AÇÃO MULTILATERAL NO ESPAÇO CIBERNÉTICO: A COOPERAÇÃO ENTRE BRASIL E ARGENTINA EM DEFESA CIBERNÉTICA

MULTILATERAL ACTION ON CYBERSPACE: THE COOPERATION BETWEEN BRAZIL AND ARGENTINA ON CYBER DEFENSE

CAMILA MARQUES DE OLIVEIRA[1]

Centro de Ensino Universitário do Distrito Federal - UDF
E-mail: camilamarquesoliveira@outlook.com

Resumo: Este trabalho busca analisar a importância da ação multilateral entre Estados no que diz respeito às respostas a ataques cibernéticos, pois a maioria dos ataques cibernéticos é transfronteiriço, podendo afetar todos os atores do espaço cibernético e, dessa forma, a troca de informações e experiências entre Estados pode beneficiá-los a evitar danos maiores. Foi apresentado, de forma geral, como os países da América do Sul têm lidado com essas ameaças e foi feita a descrição, baseada em *sites* do governo e nas respostas de um questionário elaborado pela autora e respondido pelo Centro de Defesa Cibernética (CDCiber), da cooperação entre Brasil e Argentina nesta seara. Em termos metodológicos, o artigo baseou-se na revisão de literatura de teorias das Relações Internacionais e temas atinentes à segurança e defesa cibernética, além de pesquisas em *sites* do governo e relatórios de organizações internacionais. Por fim, conclui-se que a cooperação internacional é a melhor maneira de se assegurar o espaço cibernético.

Palavras-chave: Segurança cibernética. Defesa cibernética. Cooperação internacional. Brasil e Argentina.

Abstract: This article seeks to analyze the multilateral action among states concerning responses to cyberattacks, since most cyberattacks are cross-border, can affect all the cyberspace actors and, therefore, the exchanges of information and experiences among states can benefit them in order to prevent greater damages. It was presented, in general terms, how South America countries have dealt with those threats and it was done the description, based on the responses of a questionnaire elaborated by this article's author and answered by the Cyber Defense Center (CDCiber), of the cooperation between Brazil and Argentina on this field. In methodological terms, this article was based on the bibliographical review of international relations theories and issues related to cybersecurity and cyber defense. Finally, one can conclude that the international cooperation is the best way to secure the cyberspace.

Key-words: Cyber Defense. International cooperation. Brazil and Argentina.

[1] Graduada em Relações Internacionais.

INTRODUÇÃO

O espaço cibernético é caracterizado por suas inerentes vulnerabilidades, sendo algumas delas: a possibilidade de qualquer um de seus atores – Estados, organizações e indivíduos – realizar um ataque cibernético; a dificuldade de imputar um ataque cibernético, uma vez que todos são feitos de forma anônima; o baixo custo de se realizar um ataque cibernético; o fato de este espaço não possuir fronteiras, portanto os ataques cibernéticos podem ser transfronteiriços, e a dificuldade de regular este espaço. Devido a essas vulnerabilidades, enfrentadas por diferentes tipos de Estado, alguns têm optado pela securitização do espaço cibernético.

Além disso, este espaço é considerado um bem comum global – como o mar, a Antártida e o espaço exterior –, que não pertence a um Estado, mas a todos, fato este que enfatiza a necessidade da cooperação internacional para que a utilização deste seja assegurada para todos. Assim sendo, o presente artigo apresenta como problema a seguinte pergunta: qual é a importância da ação multilateral no que diz respeito às respostas a ataques cibernéticos?

Para responder a essa pergunta foi elaborada a seguinte hipótese: a maneira mais eficiente de responder a um ataque cibernético é por meio da ação multilateral. Pois pelo fato de o espaço cibernético ser considerado um bem comum global, todos os Estados devem cooperar para assegurar a utilização deste espaço por todos os atores e, tendo em vista que os ataques cibernéticos podem atravessar fronteiras, e envolver atores de diversos países, o mais eficiente é respondê-los através da ação multilateral, por meio do compartilhamento de informações, experiências, por meio da cooperação internacional.

Como exemplo, pode-se citar o caso da Estônia, que em 2008 sofreu diversos ataques cibernéticos em *sites* de seu Parlamento, do Primeiro-Ministro, do Presidente, em *sites* jornalísticos e, inclusive, um banco recebeu ataques cibernéticos, causando uma perda de mais de um milhão de dólares a ele. Diante desta situação, a Organização do Tratado do Atlântico Norte (OTAN) – organização da qual a Estônia é Estado-membro – criou um centro para lidar com guerra cibernética, ou seja, não se tratou de uma resposta unilateral, mas de uma resposta coletiva dos Estados-membros da OTAN, pois, naquele momento, considerou-se que foi acionado o pacto de segurança coletiva dessa organização (SHACKELFORD, 2009).

Neste trabalho, a cooperação entre Brasil e Argentina é adotada como estudo de caso pelo fato de a Argentina ter sido o primeiro país cooperante, da América do Sul, com o Brasil, nesta seara de defesa cibernética. Além disso, há algumas pesquisas relacionadas à segurança e à defesa do espaço cibernético, porém, carentes são aquelas que versem sobre a importância da cooperação em defesa do espaço cibernético. Assim, esse estudo justifica-se na medida em que despertou interesse de analisar essa importância. Entende-se ainda que, divulgar essa relação pode contribuir para formulações mais eficientes de políticas públicas na seara de cooperação para a defesa cibernética.

