Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas

Jéssica Maria Grassi | Danielle Jacon Ayres Pinto | Graciela de Conti Pagliari

INTRODUÇÃO

A internet, que já foi compreendida como uma força para liberdade e para democracia, tem se tornado um espaço para amplificação da desinformação, incitação da violência e de contestação da confiabilidade da mídia e das instituições democráticas, configurando-se um local favorável para a ascensão e difusão dos radicalismos de extrema-direita[1]. Sobre isso, a última década mostrou à sociedade mundial – em especial à sul-americana – os grandes desafios aos quais as democracias estarão submetidas no século XXI. Com processos cada vez mais deturpados sobre o conteúdo verídico das informações sobre política, economia, política externa, cultura, segurança e defesa, é possível observar um movimento de crescente descrença da sociedade no conteúdo da informação que recebe dos tradicionais canais de notícias. O resultado desse movimento tem sido um exponencial aumento da crença dos indivíduos em informações de conteúdo falso, transmitida por agentes de espectro ideológico próximo ao do cidadão.

Como consequência, o novo meio digital de sociabilidade da informação tem provocado sérios danos aos pilares democráticos dos Estados, pois a desinformação e as informações falsas têm virado recurso do debate político oficial. Nessa perspectiva, entre as diversas ameaças obser-

RESUMO

A última década mostrou à sociedade mundial – em especial a sociedade sul-americana – os grandes desafios aos quais as democracias estarão submetidas no século XXI. Entre as diversas ameaças observadas no ciberespaço estão as denominadas campanhas de desinformação e as interferências híbridas. Diante disso, esse novo meio digital de sociabilidade da informação tem provocado sérios danos aos pilares democráticos dos Estados, pois a desinformação e as informações falsas têm virado recurso no debate político. Isso posto, o artigo buscará analisar a construção de processos cooperativos na área de segurança e defesa cibernética entre os países sul-americanos entre 2012 e 2020 e seus efeitos na proteção da democracia e do Estado de direito. Defende-se que, devido à dinâmica transfronteiriça do mundo digital e do disseminado alcance de suas ações e consequências, a busca por uma solução a essas demandas perpassa um processo de aprofundamento da cooperação estatal no qual as estratégias de política externa dos Estados são fundamentais para a construção de uma resposta efetiva a esse tipo de ameaça à democracia em âmbito internacional. Nessa perspectiva, com-

→

 https://doi.org/10.23906/ri2024.82a02

preende-se a interdependência entre os Estados nessa esfera e adota-se uma concepção cooperativa para refletir sobre os obstáculos enfrentados pelos países sul-americanos.

Palavras-chave: segurança cibernética, interferências híbridas, democracia, cooperação cibernética.

ABSTRACT

Cooperation in cyber security and cyber defense and the protection of South American democracies

The last decade has shown the global society, especially South American society, the great challenges that democracies will face in the 21st century. Among the various threats observed in cyberspace are the so-called disinformation campaigns and hybrid interference. As a result, this new digital means of information socialization has caused serious damage to the democratic pillars of states, as disinformation and false information have become a feature of political debate. Based on this, the article seeks to analyze how South American countries are building cooperation in cybersecurity and cyber defense between 2012 and 2020, and what the implications are for the protection of democracy and the rule of law. It is argued that, due to the transnational dynamics of the digital world and the wide reach of its actions and consequences, the search for a solution to these demands goes through a process of deepening state cooperation, in which the foreign policy strategies of states are fundamental for building an effective response to this type of threat to democracy at the international level. From this perspective, we understand the interdependence between States in this sphere and adopt a cooperative conception to reflect on the obstacles South American countries face.

Keywords: cybersecurity, hybrid interference, democracy, cyber cooperation.

vadas nesse novo espaço estão as denominadas interferências híbridas, campanhas de desinformação, *fake news*[2], propaganda computacional e outras formas de manipulação da informação por meio do ciberespaço. Tais ferramentas possuem o potencial de comprometer valores democráticos e desestabilizar instituições políticas. Também podem pressionar organizações econômicas e financeiras de um país, afetar seu moral e moldar o cenário interno, conforme as preferências de determinado grupo ou país. Isso tudo com a vantagem do anonimato, já que é extremamente difícil a identificação da origem exata desse tipo de campanha cibernética.

