Revista Latino-Americana de
RELAÇÕES INTERNACIONAIS
Campos Neutrais

FURG

A construção de capacidade cibernética na América do Sul

Jéssica Maria Grassi[1]

Danielle Jacon Ayres Pinto[2]

Resumo: A construção de capacidade cibernética tornou-se tema central de discussão à medida que o ciberespaço passou a impactar substancialmente o desenvolvimento e a segurança dos Estados. Diante disso, o objetivo central da pesquisa é analisar a inserção dos países sul-americanos no contexto da construção de capacidades cibernéticas. Esta é uma pesquisa exploratória, descritiva e analítica, que parte de revisão bibliográfica, analisando perspectivas teórico-conceituais sobre a temática, bem como dados disponíveis em importantes repositórios, como o Global Cybersecurity Index.

Palavras-chaves: Capacidade Cibernética; Segurança Cibernética; Defesa Cibernética.

Cyber capacity building in South America

Abstract: Cyber capacity building has become a central topic of discussion since cyberspace started impacting the development and security of states. Therefore, the main objective of this research is to analyze South American countries in the context of building cyber capacities. This is an exploratory, descriptive and analytical research, that starts from a bibliographic review, analyzing theoretical-conceptual perspectives on the subject, as well as data available in important repositories, such as the Global Cybersecurity Index.

Key words: Cyber Capacity; Cybersecurity; Cyber Defense.

Introdução

Nos últimos anos os recursos cibernéticos tornaram-se centrais nas relações internacionais, ao passo que o ciberespaço passou a impactar todas as esferas do desenvolvimento e da segurança dos Estados, possuindo um papel protagônico na política internacional. Nas dinâmicas geopolíticas do século XXI, 'espaço e poder' tornaram-se

[1] Professora no Curso de Relações Internacionais da Universidade Federal do Rio Grande (FURG). Doutoranda em Relações Internacionais na Universidade Federal de Santa Catarina (UFSC), com Bolsa CAPES. Mestra em Integração Contemporânea da América Latina (UNILA) e Graduada em Relações Internacionais (UFSM). Pesquisadora do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea (GEPPIC).

[2] Coordenadora da Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). Doutora em Ciência Política, na linha de Política Internacional (UNICAMP), com pós-doutorado em Ciências Militares na Escola de Comando e Estado-Maior do Exército (ECEME). Vice-Presidente da ABED - gestão 2020-2022. Líder do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea (GEPPIC).

'informação e poder' e o ciberespaço passou a ter destaque à medida que proporciona aos atores, estatais e não estatais, novas ferramentas para exercer poder e controle (FERREIRA NETO, 2014; FERREIRA, 2017; PORTELA, 2018). Nesse sentido, tem-se observado a utilização desses novos recursos para conduzir ações, intervenções e ataques a diversos países ao redor do globo.

Os países sul-americanos sofrem de modo significativo com essas novas dinâmicas impostas pelo ciberespaço, com crescente uso das ferramentas cibernéticas pelos governos e por suas populações, de modo geral. Ao mesmo tempo suas capacidades de proteção no ambiente digital ainda são muito limitadas, principalmente se pensarmos nas dificuldades que enfrentam em termos de investimento em pesquisas e desenvolvimento tecnológico (MULLER, 2015; BID; OEA, 2020; CALDERARO; CRAIG, 2020).

Sendo assim, a pergunta central que direciona esta pesquisa é: Como a América do Sul têm se inserido no processo de construção de capacidades cibernéticas? Ressalta-se que a resposta dessa pergunta caminhará pela análise teórica e conceitual e por dados sobre segurança e defesa cibernética, principalmente os obtidos no Global Cybersecurity Index (GCI), da União Internacional de Telecomunicações (UIT) da Organização das Nações Unidas (ONU) e os disponíveis no Relatório sobre Cibersegurança do Observatorio de la Ciberseguridad em América Latina y el Caribe. Serão utilizados também outras estatísticas disponíveis no Internet World Stats.

