina e Brasil, as estruturas militares de defesa cibernética estarão a cargo do Ministério da Defesa. Outro ponto trabalhado pelos países em seus documentos e que merece devida atenção é a questão da preparação da gestão de pessoas que irão lidar com defesa e segurança cibernética, pois, apesar do ciberespaço ser majoritariamente digital, as decisões realizadas neste ambiente são feitas, no fim, por seres humanos, e portanto estes que irão trabalhar no setor cibernético devem estar devidamente treinados para evitar que ocorrem decisões errôneas e que possam comprometer a atuação dos Estados.

CONSIDERAÇÕES FINAIS

A partir da realização deste trabalho, se espera que tenham sido elucidadas e esclarecidas questões a respeito da segurança e defesa cibernética de Argentina, Brasil e Uruguai. No primeiro capítulo foram explorados casos relevantes sobre ciberataques no sistema internacional e com impacto na política internacional. O caso Stuxnet sofrido pelo Irã foi um marco para a cibernética no mundo pois, a partir dele, diversos países ao redor do globo perceberam a necessidade de securitização do ciberespaço para garantir que sua soberania, a segurança de sua população e de suas infraestruturas críticas não sofressem danos com ações externas por meio do espaço cibernético.

Também se espera que tenham se tornado mais claras as definições acerca de segurança cibernética e defesa cibernética para os três casos explorados, como a exemplo disso, o caráter mais militarizado voltado para a defesa nacional quanto a inimigos externos e o caráter de segurança pública da segurança cibernética, buscando manter o funcionamento das instituições dentro dos Estados como é apontado pelos Estados em seus documentos oficiais.

Foram trabalhados também os organismos responsáveis pelas questões de cibersegurança e ciberdefesa, como o CCCD na Argentina, o ComDCiber no Brasil, além dos CIC-CERT, CERT.br, CERTuy, AGESIC, entre outros, todos órgãos de extrema relevância para as esferas de defesa e segurança cibernética e para a proteção dos países e de suas infraestruturas críticas. Como se tornou claro por meio da análise dos documentos oficiais dos países, nos quais em todos os casos a necessidade de proteção às IFCs estava presente, devido a sua importância para manter o funcionamento e normalidade dos países, bem como o funcionamento dos diversos tipos de serviços que dependem de energia ou de sistemas telefônicos, por exemplo.

No segundo capítulo foram exploradas diferentes abordagens sobre o ciberespaço no século XXI, assim como diferentes visões acerca do ciberespaço como um novo domínio, junto ao aéreo, espacial, marítimo e terrestre. Esta visão é extremamente relevante, pois o ciberespaço além de ser considerado um novo domínio, como foi demonstrado ao longo do trabalho, este possui uma capacidade que o torna único: a possibilidade de penetrar e influenciar todos os outros domínios. No terceiro e último capítulo, foi exposto o foco principal do trabalho, sendo este o

estudo exploratório das estratégias de defesa e segurança cibernética de Argentina, Brasil e Uruguai Este mapeamento é extremamente necessário visto que essa é uma temática bastante nova e pouco explorada e, esperançosamente, esse mapeamento será utilizado para a realização e aprofundamento de futuras pesquisas na área.

A partir desse mapeamento foi possível perceber uma preocupação comum entre os três casos que é relacionada a proteção de suas infraestruturas críticas nacionais, como telefonia, abastecimento de água ou energia. Outro ponto importante, e que se tornou perceptível, foi a realidade híbrida de Argentina e Brasil quanto a ciberdefesa e cibersegurança, o que se efetiva a partir do momento em que os organismos responsáveis pela primeira são militares e os responsáveis pela segunda são civis. Entretanto, é preciso enfatizar que existe cooperação entre os órgãos militares e civis em ambos os países. O Uruguai, apesar de ainda não ter seu Comando militar cibernético estruturado (o Comando, de acordo com o país, já está sendo desenvolvido e será inaugurado em breve), possui grande relevância na temática por ser um líder regional no desenvolvimento de softwares de segurança cibernética e ter esse mercado em ascensão.