Para a descrição dessa cooperação bilateral, foram consideradas notícias de diversos *sites*, dentre eles, o do Ministério da Defesa e do Centro de Defesa Cibernética do Exército (CDCiber), e as respostas de um questionário sobre a cooperação entre Brasil e Argentina em defesa cibernética respondido pelo CDCiber.

O presente artigo encontra-se estruturado em três seções e algumas subseções. A primeira seção busca ambientar o leitor no tema de segurança e defesa cibernética, apresentando, dessa forma, os principais conceitos de espaço cibernético, segurança e defesa cibernética. São apresentados também alguns ataques cibernéticos relatados que alguns países sofreram. Na segunda seção, é discutida a possibilidade de se considerar o espaço cibernético como um bem comum global securitizado. E na última seção, é apresentado, de uma forma geral, como os países da América do Sul têm lidado com a proteção do espaço cibernético, e é feita uma descrição da cooperação bilateral entre Brasil e Argentina em defesa cibernética.

1. ESPAÇO CIBERNÉTICO

O espaço cibernético não é um espaço natural – como o mar, o espaço exterior –, mas um espaço criado pelo homem, que nasce em 1969, a partir da conexão de quatro dispositivos centrais (PORTELA, 2016).

Vale mencionar que ele foi criado com o objetivo de facilitar a difusão de informações e intercomunicações (KUEHL, 2009). Trata-se de um objeto de estudo que tem ligações desde a ciência da computação até as ciências sociais (PORTELA, 2016), pois além de

envolver *hardwares* e *softwares*, envolve uma camada chamada por Ventre (2012) de *peopleware*, na qual está a parte cognitiva do usuário, além de dados bancários, dados pessoais, ou seja, informações que podem impactar a sociedade como um todo.

O Ministério da Defesa brasileiro definiu este espaço como um

> [e]spaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas. Ações ofensivas no espaço cibernético podem impactar, inclusive, a segurança nacional (BRASIL, 2010 apud CARVALHO, 2011, p.17).

Vale mencionar, também, a transversalidade do espaço cibernético, pois um ataque nele pode impactar os outros espaços convencionais (aéreo, terrestre, marinho). Destaca-se que tanto um ator estatal quanto um ator não estatal pode cometer os mesmos crimes cibernéticos, dificultando a imputação de um ataque cibernético (VENTRE, 2012).

Joseph Nye (2010) divide os atores do espaço cibernético em três categorias: governos, organizações com redes altamente estruturadas e indivíduos. Destaca também que o baixo custo de se cometer um ataque cibernético é um fator permissivo para que pequenos Estados e atores não estatais tenham um papel significativo nesse ambiente. Nye (2010) também comenta sobre a dificuldade de afirmar que determinado Estado é dominante no espaço cibernético, como alguns o são no mar ou no ar, pois mesmo aqueles Estados que tenham consideráveis recursos de *soft* e *hard power*, estão lidando com novos atores e com novos desafios inerentes ao espaço cibernético.

Ademais, mesmo que alguns países possuam leis nacionais que tipifiquem o crime, ainda não há um tratado internacional abrangente que lide com os crimes e criminosos atuantes no espaço cibernético. Trata-se de um entrave a este tipo de punição, pois, na maioria das vezes, os ataques cibernéticos são provenientes de outros Estados, e a inexistência de um tratado desse tipo dificulta a punição aos respectivos criminosos (KRAMER, 2009).

O maior tratado internacional feito acerca do tema foi a Convenção de Budapeste, que foi elaborada em 2001, no âmbito do Conselho da Europa. Dos países da América do Sul, somente a Argentina e o Chile ratificarem este tratado, porém, apesar de não ser tão

abrangente, ele reconhece a importância da cooperação internacional na luta contra os crimes cibernéticos (Convenção de Budapeste, 2001).

Por fim, frisa-se a importância de se proteger o espaço cibernético, para que as infraestruturas críticas nacionais sejam asseguradas, pois

> [u]m ataque de grandes proporções poderia fazer com que informações detalhadas sobre planos militares vazassem para as mãos de grupos ou Estados inimigos, debilitando as estratégias do Exército, além de poder causar o bloqueio de dados bancários e interferir na bolsa de valores. Sistemas de transporte e de saúde também poderiam entrar em colapso ao serem violados em um ataque (MIRANDA, 2009).

Além disso, vale mencionar a importância da cooperação entre o setor público e o setor privado, pois, de acordo com Meyer (2016), a maior parte das infraestruturas do espaço cibernético pertencem ao setor privado, fato esse que reitera a importância da cooperação entre esses dois setores.

2.1 Segurança e defesa cibernética

A segurança cibernética tem como fundamento geral garantir a segurança pública no espaço cibernético, tentado proteger o espaço cibernético contra os ilícitos nacionais e internacionais e evitando que os atores que utilizam este espaço tenham seus dados violados ou disseminados por criminosos que neste espaço atuam. Carvalho (2011) define a segurança cibernética como

> [a] proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF) (CARVALHO, 2011).