1 Delimitações teórico-conceituais: perspectivas sobre ciberespaço, poder, segurança, defesa e capacidades cibernéticas

Quando se trata dos fenômenos que envolvem a dimensão cibernética, observa-se, de modo geral, problemas de imprecisão conceitual. Desde o próprio conceito de ciberespaço, de segurança e defesa cibernética, passando por capacidades cibernéticas, possuem diferentes interpretações e conceituações, tanto por parte dos pesquisadores da área quanto por parte dos Estados. Portanto, não há definições globalmente aceitas para uma variedade de conceitos que envolvem a cibernética (KUEHL, 2009; SINGER; FRIEDMAN, 2014; AYRES PINTO; GRASSI, 2020; MEDEIROS; GOLDONI, 2020).

Como ponto de partida, podemos citar a definição de ciberespaço proposta por Singer e Friedman (2014, p. 13, tradução nossa) que afirmam que "[...] o ciberespaço é o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas,

compartilhadas e comunicadas on-line."[3] Ou, ainda, a definição de Kuehl (2009, p. 28, tradução nossa), para o qual:

> [...] o ciberespaço é um domínio global [...] cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informação através de redes interdependentes e interconectadas usando tecnologias de informação e comunicação.[4]

Portanto, o espaço cibernético não é um apenas físico, nem puramente virtual. Além disso, importa lembrar que o ciberespaço e a internet não são sinônimos, já que o segundo só existe devido à criação do primeiro (LOBATO; KENKEL, 2015).

Quanto aos conceitos de segurança cibernética e defesa cibernética, estes também possuem diferentes variações nas suas definições. Quando observamos as definições propostas pelos Estados em seus documentos oficiais, também encontramos alguns pontos de diferenciação. O Glossário das Forças Armadas do Brasil, por exemplo, define segurança cibernética 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." (BRASIL, 2015, p. 249). Já a defesa cibernética é posta nestes termos:

> 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 (BRASIL, 2015, p. 85).

A Colômbia, por sua vez, associa a segurança cibernética em termos da capacidade do Estado de minimizar os riscos para os "ativos do Estado" e para seus cidadãos, buscando "disponibilidade, integridade, autenticação, confidencialidade e não repúdio das interações digitais". Ademais, entende o Estado como o ator central para facilitar e promover essa segurança (COLOMBIA, 2020, p. 43). Defesa cibernética é definida como:

> Capacidade do Estado para prevenir e neutralizar qualquer ameaça ou incidente de natureza cibernética que afete a sociedade, a soberania nacional, a independência, a integridade territorial, a ordem constitucional e os interesses nacionais. A defesa cibernética envolve o uso de recursos militares em face de ameaças cibernéticas,

[3] "[…] cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online." (SINGER; FRIEDMAN, 2014, p. 13).
[4] "[…] cyberspace is a global domain […] whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." (KUEHL, 2009, p. 28)

CAMPOS NEUTRAIS - REVISTA LATINO-AMERICANA DE RELAÇÕES INTERNACIONAIS,
Rio Grande, V. 4, N. 2, p. 52 - 64, maio. / ago. de 2022 *ISSN 2596-1314 DOI: 10.14295/rcn.v4i2.14664*

> ataques cibernéticos ou atos hostis de natureza cibernética[5] (COLOMBIA, 2020, p. 42, tradução nossa).

Do ponto de vista acadêmico, podemos definir que segurança cibernética "[...] aborda questões políticas, gestão de riscos, melhores práticas de garantia e tecnologias usadas para proteger o ambiente cibernético de um país e suas organizações", ou seja, "trata de temas relacionados à segurança pública." (OLIVEIRA et al, 2017, p. 14). Já a defesa cibernética pode ser definida como o "[...] ato de defender o sistema crítico das TICs [Tecnologias de Informação e Comunicação] de um Estado", além de englobar "as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país." (OLIVEIRA et al, 2017, p. 13). Contudo, importante ressaltar que o termo "*cybersecurity*" é utilizado, comumente, como um conceito mais geral, o qual abrange no seu âmbito a "*cyber defense*". Isso deve ser levado em consideração ao interpretar os rankings internacionais sobre a temática, já que estes vão trazer o termo "cibersegurança" de modo geral.