Os países sul-americanos enfrentam uma série de fragilidades políticas e institucionais que se somam a desafios econômicos e geopolíticos enfrentados pela região. Especificamente, no âmbito cibernético, tais países carecem de capacidades cibernéticas[3] e suas debilidades estruturais se originam desde frágeis bases educacionais, especificamente, da falta de incentivos à educação cibernética da sua população, da falta de políticas públicas para a ciência nacional e para a conscientização, até a formação e capacitação de recursos humanos. Sendo a educação, a formação de talentos e o desenvolvimento científico e tecnológico um pilar estratégico para a construção de capacidades cibernéticas, que é a base da qual as demais dimensões da construção de capacidades se sustentarão e, da mesma forma, entendendo a camada *peopleware*[4] como a mais importante para a segurança cibernética de uma nação, essa carência acaba por se refletir nos atuais desafios cibernéticos e democráticos dos países da região. Essa situação deixa esse grupo de países, em sua maioria considerados subdesenvolvidos ou em desenvolvimento, vulneráveis diante das inúmeras ameaças advindas do ciberespaço. Além disso, esse contexto resulta em vantagens e oportunidades de intervenções de atores estatais mais desenvolvidos em países do Sul Geopolítico[5][6].

Diante do exposto, e devido à dinâmica transfronteiriça do mundo digital e do disseminado alcance de suas ações e consequências, entende-se que a busca por uma solução para essas demandas perpassa pelo processo de aprofun-

damento da cooperação interestatal, no qual as estratégias de política externa dos Estados são fundamentais para a construção de uma resposta efetiva a esse tipo de ameaça que traz riscos, inclusive, aos seus processos democráticos. Desse modo, o artigo pretende trabalhar a seguinte questão: os países sul-americanos estão construindo processos cooperativos regionais na área de segurança e defesa cibernética de modo a protegerem suas democracias frente aos desafios da era digital? Acredita-se que, apesar de iniciativas de cooperação cibernética terem tomado forma na região e mesmo com o potencial regional para avançar em processos cooperativos, pouco se evoluiu no sentido de implementar agendas de cooperação multilateral que auxiliem na proteção dos sistemas democráticos regionais.

Esta pesquisa parte de uma perspectiva que evidencia a interdependência entre os Estados e adota-se uma concepção cooperativa para refletir sobre os obstáculos enfrentados pelos países sul-americanos, atentando para as dinâmicas geopolíticas próprias da região. Neste sentido, pelo fato de haver dinâmicas geopolíticas e securitárias a América do Sul justifica-se como um objeto de análise por si só na medida em que este trabalho analisa os elementos de cooperação desenvolvidos a partir dos mecanismos regionais sul-americanos. Embora a analogia trazida da economia de que o Brasil seja um rinoceronte em uma loja de cristais se comparado aos demais países da América do Sul[7], a mesma não retira a capacidade analítica da região como espaço específico de análise.

Para alcançar o objetivo proposto, adota-se a técnica de pesquisa bibliográfica, utilizando, eventualmente, documentos oficiais e notícias para auxiliar na discussão dos tópicos mais atuais. Ademais, ressalta-se que, para analisar a cooperação cibernética na América do Sul, tem-se o ano de 2012 como marco temporal, visto que neste ano os membros da União das Nações Sul-Americanas (Unasul) iniciaram um plano de trabalho para cooperação multilateral na área cibernética no âmbito do seu Conselho de Defesa.

Para desenvolver essa pesquisa o artigo está dividido em três seções. Iniciamos apresentando as principais ameaças à segurança e defesa dos Estados, inclusive no que diz respeito à proteção dos sistemas democráticos. Em seguida, trazemos a discussão sobre processos de cooperação estatal no setor cibernético, destacando estudos que apontam para as vantagens de estratégias cooperativas principalmente para os países do Sul Geopolítico e para países que não possuem nítidos rivais no âmbito militar. Por fim, analisamos o processo de cooperação cibernética que tomou forma na América do Sul, os percalços ao longo dos últimos anos e os efeitos de tais processos cooperativos para a construção de capacidades e proteção das democracias dos países da região.