Vale mencionar que as infraestruturas críticas são "instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional e à segurança do Estado e da sociedade" (BRASIL, 2009). Portanto,

destaca-se também a importância de garantir a segurança das infraestruturas críticas de um Estado, e essa segurança é feita por meio da segurança cibernética, garantindo que o Estado assegure, sobretudo, sua soberania nacional (JÚNIOR, 2013).

Já a defesa cibernética está no âmbito das relações entre os Estados, envolvendo o poder cibernético e a guerra cibernética. O ministério da defesa brasileiro a define como um

> [c]onjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética (BRASIL, 2010 apud CARVALHO, 2011, p.18).

Dessa forma, a defesa cibernética é acionada quando o Estado sofre um ataque cibernético, por exemplo, em suas infraestruturas críticas nacionais e deve responder, de forma defensiva e ofensiva, podendo levar à guerra cibernética. Na próxima subseção serão apresentados alguns ataques cibernéticos cometidos a Estados.

2.2 Ataques cibernéticos

Os ataques cibernéticos da Rússia à Estônia, em 2007, e à Geórgia, em 2008, contribuíram para a inserção do tema de segurança cibernética na agenda internacional (LOBATO; KENKEL, 2015). Ainda, em 2010, um vírus chamado *Stuxnet* foi instalado nas instalações nucleares iranianas, tendo como objetivo danificar as centrífugas do programa nuclear iraniano (LOBATO; KENKEL, 2015b).

Em 2012, os Estados Unidos da América (EUA) afirmaram a obtenção não autorizada da China ao *design* e às informações do caça estadunidense F-35, dessa forma podendo criar mecanismos e proteger-se contra este (LIPINSKI, 2012).

Foi revelado, em 2013, pelo Edward Snowden, ex-técnico em segurança digital da *Central Intelligence Agency* (CIA), que os EUA estavam monitorando, bem como, interceptando *e-mails*, de diversos cidadãos e até de chefes de governos – o que foi o caso da descoberta de intercepção de e-mails e chamadas telefônicas da ex-presidente Dilma Rousseff (BBC,

2014). Foi nesse momento que se percebeu uma relevância maior dado pelo Brasil ao tema de segurança e defesa cibernética, por meio da assinatura de diversos tratados de cooperação, por exemplo.

Já em 2014, alguns *sites* da OTAN sofreram ataques de negação de serviço (*Distributed Denial of Service* - DDoS) – que têm como objetivo exceder os limites de requisição de um servidor – por consequência da crise da Crimeia (LOBATO; KENKEL, 2015b) e em 2016, o *Federal Bureau of Investigation* (FBI) percebeu que as eleições estadunidenses foram alvo de *hackers* (GROLL, 2016).

Vale lembrar também do ataque cibernético do tipo *ransomware* que atingiu o Serviço Nacional de Saúde da Inglaterra, em 2017, no qual foram paralisados computadores e telefones de 16 hospitais de três regiões da Inglaterra. Além da Inglaterra, esse vírus afetou mais de 150 países (EL PAÍS, 2017).

Assim sendo, a partir desses ataques pode-se perceber que as consequências que eles causam não ficam somente no plano virtual, atingindo o plano real e ameaçando a segurança nacional dos Estados. Além disso, é importante ressaltar que o poder cibernético é mais difuso no sistema internacional, podendo ser exercido por qualquer ator dele. Dessa forma, é notória a necessidade da ação multilateral no espaço cibernético, pois a partir da troca de informações e experiências, pode-se facilitar a localização dos criminosos, bem como sua punição.

3. O ESPAÇO CIBERNÉTICO SECURITIZADO

A Escola de Copenhague defende que a agenda de segurança internacional pode ser expandida para além de assuntos militares, podendo tratar, também, de ameaças que podem atingir os setores ambiental, societal e econômico. Essa expansão propicia um tratamento especial – no que diz respeito à formulação de respostas adequadas na área da segurança e defesa – àqueles assuntos que antes não eram vistos como pertencentes ao campo da segurança internacional. Um exemplo disso é a securitização do espaço cibernético.

Tendo em vista os ataques cibernéticos sofridos por diversos Estados, alguns têm optado pela securitização do espaço cibernético, ou seja, eles têm tratado o espaço cibernético como uma ameaça existencial, que requer medidas emergenciais e que justifica a tomada de ações que não estão dentro dos limites dos processos políticos (BUZAN ET AL, 1998). Outro fator determinante que influencia o processo de securitização é o discurso dos atores securitizantes – aqueles que securitizam determinada questão ao tratar algum objeto de referência como ameaçado –, pois

> [u]m discurso que assume a forma de apresentar algo como uma ameaça existencial a um objeto de referência não cria, por si só, a securitização - esse é um movimento securitizador, mas a questão é securitizada somente se e quando o público a aceitar como tal (BUZAN ET AL, 1998, p. 25, tradução nossa)[2].