Partindo para o entendimento de capacidade cibernética, este é um conceito particularmente difícil de mensurar, não havendo consenso sobre seus componentes e indicadores. Para Hurel (2021), isso ocorre, em grande medida, pelo fato que essas questões devem ser relacionadas aos múltiplos contextos e realidades sociais, econômicas e políticas dos países nos quais essas capacidades são avaliadas.

O Global Cybersecurity Index (GCI), da União Internacional de Telecomunicações (UIT), avalia a segurança cibernética nos 194 Estados membros das Nações Unidas (ONU) a partir de cinco pilares: 1) Medidas legais; 2) Medidas técnicas; 3) Medidas organizacionais; 4) Medidas de desenvolvimento de capacidades; e 5) Medidas de cooperação (UIT, 2020).

Já o Observatorio de Ciberseguridad da Organização dos Estados Americanos (OEA), por utilizar o modelo Modelo de Maturidade da Capacidade de Cibersegurança para as Nações, desenvolvido pelo Global Cyber Security Capacity Centre (GCSCC) da Universidade de Oxford, utiliza outras dimensões para medir a maturidade da cibercapacidade dos Estados. São essas: 1) Políticas e estratégias; 2) Cultura cibernética e sociedade; 3) Educação, capacitação e habilidades; 4) Marcos legais e regulatórios; e 5) Padrões, organizações e tecnologias (BID; OEA, 2020).

[5] "Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética" (COLOMBIA, 2020, p. 42)

Além disso, pesquisadores têm se dedicado aos estudos sobre a construção de capacidades cibernéticas. Schia (2018) pondera que os modelos de construção capacidade cibernética, geralmente, são definidos em três categorias: recursos tecnológicos, humanos e organizacionais. Muller (2015, p. 2, tradução nossa), por sua vez, defende que "a construção de capacidade cibernética requer uma abordagem horizontal em diferentes campos da política de desenvolvimento, focando em melhorar a governança, proteger a infraestrutura, endossar o estado de direito e fornecer treinamento."[6]

Já Calderaro e Craig (2020, p. 14, tradução nossa) defendem que o conhecimento em ciência e tecnologia é crucial para o desenvolvimento da segurança cibernética. Somadas a esses conhecimentos estão as habilidades de governança e diplomacia, formando os componentes mais robustos para a análise do nível de construção de capacidades cibernéticas. Nessa direção, para medir a capacidade cibernética de um país seria necessário pensar em termos de investimentos na área, capacidade industrial em tecnologias de comunicação e informação, nível de conhecimento e habilidades (CALDERARO; CRAIG, 2020).

Destaca-se aqui também a definição de poder cibernético, o qual é compreendido por Kuehl (2009, p. 38) como a "capacidade de usar o ciberespaço para criar vantagens, produzir resultados e influenciar eventos em todos os ambientes operacionais e através os instrumentos de poder"[7]. Este é moldado por múltiplos fatores, entre eles, tecnologia, fatores organizacionais e, o mais importante, a informação. Para Nye (2010, p. 3, tradução nossa), "o comportamento do poder cibernético se baseia em um conjunto de recursos relacionados à criação, controle e comunicação da informação eletrônica e computacional"[8], ou seja, infraestrutura, redes, software e habilidades humanas. Esse poder é utilizado para influenciar e produzir resultados no âmbito do ciberespaço e fora dele, uma vez que o ciberespaço perpassa todos os domínios físicos.

Partindo dos elementos mencionados, pode-se compreender que da construção de capacidades cibernéticas depende a manutenção ou incremento da cibersegurança, da ciberdefesa e da resiliência dos Estados, bem como sua obtenção ou aumento de poder cibernético. No século XXI, o ciberespaço tornou-se essencial para o desenvolvimento dos

[6] "Cyber capacity building requires a horizontal approach across different development policy fields, focusing on improving governance, protecting infrastructure, endorsing the rule of law and providing training." (MULLER, 2015, p. 2).
[7] "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power." (KUEHL, 2009, P. 38).
[8] "Cyber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information […]" (NYE Jr., 2010, p. 3).