Tratando especificamente do problema de pesquisa, que questiona como se dá o estabelecimento de estratégias de defesa e segurança cibernética na Argentina, Brasil e Uruguai, foi possível perceber a partir da exploração e da análise dos documentos que a crescente presença de ameaças e a realização de agressões por meio do ciberespaço, especialmente a partir do século XXI, fez com que os Estados voltassem sua atenção e esforços para elaborar estratégias que possibilitassem manter sua proteção e soberania no ciberespaço. Se pode perceber que Argentina e Brasil já possuem em seus documentos (inclusive alguns documentos específicos para tratar sobre estratégias relativas à defesa e segurança no ciberespaço) estratégias bem elaboradas para lidar com a temática. Isso se manifesta no desenvolvimento de sistemas de computadores de alto padrão para efetivar a defesa cibernética, na capacitação de pessoal para lidar com o ciberespaço e no desenvolvimento de sistemas de segurança para proteger as infraestruturas críticas (o que também é visto no caso uruguaio).

Contudo, um ponto comum aos três casos, é que eles não especificam em seus documentos oficiais como as suas estratégias - que já foram elaboradas - serão, de fato, colocadas em ação. Medida que pode ser interpretada, como forma de manter a

segurança e soberania dos países, pois, ao não divulgar precisamente como a defesa e segurança cibernética serão realizadas, os países não correm o risco de terem seus oponentes melhor se preparando especificamente para lidar com os sistemas de defesa nacionais mas que, ao mesmo tempo, também pode ser interpretada como uma forma que os Estados encontraram para não limitar sua atuação no ciberespaço. Pois ao não estar explicito como, de fato, Argentina, Brasil e Uruguai irão lidar com as ameaças no ciberespaço, eles possuem liberdade para agir da maneira que acharem necessário.

REFERÊNCIAS

AGESIC. **MARCO DE CIBERSEGURIDAD:** Marco de Referencia. 2018. Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento. Disponível em: <https://www.agesic.gub.uy/innovaportal/file/5823/1/marco-de-ciberseguridad-4.0-completo.pdf>. Acesso em: 29 maio 2019.

ARGENTINA. **Ciberdefensa - Ciberseguridad:** Riesgos y Amenazas. 2013. Disponível em: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf. Acesso em: 03 jun. 2019.

ARGENTINA. **Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas.** 2019. Disponível em: http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx. Acesso em: 03 jun. 2019.

ARGENTINA. **Decisión Administrativa 15/2015.** 2015. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/244566/norma.htm. Acesso em: 03 jun. 2019.

ARGENTINA. **Decreto 703/2018.** 2018. Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/189076/20180731. Acesso em: 03 jun. 2019.

ARGENTINA. **Dirección Nacional de Infraestructura Criticas de Información e Ciberseguridad.** 2016. Disponível em: https://www.argentina.gob.ar/modernizacion/infraestructuras-criticas-de-informacion-y-ciberseguridad/normativa. Acesso em: 03 jun. 2019.

ARGENTINA. **Ley 25.520 de Inteligencia Nacional.** 2001. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm. Acesso em: 03 jun. 2019

ARGENTINA. **Libro Blanco de la Defensa.**. Ministerio de Defensa, 2010.

ARGENTINA. **Livro Branco de Defesa.** 2015. Disponível em: <http://ceed.unasursg.org/Espanol/09-Downloads/Info-Pais/Arg/LB/Libro_blanco_2015.pdf>. Acesso em: 03 jun. 2019.

ARGENTINA. **Resolución 344/2014.** 2014. Disponível em: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-344-2014-229956. Acesso em: 03 jun. 2019.

ARGENTINA. **Resolución 580/2011.** 2011. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm. Acesso em: 03 jun. 2019.

ASSIS, Ana Carolina de Oliveira. **Política de Defesa Cibernética Brasileira: Um Mapeamento dos Atores e Processos.** 2018. Disponível em: <https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/XV

_cadn/politica_de_defesa_cibernetica_brasileira_um_mapeamento_dos_atores_e_processos.pdf>. Acesso em: 03 jun. 2019.

AROCENA, Gustavo A. **La regulación de los delitos informáticos en el Código Penal argentino:** Introducción a la Ley Nacional núm. 26.388. Boletín mexicano de derecho comparado, v. 45, n. 135, p. 945-988, 2012.