Dessa forma, o processo de securitização depende também do discurso, e Buzan et al (1998) assinala que a palavra 'segurança' nem precisa ser dita nesse discurso, pois o essencial é designar uma ameaça existencial que requer ações emergenciais ou medidas especiais, além da aceitação dessa designação por um público. Assim, pode-se perceber que a securitização é socialmente construída. Ainda, Buzan et al (1998) assinala que "uma securitização bem-sucedida não é decidida pelo securitizador, mas pelo público do discurso de segurança [...]" (p.31, tradução nossa)[3].

Dessa forma, esse artigo utilizará o modelo feito por Hare (2010), que se baseou na estrutura do livro de Buzan (1991) "*People, States and Fear*", para categorizar as vulnerabilidades do espaço cibernético. Menciona-se que a estrutura de Buzan classifica as ameaças à segurança nacional vistas por tipos de Estados diferentes (HARE, 2010).

Os agentes que causam ameaças no espaço cibernético são terroristas, hackers, Estados e criminosos cibernéticos. Suas vítimas podem ser os próprios Estados, indivíduos, empresas, instituições (HARE, 2010). Vale mencionar que

> [e]m casos onde cidadãos individuais lidam com um risco existencial ao seu bem-estar, ou diretamente ou através de uma perda de instituições estatais, uma

[2] Em inglês, "*A discourse that takes the form of presenting something as an existential threat to a referent object does not by itself create securitization —this is a securitizing move, but the issue is securitized only if and when the audience accepts it as such*".

[3] Em inglês, "*Successful securitization is not decided by the securitizer but by the audience of the security speech act*".

> justificativa para a ação pública pode ser feita porque defesa nacional é considerada um bem público. Políticos, são, portanto, motivados a securitizar ameaças a cidadãos individuais, porque eles são responsáveis por representar seus interesses constituintes (HARE, 2010, p.213, tradução nossa)[4].

Dessa forma, Hare (2010), utilizando o modelo de Buzan et al (1998), analisa as vulnerabilidades cibernéticas de acordo com o tipo de poder e coesão sócio-política – classificados em forte ou fraco – de cada Estado, conforme demonstrado na Tabela 1. Assim, a partir do quadrante que determinado Estado ocupar, este tomará diferentes medias e políticas públicas.

Tabela 1 - Vulnerabilidades cibernéticas e tipos de Estados

		Coesão sócio-política	
		Fraco	Forte
Poder	Fraco	Desestabilizar ações políticas no espaço cibernético, ataques a infraestrutura da Internet, atividades criminosas	DDoS e outros maiores ataques na infraestrutura crítica
	Forte	Ações políticas desestabilizadoras no espaço cibernético	Atividades criminais no espaço cibernético

Fonte: HARE, 2010, p.218, tradução nossa.

Assim, o Estado que possui poder e coesão sócio-política fraca estará preocupado com a maior parte das ameaças presentes no espaço cibernético e as estruturas governamentais desses Estados geralmente não possuem *expertise* suficiente para lidar com essas ameaças (HARE, 2010).

[4] Em inglês, "*In cases where the identified victim is the state and its institutions, the existential threat may be one of toppling the regime or one from break-away sections of the country. In cases where individual citizens face an existential risk to their welfare, either directly or through a loss of state institutions, a justification for public action can be made because national defense is considered a public good. Politicians are therefore motivated to securitize threats to individual citizens because they are charged to represent their constituents' interests*".

Já Estados que possuem poder e coesão sócio-política fortes têm a capacidade de manter forças militares e econômicas mais fortes no sistema internacional e são, dessa forma, mais relutantes a securitizar ameaças no espaço cibernético. Vale mencionar que nesses Estados, geralmente, a segurança cibernética permanece como uma responsabilidade do setor privado, e eles são um dos mais dependentes do espaço cibernético (HARE, 2010).

Aqueles com poder fraco e coesão sócio-política forte são vulneráveis à maioria das ameaças das forças militares, porque sua infraestrutura e populações são mais suscetíveis a ataques militares. Ainda, os países que estão neste quadrante, são desenvolvidos e utilizam o *e-governance*, por isso são vulneráveis a ataques cibernéticos (HARE, 2010).

Por fim, os Estados com poder forte e coesão sócio-política fraca são aqueles com forças militares fortes e fraca coesão sociocultural, são países que limitam o acesso à informação e à utilização do ambiente cibernético e, portanto, estão mais preocupados com as consequências que a propagação de informações pode causar na coesão interna desses Estados (HARE, 2010).

Por fim, Hare (2010) enfatiza a importância de os Estados formarem alianças de securitização, pois muitas vezes eles lidam com as mesmas ameaças e podem se esforçar para securitizá-las.

3.1 O espaço cibernético como um bem comum global

Alguns autores consideram o espaço cibernético como um bem comum global, ou seja, como um bem que não é controlado por um Estado em particular e que pode ser usufruído pelos Estados, indivíduos e organizações (MURPHY, 2010). Menciona-se que os outros bens comuns globais são o mar, o espaço exterior, o ar e a Antártida. Por se tratarem de bens comuns, há a importância da regulação desses bens por meio de acordos e tratados internacionais como, por exemplo, a Convenção das Nações Unidas do Direito do Mar que regula o comportamento dos Estados nesse bem comum global.