Estados. Capacidades cibernéticas bem desenvolvidas são necessárias para que os países progridam e se desenvolvam em todas as esferas, uma vez que o ciberespaço impacta a maioria dos aspectos da economia, do comércio, da política nacional e global, traz importantes impactos sociais e interfere diretamente nas dinâmicas de segurança e defesa dos países (MULLER, 2015; SCHIA, 2018; PAWLAK; BARMPALIOU, 2017; CALDERARO; CRAIG, 2020).

Cabe ressaltar que a construção de capacidades também afeta a estabilidade global no ciberespaço, uma vez que também impacta na proteção de outros países contra ações cibernéticas maliciosas que podem se originar desses países que carecem de infraestrutura e governança adequadas e de educação cibernética (SCHIA, 2018; CALDERARO; CRAIG, 2020). Nessa perspectiva, deve-se levar em consideração, por exemplo, que no ciberespaço ocorre a anulação da distância física - as ameaças podem avançar rapidamente e virem de qualquer parte do globo.

Na América do Sul, observou-se um aumento significativos de usuários de internet, passando de 155 milhões de usuários, em 2010 (GUEDES OLIVEIRA et al, 2017), para mais de 306 milhões de usuários, em 2017 (INTERNET WORLS STATS, 2021). Isso significa maior janela de oportunidade para ocorrência de cibercrimes, no campo da segurança cibernética, mas também aumento das ameaças à defesa cibernética, já que quanto mais conectado um Estado está, mais vulnerável ele se encontra.

Cabe enfatizar que a interconectividade dos sistemas e a ausência de regulamentação no ciberespaço facilitam ataques que possam promover rupturas políticas e militares, principalmente devido ao potencial desse cenário de controlar objetos físicos e a dificuldade de rastreamento do agressor (LOBATO; KENKEL, 2015).

2 Os países sul-americanos no contexto cibernético

A América do Sul possui aproximadamente 435 milhões de habitantes, pouco mais de 342 milhões de usuários de internet. A taxa de penetração da internet fica em torno de 79% - o que significa que pouco mais de 20% da população sul-americana não possui acesso à internet. Contudo, a região não é um bloco homogêneo e sim uma região consideravelmente assimétrica, tanto em termos de população e território, quanto em termos econômicos, sociais e político-democráticos e, da mesma forma, em relação aos usuários e penetração da internet. Nesse sentido, por exemplo, a taxa de penetração da internet na região varia de 65% a 92% entre os

países (INTERNET WORLD STATS, 2021). Do mesmo modo, observam-se disparidades significativas nos índices de segurança cibernética entre os países.

Se considerarmos os indicadores e avaliações do Global Cybersecurity Index (GCI), da União Internacional de Telecomunicações (UIT), temos o cenário disposto na Figura 1.

Figura 1 – Global Cybersecurity Index (América)