AYRES PINTO, Danielle Jacon. **SEGURANÇA E DEFESA CIBERNÉTICA: DESAFIOS E PERSPECTIVAS PARA OS PAÍSES DA AMÉRICA DO SUL.** 2017. Disponível em: <http://www.encontro2017.abri.org.br/resources/anais/8/1499705250_ARQUIVO_SegurancaeDefesaCibernetica-DanielleJaconAyresPInto.pdf>. Acesso em: 03 jun. 2019.

BARANIUK, Chris. **The cyber-attack that sent an Alaskan community back in time.** 2019. Disponível em: <http://www.bbc.com/future/story/20190108-the-cyber-attack-that-sent-an-alaskan-community-back-in-time>. Acesso em: 03 jun. 2019.

BRASIL. **Decreto nº 8793/2016.** 2016 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em: 03 jun. 2019.

BRASIL. **Doutrina Militar de Defesa Cibernética.** 2014. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 03 jun. 2019.

BRASIL. **Estratégia Nacional de Defesa.** 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 03 jun. 2019.

BRASIL. **Estratégia Nacional de Defesa.** 2012. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 03 jun. 2019.

BRASIL. **Estratégia Nacional de Defesa.** 2016. Disponível em: <https://www.defesa.gov.br/arquivos/2017/mes03/pnd_end.pdf>. Acesso em: 03 jun. 2019.

BRASIL. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal.** 2015. Disponível em: http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view. Acesso em: 03 jun. 2019.

BRASIL. **Estratégia Nacional de Segurança Cibernética (E-Ciber).** 2019. Disponível em: http://www.participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber. Acesso em: 03 jun. 2019.

BRASIL. **Livro Branco de Defesa Nacional.** 2012. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/livrobranco.pdf>. Acesso em: 03 jun. 2019.

BRASIL. **Livro Branco de Defesa Nacional.** 2017

BRASIL. **Livro verde: segurança cibernética no Brasil.** Brasília: GSIPR/SE/DSIC, v. 1, p. 5-15, 2010.

BRASIL. **Política Nacional de Defesa.** 2012. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 03 jun. 2019.

DA CRUZ JÚNIOR, Samuel César. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Texto para Discussão, Instituto de Pesquisa Econômica Aplicada (IPEA), 2013.

DE LIMA, MARIA REGINA SOARES et al. ATLAS DA POLÍTICA BRASILEIRA DE DEFESA. **Atlas da Política Brasileira de Defesa**, 2017.

DEMCHAK, Chris C.; DOMBROWSKI, Peter. **Rise of a cybered westphalian age**. AIR UNIV MAXWELL AFB AL STRATEGIC STUDIES QUARTERLY, 2011.

FINKLE, J.; SKARIACHAN, D. **Target cyber breach hits 40 million payment cards at holiday peak.** Retrieved January, v. 23, p. 2019, 2013.

GALINEC, Darko; MOŽNIK, Darko; GUBERINA, Boris. **Cybersecurity and cyber defence:** national level strategic approach. Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, v. 58, n. 3, p. 273-286, 2017.

GOLDSMITH, Jack. **How cyber changes the laws of war.** European Journal of International Law, v. 24, n. 1, p. 129-138, 2013.

GOMES, Helton Simões. **Exército brasileiro incluirá Argentina em treinamento de guerra cibernética.** 2014. Disponível em: http://g1.globo.com/tecnologia/noticia/2014/05/exercito-brasileiro-incluira-argentina-em-treinamento-de-guerra-cibernetica.html. Acesso em: 03 jun. 2019.

GUEDES, Marcos et al. **Guia de defesa cibernética na América do Sul.** Recife: UFPE, 2017.

GONZALES, Selma Lúcia; PORTELA, Lucas Soares. **A GEOPOLÍTICA DO ESPAÇO CIBERNÉTICO SUL-AMERICANO:** (IN) CONFORMAÇÃO DE POLÍTICAS DE SEGURANÇA E DEFESA CIBERNÉTICA?. AUSTRAL: Brazilian Journal of Strategy & International Relations, v. 7, n. 14.

HANSEN, Lene; NISSENBAUM, Helen. **Digital disaster, cyber security, and the Copenhagen School.** International studies quarterly, v. 53, n. 4, p. 1155-1175, 2009.