Porém, o espaço cibernético ainda não possui um tratado ou acordo que regulamente a atuação de seus atores, pois, além da dificuldade inerente de se regulamentar um bem

comum global, deve-se destacar que a maior parte do espaço cibernético pertence ao setor privado. Murphy (2010) comenta que

> [o] espaço cibernético é o domínio mais singular dos bens comuns globais: é feito pelo homem; facilita a transferência de informação e dados em vez de pessoas, navios e mercadorias; e é em grande parte controlado pelo setor privado (p.40, tradução nossa)[5].

Por isso deve-se também enfatizar a importância da cooperação entre o setor público e o setor privado no que diz respeito à coordenação de respostas a ameaças e a ataques cibernéticos (MEYER, 2016).

Outra variável que explica a importância da regulamentação do espaço cibernético é a necessidade de dificultar a ocorrência da Tragédia dos Bens Comuns – que acontece quando os indivíduos buscam maximizar seu autointeresse em detrimento dos interesses da sociedade como um todo, enquanto exploram um bem comum (MURPHY, 2010) –, pois ao ter sua confiança sobre-explorada nesse espaço, o usuário tem sua confiança e bem-estar diminuídos. Dessa forma, deve-se cooperar no espaço cibernético, para que se evite a ocorrência da Tragédia dos Bens Comuns e seja assegurado o bem-estar dos atores deste espaço (HURWITZ, 2012).

Tendo em vista isso, questionou-se a possibilidade de se considerar o espaço cibernético como um bem comum global securitizado. Porventura, a securitização do espaço cibernético possa contribuir na sua manutenção como um bem comum global, pois medidas extraordinárias seriam autorizadas e tomadas, assegurando a utilização desse bem por todos seus usuários. Assim, esse tema será melhor defendido no próximo tópico.

3.2 O espaço cibernético como um bem comum global securitizado

Devido às vulnerabilidades inerentes ao espaço cibernético – facilidade e baixo custo de se realizar um ataque cibernético a qualquer um de seus atores; dificuldade de imputar um ataque cibernético; facilidade de realizar um ataque sob garantia de anonimato; falta de

[5] Em inglês, "*cyberspace is the most unique domain of the global commons: it is manmade; it facilitates the transfer of information and data rather than people, vessels, and goods; and it is in large part owned by the private sector*".

regulamentação deste bem comum – e por se tratar de uma ameaça existencial, alguns Estados têm optado pela securitização desse espaço.

Assim sendo, alguns Estados têm buscado lidar com ataques cibernéticos de diversas maneiras, a partir da cooperação internacional, instituições, estabelecimento de políticas, para que, dessa forma, possa ser assegurado o bem-estar dos usuários, a segurança nacional. Além disso, vale mencionar que tanto a teoria da securitização quanto a dos bens comuns globais prevê a necessidade de se assegurar o bem-estar dos usuários do espaço cibernético, e a teoria dos bens comuns globais defende a importância da cooperação internacional para que a Tragédia dos Bens Comuns não aconteça.

Dessa maneira, conclui-se que a securitização do espaço cibernético contribui para que esse seja mantido como um bem comum global, pois a partir do momento que se toma medidas para lidar com os ataques cibernéticos, o espaço cibernético está sendo assegurado, e dentre essas medidas, enfatiza-se a importância da ação multilateral. Forsyth Junior (2013) defende que

> [o] espaço cibernético de fato coloca desafios à ordem internacional, mas esses desafios não tornam a cooperação improvável, pelo contrário, eles tornam a cooperação inevitável (p.95, tradução nossa)[6].

Assim, com o objetivo de reforçar a tese de que a cooperação internacional é fundamental para o combate aos crimes cibernéticos, no próximo tópico será feito um breve panorama das políticas que os países da América do Sul têm adotado para o combate desses crimes e será apresentado o caso da cooperação entre o Brasil e a Argentina.

4. POLÍTICAS ADOTADAS PELOS PAÍSES DA AMÉRICA DO SUL

A América do Sul é considerada, pela Política Nacional de Defesa de 2012, parte do entorno estratégico brasileiro. Em 2004, foi aprovado, na assembleia geral da Organização dos Estados Americanos (OEA), um documento com o título "Estratégia Interamericana Integral para Combater as ameaças à segurança cibernética", a qual destacou a relevância da constituição de Equipes de Respostas a Incidentes de Segurança em Computadores (*Computer Security Incident Response Teams* - CSIRTs) nacionais. As CSIRTs são

[6] Em inglês, "*Cyberspace does indeed pose challenges to international order, but those challenges do not make cooperation unlikely; on the contrary, they make cooperation inevitable*".

capazes de responder de forma rápida a crises e ameaças cibernéticas, e permitem uma melhor comunicação entre outras equipes de outros Estados. Ressalte-se também que

> [a] adoção de uma estratégia de segurança cibernética nacional é possivelmente um dos elementos mais importantes do compromisso de um país em assegurar a infraestrutura cibernética, serviços e ambiente de negócios dos quais dependem seu futuro digital e bem-estar econômico (OEA; BID, 2016, p.115, tradução nossa)[7].