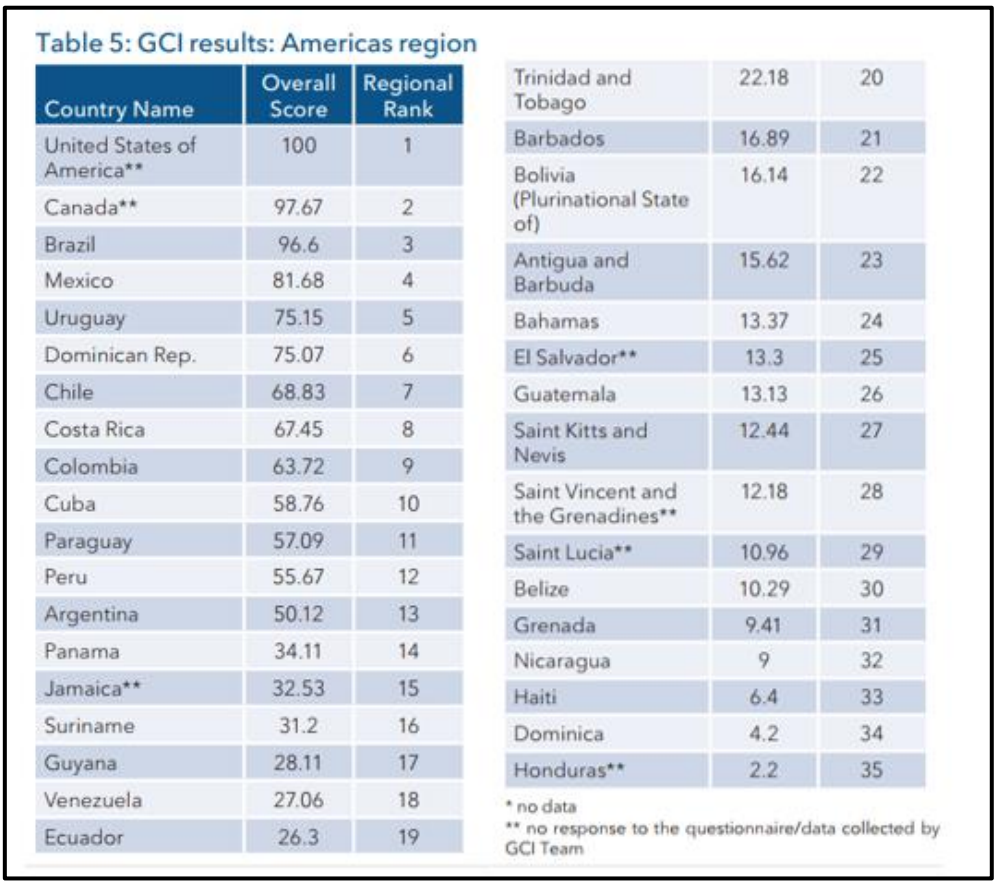

Table 5: GCI results: Americas region

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10
Paraguay	57.09	11
Peru	55.67	12
Argentina	50.12	13
Panama	34.11	14
Jamaica**	32.53	15
Suriname	31.2	16
Guyana	28.11	17
Venezuela	27.06	18
Ecuador	26.3	19
Trinidad and Tobago	22.18	20
Barbados	16.89	21
Bolivia (Plurinational State of)	16.14	22
Antigua and Barbuda	15.62	23
Bahamas	13.37	24
El Salvador**	13.3	25
Guatemala	13.13	26
Saint Kitts and Nevis	12.44	27
Saint Vincent and the Grenadines**	12.18	28
Saint Lucia**	10.96	29
Belize	10.29	30
Grenada	9.41	31
Nicaragua	9	32
Haiti	6.4	33
Dominica	4.2	34
Honduras**	2.2	35

* no data
** no response to the questionnaire/data collected by GCI Team

Fonte: UIT (2020, p. 28-29)

Pode-se observar na figura acima os diferentes graus de maturidades dos países americanos. Por exemplo, segundo este relatório da UIT (2020), entre as cinco dimensões analisadas, as medidas legais no Brasil são as mais destacadas, enquanto as técnicas e organizacionais precisam ser aperfeiçoadas. Ainda assim, o país estaria em um nível superior que os demais sul-americanos. Analisando o ranking global proposto nesse relatório da UIT (2020), o Brasil estaria na 18ª posição, enquanto o próximo país sul-americano, o Uruguai, estaria em 64ª colocação no ranking global, seguido do Chile na 74ª posição e Colômbia na posição 81 (figura 2).

Figura 2 – Global Cybersecurity Index (Global)

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
Brazil	96.6	18
Uruguay	75.15	64
Chile	68.83	74
Colombia	63.72	81

Fonte: recortes feitos a partir de UIT (2020, p. 25-26)

Essas informações diferem se observamos outros índices, uma vez que há divergências entre os indicadores para medir as capacidades cibernéticas dos países, conforme mencionado anteriormente. Esse fato dificulta uma compreensão objetiva acerca da real posição de cada país em termos de capacidade cibernética. Por exemplo, observando os dados disponíveis no Relatório sobre Cibersegurança do Observatorio de la Ciberseguridad en América Latina y el Caribe da Organização dos Estados Americanos (OEA), tem-se o Uruguai como o país com a melhor pontuação média em termos de maturidade cibernética, seguido por Colômbia, Brasil e Chile. Considerando este relatório, a maioria dos países da região se encontra na fase inicial ou formativa de sua maturidade cibernética, estando em níveis consideravelmente diferenciados em cada um dos indicadores propostos.