KUEHL, Daniel T.. **From Cyberspace to Cyberpower:** Defining the Problem. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K.. Cyberpower and National Security. Washington: University Of Nebraska Press, Potomac Books, 2009. p. 24-42

LASSERE, Pablo Edgardo Campos. **CIBERDEFENSA Y CIBERSEGURIDAD:** NUEVAS AMENAZAS A LA SEGURIDAD NACIONAL, ESTRUCTURAS NACIONALES DE CIBERDEFENSA, ESTRATEGIAS DE CIBERSEGURIDAD Y COOPERACIÓN INTERAGENCIAS EN ESTE ÁMBITO. 2016.

LOBATO, Luisa Cruz; KENKEL, Kai Michael. **Discourses of cyberspace securitization in Brazil and in the United States.** Revista Brasileira de Política Internacional, v. 58, n. 2, p. 23-43, 2015.

LOPES, Gills Vilar. **RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI): UMA DEFESA ACADÊMICA A PARTIR DOS ESTUDOS DE SEGURANÇA INTERNACIONAL.** 2016. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/20723/1/GillsVilarLopes-Tese-CiberRI-PPGCP-UFPE%20%281%29.pdf>. Acesso em: 03 jun. 2019.

MAZIERO, Arthur C.; AYRES PINTO, Danielle Jacon. **Poder cibernético e o espaço internacional:** uma perspectiva a partir das Teorias das Relações Internacionais. 2019.

MEDEIROS FILHO, Oscar. 2014. **"Em busca de ordem cibernética internacional".** In Segurança e Defesa Cibernética: da fronteira física aos muros virtuais, organized by Oscar Mederios Filho, Walfredo B. Ferreira Neto and Selma Lúcia de Moura Gonzalez. Coleção I - Defesa e Fronteiras Cibernéticas Pernambuco: Editora UFPE.

MINISTÉRIO DA DEFESA. **Política Cibernética de Defesa.** 2012. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf>. Acesso em: 03 jun. 2019.

NAKASHIMA, Ellen; WARRICK, Joby. **Stuxnet was work of US and Israeli experts, officials say.** Washington Post, v. 2, p. 13, 2012.

NYE JR, Joseph S. **Cyber power**. HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, 2010.

OEA; BID. **¿Estamos preparados en América Latina y el Caribe?** Washington: OEA, 2016. Disponível em: https://publications.iadb.org/handle/11319/7449?locale-attribute=es&. Acesso em: 03 jun. 2019.

REARDON, Robert; CHOUCRI, Nazli. **The Role of Cyberspace in International Relations: A View of the Literature.** 2012. Disponível em: <https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf>. Acesso em: 03 jun. 2019.

SCHMITT, Michael N. (Ed.). **Tallinn manual on the international law applicable to cyber warfare**. Cambridge University Press, 2013.

SYMANTEC. **Internet Security Threat Report.** 2019.

URUGUAY. **Administración Pública. Política de Seguridad de la Información.** 2009. Disponível em: <http://www.impo.com.uy/bases/decretos/452-2009>. Acesso em: 03 jun. 2019.

URUGUAY. **Aprobacion de la propuesta en materia de Politica de Defensa Nacional.** 2014. Disponível em: <http://www.impo.com.uy/bases/decretos/105-2014>. Acesso em: 03 jun. 2019.

URUGUAY. **Apruébase la propuesta en materia de Política de Defensa Nacional.** 2014. Disponível em: https://www.impo.com.uy/bases/decretos-originales/105-2014. Acesso em: 03 jun. 2019.

URUGUAY. **Decreto N° 451/009.** 2008. Disponível em: https://www.impo.com.uy/bases/decretos/451-2009/8. Acesso em: 03 jun. 2019.

URUGUAY. **LA DEFENSA NACIONAL.** APORTES PARA UN DEBATE. 2005. Disponível em: https://www.resdal.org/Archivo/uru-libro-blanco.htm. Acesso em: 03 jun. 2019.

URUGUAY. **Situación de la Ciberdefensa.** 2017. Disponível em: http://www.centromilitar.org.uy/Servicios/RevistaElSoldado/RevistaElSoldado192.pdf. Acesso em: 03 jun. 2019.

VENTRE, Daniel. **Seguridad global y potências emergentes em um mundo multipolar**. Ciberguerra. In: Academia General Militar. XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza, 2011.

WELCH, Larry D. **Cyberspace–The Fifth Operational Domain.** IDA Research Notes, p. 2-7, 2011.