Em 2012, as preocupações regionais em relação à defesa cibernética ganharam destaque, levando à formação de um Grupo de Trabalho (GT) no âmbito do Conselho de Defesa Sul Americana da União Sul-Americana de Nações (Unasul) que tivesse como objetivo criar políticas regionais para combater as ameaças cibernéticas (CDS, 2012).

Em 2013, frente à espionagem da NSA, o Mercosul emitiu uma nota na qual ressaltava a importância de os países do bloco trabalharem juntos para garantir a segurança cibernética deles (MERCOSUL, 2013). Na mesma época, a Unasul emitiu a Declaração de Paramaribo na qual rejeitou a espionagem feita pela NSA e ainda destacou que essas ações "[...] constituem uma ameaça à segurança e graves violações dos direitos humanos, civis e políticos, do direito internacional e da nossa soberania e que prejudicam as relações entre as nações" (UNASUL, 2013, p.8). Além disso, essa Declaração apoiou a criação de projetos de cooperação regionais ligados à defesa cibernética.

No âmbito bilateral, em 2013, os Ministros do Brasil e da Argentina assinaram a Declaração de Buenos Aires, na qual foi estabelecida a criação de um Subgrupo de Cooperação entre os dois países que tratasse de defesa cibernética.

Nos planos de ação do CDS de 2014, 2015, 2016 e 2017 foram reiterados o desejo de se continuar com o grupo de trabalho em defesa cibernética, bem como a importância da cooperação regional em torno deste tema. Ainda, na Declaração de Brasília sobre Segurança nas Fronteiras de 2016, foi ressaltada a importância da ação conjunta dos Estados da América do Sul no combate aos crimes cibernéticos.

[7] Em espanhol, "*La adopción de una estrategia de seguridad cibernética nacional es posiblemente uno de los elementos más importantes del compromiso de un país en asegurar la infraestructura cibernética, servicios y ambiente de negocios de los que dependen su futuro digital y el bienestar económico*".

Um relatório da OEA intitulado "*Cybersecurity: Are we ready in Latin America and the Caribbean?*" destaca que cada um dos países da América do Sul tem um órgão específico que lide com a segurança e defesa cibernética. Alguns deles possuem campanhas de conscientização à população sobre a importância da segurança cibernética, graduações em segurança cibernética, e mostra como as forças militares de cada país têm lidado. Analisando esse relatório percebeu-se que todos possuem uma CSRIT, porém nem todos possuem políticas ou estratégias de defesa cibernética. Ainda, cada país designou sua polícia nacional para lidar com crimes cibernéticos.

4.1 A cooperação em defesa cibernética entre Brasil e Argentina

A escolha da descrição da cooperação em defesa cibernética entre Brasil e Argentina foi motivada pelo fato de esses dois países já possuírem cooperação consolidada em algumas áreas da defesa como, por exemplo, no setor nuclear. Dessa forma, pretendeu-se analisar como essa parceria poderia contribuir para o setor de defesa cibernética. Menciona-se que essa subseção foi escrita a partir das respostas obtidas de um questionário enviado ao CDCiber e de pesquisas a *sites* do governo.

Destaca-se que após as revelações de espionagem realizadas pela NSA, o Brasil e a Argentina estabeleceram uma agenda de cooperação em defesa cibernética, resultando na assinatura da Declaração de Buenos Aires, que previu: a formação de um Subgrupo de Cooperação em Defesa Cibernética, na visita de oficiais argentinos ao CDCiber e no convite de oficiais argentinos para realizarem o curso de Guerra Cibernética que ocorreu no Brasil em 2014 e 2015.

Menciona-se, porém, que o CDCiber não considerou este caso como fator preponderante para o início dessa cooperação, pois a Diretriz para as Atividades do Exército Brasileiro na Área Internacional (DAEBAI) tem como objetivo realizar ações de cooperação e integração entre os países da América do Sul, então a cooperação em defesa cibernética era esperada.

O mencionado Subgrupo se reuniu em 2014 e 2015 com o objetivo de discutir questões como: Intercâmbio Doutrinário, Capacitação, Exercícios de Defesa Cibernética, Intercâmbio Operacional e Visitas Mútuas de Delegações.

Em 2014, um oficial argentino participou do Curso de Guerra Cibernética realizado no Brasil e, em contrapartida, um oficial brasileiro participou de um curso relacionado à segurança de rede e criptografia na Argentina. Vale mencionar que se tratou da primeira experiência entre os dois países no âmbito deste tema, e em maio de 2016, o governo brasileiro convidou a Argentina para participar do Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas, que foi ministrado pelo Centro de Instrução de Guerra Eletrônica (CIGE).

No mesmo ano, foi realizado, em Madri, o *Foro Iberoamericano de Ciberdefensa* no qual foi elaborada uma Carta de Intenções, com expectativas de que os países participantes – Argentina, Brasil, Chile, Colômbia, Espanha, México, Peru e Portugal – realizassem exercícios no âmbito da defesa cibernética. Assim sendo, em outubro de 2017, foi realizado em Brasília o I Exercício Ibero-Americano de Defesa Cibernética, onde estiveram reunidos militares da Argentina, Brasil, Colômbia, Espanha, México, Portugal e observadores do Peru (EXÉRCITO, 2017). As atividades foram realizadas no CIGE com o objetivo de estreitar as relações entre os países participantes. Ainda, foi destacada a importância da cooperação no que diz respeito ao combate de ataques neste espaço.