No ranking estabelecido a partir desse relatório, percebe-se, por exemplo, que o Uruguai se destaca nas dimensões "Cultura cibernética e sociedade", "Educação, capacitação e habilidades" e "Padrões, organizações e tecnologias". A Colômbia possui a posição mais relevante na dimensão "Política e Estratégia de Cibersegurança", possuindo também a melhor pontuação no indicador de ciberdefesa. Já o Brasil se destaca em termos de marcos legais e regulatórios, além de se destacar no indicador de defesa cibernética.

Especificamente no âmbito da defesa cibernética brasileira, cabe mencionar a relevante produção de documentos no âmbito, da organização do Sistema Militar de Defesa Cibernética, com a criação do Centro de Defesa Cibernética (CDCiber), do Comando de Defesa Cibernética (ComDCiber), da Escola Nacional de Defesa Cibernética (ENaDCiber) e outros mecanismos nesse setor. Contudo, o país ainda carece, por exemplo, de aporte financeiro, de incentivos e desenvolvimento científico e tecnológico, de precisão em termos de estratégia no setor, e de

CAMPOS NEUTRAIS - REVISTA LATINO-AMERICANA DE RELAÇÕES INTERNACIONAIS,
Rio Grande, V. 4, N. 2, p. 52 - 64, maio. / ago. de 2022 *ISSN 2596-1314 DOI: 10.14295/rcn.v4i2.14664*

uma estrutura organizacional em que ocorra efetivamente uma atuação em tríplice hélice (setor público, setor privado e academia) (AYRES PINTO; GRASSI, 2020; GRASSI; AYRES PINTO, 2021).

Com relação à documentos oficiais, uma questão importante de ser mencionada é o fato de, na América do Sul, apenas Colômbia (2016), Chile e Paraguai (2017), Argentina (2019) e Brasil (2020) possuírem uma Estratégia Nacional de Cibersegurança (BID; OEA, 2020). Outro dado relevante é que os quatro países que mais têm sofrido ciberataques nos últimos anos são Brasil, Argentina, Colômbia e Chile (CHILE, 2017a).

Partindo do exposto, é necessário ponderar sobre os variados tipos de ações cibernéticas (ciberespionagem, cibercrime, subversão, ciberataques, ciberguerra...) e as possibilidades de poderem causar significativos impactos políticos, econômicos, militares, danos a infraestruturas e afetar efetivamente os Estados e suas populações, principalmente quando se observa a intensificação de ações nessa seara que evoluem constantemente em termos tecnológicos, de alcance e potencial danoso (AYRES PINTO; GRASSI, 2020). Nesse sentido, é notório que os Estados devem voltar esforços para ações centradas tanto em nível nacional quanto regional e internacional, que busquem respostas que ultrapassem as tradicionais reações securitárias praticadas frentes as ameaças securitárias e de defesa tradicionais.

Conforme Mikser (2020), Ministro de Relações Exteriores da Estônia, pensar a construção de capacidades cibernéticas desde uma perspectiva cooperativa regional pode melhorar as condições dos países se desenvolverem neste setor, construindo capacidades mais sólidas, aumentando sua consciência sobre as ameaças emergentes e propondo mecanismos mais efetivos para enfrentá-las. Isso propiciaria um espaço mais estável, principalmente levando em consideração a interconexão entre os Estados no ciberespaço.

Assim, refletindo sobre o histórico das iniciativas de cooperação e integração na América do Sul, principalmente tomando a criação do Conselho de Defesa Sul-Americano (CDS) da União das Nações Sul-Americanas (Unasul), e os avanços que tais processos proporcionaram no auge de seus funcionamentos, bem como pensando nas fragilidades que os Estados sul-americanos precisam superar em sua construção de capacidades, entende-se que a abordagem cooperativa seria um caminho viável para a região. Sobre isso, houve diálogos sobre defesa cibernética no âmbito do CDS, os quais buscaram possibilidades de coordenação de posições e de estabelecimento de políticas e mecanismos regionais para combater as ameaças cibernéticas.

Essas iniciativas, porém, encontraram um obstáculo inicial diante das diferentes conceituações em relação ao ciberespaço em cada país membro da Unasul. Sendo assim, o primeiro passo seria a definição de conceitos comuns na área, para, a partir disso, poderem avançar na criação de políticas e mecanismos para lidar com as ameaças cibernéticas (JUSTRIBÓ, 2014; GUEDES OLIVEIRA et al, 2017; GONZALES; PORTELA, 2018).

Apesar disso, os direcionamentos que vinham sendo dados no âmbito do CDS foram paralisados com as dificuldades e crises internas na região levaram ao atrofiamento e desmonte da organização e, consequentemente, os avanços que vinham sendo observados nas conversações a respeito da agenda cibernética (JAEGER, 2018; BIDARRA; GRASSI; KERR OLIVEIRA, 2020).

Assim, a despeito do caráter transnacional do ciberespaço, o qual modifica a noção tradicional de fronteiras, a temática ainda é tratada de modo individual, no âmbito doméstico. Além disso, não há homogeneidade nem em termos conceituais nem em termos de políticas e estratégias para o setor (JUSTRIBÓ, 2014; GONÇALES; PORTELA, 2018). Como pondera Justribó (2014), os países sul-americanos apresentam marcos legislativos, políticos e doutrinários diferentes, o que resultam em avanços heterogêneos. Isso tudo pode dificultar posicionamentos e avanços conjuntos em processos cooperativos na América do Sul e coloca a região em mais um cenário de dependência dos atores hegemônicos do sistema.

Considerações finais

Tendo em vista que o conceito de capacidade cibernética não possui uma delimitação precisa, buscou-se nesta pesquisa, em um primeiro momento, investigar indicadores que são dispostos para medir o nível de capacidade cibernética de um país e, logo, compreender por que a construção dessas capacidades é particularmente importante nos Estados do Sul Global.

Para prevenir, o quanto possível, que ataques cibernéticos venham a prejudicar suas infraestruturas ou causar danos às suas populações e melhorar sua resiliência quando esses ataques não puderem ser evitados, bem como melhorar seu grau de influência frente às discussões internacionais nesse campo, é crucial que os Estados desenvolvam estratégicas efetivas para construir capacidades cibernéticas.

Nessa breve pesquisa, observou-se que, de modo geral, a região possui processos heterogêneos e consideravelmente limitados. Isso demonstra uma clara falta de projeto nacional e regional dos Estados na busca por entender essa nova esfera do poder e da relação humana

como um lugar para, também, proteger de forma soberana, exercer poder e buscar a satisfação de suas demandas nacionais.

Nessa perspectiva, ressalta-se a relevância da realização e aprofundamento das pesquisas sobre a temática, que levem em consideração o cenário que os países sul-americanos estão inseridos e que busquem superar as lacunas existentes na área. Diante disso, será possível propor estratégias mais adequadas, elencando as prioridades e os novos moldes de atuação, que resultem em processos mais eficientes para a construção de capacidades cibernéticas por esses países, capacidades as quais são indispensáveis frente as novas dinâmicas e novos desafios emergidos na era digital. Desse modo, a pesquisa seguirá justamente nessa direção, buscando superar lacunas presentes neste estudo, tais como aprofundar o entendimento das heterogeneidades e as limitações regionais no âmbito da construção de capacidades cibernéticas e refletir sobre possíveis caminhos para a superação dessas problemáticas.

Referências

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**. v. 7, n. 2, p. 103-131, jul./dez., 2020.

BIDARRA, Beatriz Soares; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas. A crise da Unasul pelas agências internacionais de notícias: a veiculação do colapso da integração regional Sul-americana pela mídia. **Revista Debates**, Porto Alegre, v. 14, n. 2, p. 207-238, 2020.

BID; OEA. **Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe**. Observatorio de la Ciberseguridad en América Latina y el Caribe, Report Ciberseguridad 2020.

BRASIL, Ministério da Defesa do. **Glossário das Forças Armadas**. 5. ed. Brasília, 2015. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf.

CALDERARO, Andrea; CRAIG, Anthony J. S. Transnational governace of cybersecurity policy challenges and global inequlities in cyber capacity building. **Third World Quarterly**, v. 41, n. 6, p. 917-938, 2020.