Enfim, vale mencionar os benefícios desta cooperação mencionados pelo CDCiber: fortalecimento da proteção cibernética de órgãos governamentais e infraestruturas críticas de ambos os países; possibilidade de cooperação acadêmica e industrial; e estabelecimento de medidas de construção de confiança em defesa cibernética.

CONCLUSÃO

O espaço cibernético não é domínio de nenhum Estado e, portanto, todos estão vulneráveis às ações de hackers maliciosos, independente de seus poderes militares ou econômicos, pois conforme demonstrado, todos os Estados lidam com vulnerabilidades inerentes a este espaço. Ainda, ataques cibernéticos podem atingir todos os atores desse espaço e se cometidos contra as infraestruturas críticas nacionais de determinado país, podem colocar em risco sua segurança nacional. Assim sendo, alguns países encaram esse espaço como uma ameaça existencial que necessita de políticas não convencionais, ou seja, tratam o espaço cibernético como securitizado.

Ainda, pelo fato de esse espaço não ser domínio de nenhum Estado, ele é considerado como um bem comum global, requerendo a cooperação internacional para que seja mantida a utilização desse espaço por todos os Estados, organizações e indivíduos. Destaca-se, também, a necessidade da cooperação e regulamentação do espaço cibernético, para evitar que a Tragédia dos Bens Comuns – quando um ator utiliza um bem comum global para maximizar seu autorinteresse – aconteça.

Vale mencionar que a ação multilateral pode ser realizada por meio do compartilhamento de informações entre Estados, maior integração das CSIRTs, pelas trocas de experiências, intercâmbios de profissionais, pela adoção de políticas comuns no combate aos crimes cibernéticos. Com o objetivo de destacar a importância da cooperação no espaço cibernético, apresentou-se um breve panorama de como os países da América do Sul têm lidado com as vulnerabilidades desse espaço para, então, descrever a cooperação entre Brasil e Argentina em defesa cibernética. Percebeu-se que esses dois países possuem uma cooperação significativa nesse tema e que eles têm trabalhado para fortalecê-la, além de não deixarem de tratar dele no âmbito regional.

Por fim, concluiu-se que, apesar de os Estados serem diferentes e de cada um lidar com tipos diversos de vulnerabilidades, a ação multilateral é a maneira mais eficiente de se responder às ameaças e crimes do espaço cibernético. Pois, conforme demonstrado alhures, ataques cibernéticos podem atingir diversos Estados, reiterando a necessidade da cooperação internacional.

REFERÊNCIAS

BBC. 2014. Edward Snowden: Leaks that exposed US spy programme. Disponível em: <https://www.bbc.com/news/world-us-canada-23123964>. Acesso em: 06 ago. 2018.

BRASIL. Gabinete de Segurança Institucional. Portaria nº 45, de 08 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Brasília, Disponível em: <https://www.legisweb.com.br/legislacao/?id=213726>. Acesso em: 06 ago. 2018.

BUZAN, B.; WAEVER, O.; WILDE, J. 1998. Security: A New Framework for Analysis. Colorado: Lynne Rienner Publishers.

CARVALHO, P. S. M. d. 2011. Conferência de Abertura: O Setor Cibernético nas Forças Armadas Brasileiras. In: BARROS, O. S. R.; GOMES, U. M.; FREITAS, W. L. (orgs.). Desafios estratégicos para a segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. pp. 13-34.

CDS. UNASUL. 2012. Plan de Acción CDS - 2012. Disponível em: <http://ceed.unasursg.org/Espanol/09-Downloads/Esp-PA/PA-CDS-2012.pdf>. Acesso em: 06 ago. 2018.

Convenção de Budapeste. 2001. Tratado nº 185, de 2001. Convention On Cybercrime. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>. Acesso em: 06 ago. 2018.

EL PAÍS. 2017. Cibertaque: o vírus WannaCry e a ameaça de uma nova onda de infecções. Disponível em: <http://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html>. Acesso em: 06 ago. 2018.

EXÉRCITO. 2017. Exercício Ibero-Americano de Defesa Cibernética promove Intercâmbio na Área de Segurança da Informação. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercicio-ibero-americano-de-defesa-cibernetica-promove-intercambio-na-area-de-seguranca-da-informacao->. Acesso em: 06 ago. 2018.

FORSYTH, J. J. W. 2013. What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace. Strategic Studies Quaterly, v. 7, n. 1, pp.93-113. Disponível em: <https://www.files.ethz.ch/isn/162442/spring_2013.pdf>. Acesso em: 06 ago. 2018.

GROLL, E. 2016. Spy Chief: Hackers Are Targeting Clinton and Trump Campaigns. Foreign Policy, mai. Disponível em: <https://foreignpolicy.com/2016/05/18/spy-chief-hackers-are-targeting-clinton-and-trump-campaigns/>. Acesso em: 06 ago. 2018.