COLOMBIA, Consejo Nacional de Política Económica y Social da. **CONPES 3995: Política Nacional de Confianza y Seguridad Digital**. Bogotá, 01 de julho de 2020. Disponível em: https://www.csirtasobancaria.com/publicaciones/conpes-3995-politica-nacional-de-confianza-y-seguridad-digital.

FERREIRA, Juliana Aguilar de Barros. **A questão cibernética nas relações entre os Estados: uma nova forma de projeção de poder na atualidade.** 121 p. Dissertação (Mestrado em Estudos Estratégicos da Defesa e da Segurança) – Instituto de Estudos Estratégicos, Universidade Federal Fluminense, Niterói, 2017.

FERREIRA NETO, Walfredo Bento. Territorializando o "Novo" e (Re)territorializando os Tradicionais: a Cibernética como Espaço e Recurso de Poder**. Revista das Ciências Militares**, Coleção Meira Mattos, v. 1, p. 7-18, jan./abr., 2014.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. A geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética? **Austral: Revista Brasileira de Estratégia e Relações Internacionais**, Porto Alegre, v. 7, n. 14, p. 217-241, jul./dez., 2018.

GRASSI, Jéssica Maria; AYRES PINTO, Danielle Jacon. O Sistema de Defesa Cibernética e a Dinâmica Civil-Militar no Brasil. **XI Encontro Nacional da Associação Brasileira de Estudos de Defesa**, 08 a 10 de setembro de 2021.

GUEDES OLIVEIRA, Marcos Aurelio; PAGLIARI, Graciela De Conti; MARQUES, Adriana A.; PORTELA, Lucas Soares; FERREIRA NETO, Walfredo Bento. **Guia de Defesa Cibernética da América do Sul.** Recife: Ed. UFPE, 2017.

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, AE 54, abr., 2021.

INTERNET WORLD STATS. **Internet Usage and Population in South America**. Março, 2021. Disponível em: https://www.internetworldstats.com/stats15.htm.

ITU - International Telecommunication Union. **Global Cybersecurity Index**. United Nations, 2020. Disponível em: https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020.

JAEGER, Bruna Coelho. Crise e colapso da UNASUL: o desmantelamento da integração sul-americana em tempos de ofensiva conservadora. **Conjuntura Austral**. Porto Alegre, v. 10, n. 49, p. 5-12, 2019.

JUSTRIBÓ, Candela. Ciberdefensa: Una visión desde la UNASUR. **VII Congreso del Instituto de Relaciones Internacionales**. Buenos Aires: UNLP, 2014.

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, F. D.; STARR, S. S.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. University of Nebraska Press, 2009.

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

MEDEIROS, Breno Pauli; GOLDONI, Luiz. Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, v. 42, n. 1, p. 31-54, 2020

MIKSER, Sven. La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: El camino a seguir. In: BID; OEA. **Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe**. Observatorio de la Ciberseguridad en América Latina y el Caribe, Report Ciberseguridad 2020.

MULLER, Lilly Pijnenburg. Cyber Security Capacity Building in Developing Countries. **Norwegian Institute for International Affairs** (NUPI), 15, 2015.

NYE, Jr., Joseph. **Cyber Power**. Cambridge: Belfer Center For Science and International Relations, 2010.

PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; VIGGIANO, Juliana Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: Um estudo prospectivo. In: GUEDES OLIVEIRA, Marco Aurélio (Org.). **Defesa Cibernética e Mobilização Nacional**. Recife: Ed. UFPE, 2020. p. 153-174.

PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia. Politics of cybersecurity capacity building: conundrum and opportunity. **Journal of Cyber Policy**. v. 2, n.1, p. 123-144. 2017.

PORTELA, Lucas Soares. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. **Revista Brasileira de Estudos em Defesa**, v. 5, n. 1, p. 141-165, jan./jun. 2018.

SCHIA, Niels Nagelhus. The Cyber Frontier and Digital Pitfalls in the Global South. **Third World Quarterly**, v. 39, n. 5, p. 821–837, 2018.

SINGER, Peter Warren; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know.** Oxford University Press, 2014.