HARE, F. 2010. The Cyber Threat to National Security: Why can't we agree? Paper apresentado na Conference on Cyber Conflict, Tallin. p. 211 - 225. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Hare%20-%20The%20Cyber%20Threat%20to%20National%20Security%20Why%20Cant%20We%20Agree.pdf>. Acesso em: 06 ago. 2018.

HURWITZ, R. 2012. Depleted Trust in the Cyber Commons. Strategic Studies Quarterly, v. 6, n. 3, pp.20-45. Disponível em: <http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2014/2014-3/2014_3_06_hurwitz_s_eng.pdf>. Acesso em: 06 ago. 2018.

JÚNIOR, S. C. C. 2013. A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual. Brasília: Ipea. Disponível em: <http://www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf>. Acesso em: 06 ago. 2018.

KRAMER, F. D. 2009. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). Cyberpower and National Security. Center For Technology & National Security Policy, pp. 1-18. Disponível em: <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-01.pdf>. Acesso em: 06 ago. 2018.

KUEHL, D. T. 2009. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). Cyberpower and National Security. Center For Technology & National Security Policy, pp. 1-17. Disponível em: <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf>. Acesso em: 06 ago. 2018.

LIPINSKI, Congressman Daniel. 2012. House Passes Lipinski-McCaul Cybersecurity Enhancement Act to Secure Federal Networks, Critical Infrastructure and America's Competitive Edge. Disponível em: <https://lipinski.house.gov/press-releases/house-passes-lipinskimccaul-cybersecurity-enhancement-act-to-secure-federal-networks-critical-infrastructure-and-americas-competitive-edge/>. Acesso em: 06 ago. 2018.

LOBATO, L.; KENKEL, K. M. 2015. A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra. Contexto internacional, v. 37, n. 2, pp. 629-660. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292015000200629&lng=en&nrm=isso>. Acesso em: 06 ago. 2018.

LOBATO, L.; KENKEL, K. M. 2015b. Discourses of cyberspace securitization in Brazil and in the United States. Revista brasileira política internacional, v. 58, n. 2, pp. 23- 43. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292015000200023&lng=en&nrm=isso>. Acesso em: 06 ago. 2018.

MERCOSUL. 2013. Decisión sobre el rechazo al espionaje por parte de los Estados Unidos sobre los países de la región. Disponível em: <http://www.mercosur.int/innovaportal/file/4506/1/decision_sobre_espionaje_es.pdf>. Acesso em: 06 ago. 2018.

MEYER, P. 2016. Outer Space and Cyberspace: A Tale of Two Security Realms. In: OSULA, A.; RÕIGAS, H. (Ed.). International Cyber Norms: Legal, Policy & Industry Perspectives. Tallin: Nato CCD COE Publications, 2016. cap. 8., pp. 155- 169. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch8.pdf>. Acesso em: 06 ago. 2018.

MIRANDA, R. 2009. EUA investem em defesa cibernética: Governo de Obama prevê investimento de US$ 355 milhões para tornar redes públicas e privadas mais seguras. O Estadão, mar. Disponível em: <https://internacional.estadao.com.br/noticias/geral,eua-investem-em-defesa-cibernetica,339088>. Acesso em: 06 ago. 2018.

MURPHY, T. 2010. Security Challenges in the 21st Century Global Commons. Yale Journal Of International Affairs. New Haven, Connecticut, pp. 28-43. Disponível em: <http://yalejournal.org/wp-content/uploads/2010/09/105205murphy.pdf>. Acesso em: 06 ago. 2018.

NYE, Joseph S. Jr. 2010. Cyber Power. Harvard Kennedy School, Belfer Center For Science And International Affairs, pp.1-24. Disponível em: <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>. Acesso em: 06 ago. 2018.

OEA; BID. 2016. Cybersecurity: Are We Ready in Latin America and the Caribbean?. Observatory Cybersecurity In Latin America And The Caribbean. Disponível em: <https://publications.iadb.org/handle/11319/7449>. Acesso em: 06 ago. 2018.

PORTELA, L. S. 2016. Agenda de Pesquisa sobre o Espaço Cibernético nas Relações Internacionais. Revista Brasileira de Estudos de Defesa, v. 3, n. 1, pp.91- 113. Disponível em: <https://rbed.abedef.org/rbed>. Acesso em: 06 ago. 2018.

SHACKELFORD, S. J. 2009. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley Journal Of International Law, v. 27, n. 1, pp.192-251. Disponível em: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1368&context=bjil>. Acesso em: 06 ago. 2018.

UNASUL. 2013. Declaração de Paramaribo, Aprovada na VII Reunião Ordinária do Conselho de Chefes de Estado e de Governo da União das Nações Sul-americanas. Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/2193-declaracao-de-paramaribo-aprovada-na-vii-reuniao-de-cupula-da-unasul>. Acesso em: 06 ago. 2018.

VENTRE, D. D. 2011. Ciberguerra. Paper apresentado no XIX Curso Internacional de Defensa, Seguridad Global y Potencias Emergentes em um Mundo Multipolar, Jaca, 2011. Catálogo General de Publicaciones Oficiales. Jaca: Ministerio de Defensa, 2012. pp. 32 - 45. Disponível em: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF48.pdf>. Acesso em: 06 ago. 2018.