AMEAÇAS CIBERNÉTICAS E OS RISCOS À DEMOCRACIA NO SÉCULO XXI

As ferramentas do ciberespaço vêm sendo aperfeiçoadas de maneira a revolucionar o modo de se fazer a guerra no século XXI e esse cenário tornou a ciberguerra uma das

grandes preocupações das defesas nacionais hoje em dia[8]. Isso se deve às características que tornam esse espaço diferenciado dos demais[9], à crescente digitalização dos processos e das infraestruturas críticas dos Estados e às consequentes vulnerabilidades inerentes dessas infraestruturas que dependem dos sistemas computacionais[10]. Com isso, constroem-se cenários potencialmente catastróficos, no qual o poder cibernético se traduz em diversas vantagens em conflitos.

AS FERRAMENTAS DO CIBERESPAÇO VÊM SENDO APERFEIÇOADAS DE MANEIRA A REVOLUCIONAR O MODO DE SE FAZER A GUERRA NO SÉCULO XXI: CONSTROEM-SE CENÁRIOS POTENCIALMENTE CATASTRÓFICOS, NO QUAL O PODER CIBERNÉTICO SE TRADUZ EM DIVERSAS VANTAGENS EM CONFLITOS.

Entretanto, segundo Thomas Rid, a probabilidade de uma guerra autônoma no ciberespaço é baixa, quando se conceitua corretamente o termo e se observa as formas mais comuns de atuação dos atores nesse espaço. Para o autor, os atores têm utilizado ferramentas digitais para sabotagem, espionagem e subversão, as quais podem acompanhar operações militares tradicionais, mas não a guerra como a conhecemos desde a teorização clausewitzina[11]. Contudo, tendo em vista as oportunidades que os recursos cibernéticos apresentam para os atores, é necessário entender o crescimento das campanhas de desinformação, propaganda computacional ou manipulação da informação como um elemento promotor do conflito na esfera cibernética[12]. Sobre isso, é importante apresentar o que se tem denominado por interferências híbridas. Interferências híbridas podem ser definidas como ataques sutis, como manipulação da informação, uso de campanhas de desinformação e uma série de recursos não militares, utilizados como meios indiretos para influenciar o debate público, acelerar polarizações políticas, ideológicas, econômicas e sociais de um país e minar sua coesão interna[13].

Elemento central das interferências híbridas é a subversão, citada por Rid, na qual o alvo é a mente humana e sua consciência identitária dentro da sociedade. A subversão pode ser entendida como tentativas de desestabilizar ou minar a integridade ou autoridade do Estado alvo através de atores locais, usando como ferramentas as campanhas de desinformação[14]. Nesse sentido, tais interferências podem ser utilizadas como estratégias complementares (em situações de conflito ou não) para desestabilizar um país e fazê-lo adotar determinada postura. Isso tudo com a vantagem do anonimato e sem ultrapassar o limiar do conflito. Somando-se a isso, essas ações possuem um custo financeiro baixo e menor aporte tecnológico e intelectual. Ao mesmo tempo, são altamente prejudiciais, podendo resultar em importantes danos no «mundo físico», além de serem de difícil contenção e resiliência por parte do ator atacado.

As campanhas de desinformação têm como elemento central a distorção da verdade, de modo que se torna cada vez mais difícil distinguir fato de ficção. Tais ferramentas digitais tornaram-se fundamentais para obter vantagens em períodos eleitorais e têm sido utilizadas para promover artificialmente ou manipular pontos de vista que favorecem líderes políticos, para abafar opiniões divergentes ou para atacar ou desacreditar

opositores. Desse modo, têm potencial de acelerar a polarização, interferir ou alterar resultados políticos e, de forma efetiva, desestabilizar os pilares das democracias liberais, pondo em risco as liberdades civis[15].

Apontou-se, em estudo publicado em 2019, que 68% dos países utilizaram *trolls*, patrocinados pelo Estado, para atingir opositores e/ou jornalistas; 89% usaram de propaganda computacional para atacar a oposição política; e 75% dos países usaram desinformação e manipulação da mídia para enganar os usuários. Constatou-se que, pelo menos, 70 países vêm realizando campanhas cibernéticas com fins políticos[16]. De forma similar, em investigações realizadas entre 2016 e 2019, as quais analisaram 97 eleições nacionais em países livres ou parcialmente livres, identificou que em 20 países[17] houve claras evidências de interferências estrangeiras. Entre os 20 países citados neste estudo estão Brasil e Colômbia[18].

As eleições presidenciais do Brasil, em 2018 e 2022, são importantes exemplos na região sul-americana do potencial desestabilizador das ferramentas digitais, uma vez que o processo foi caracterizado pelo uso das redes sociais para disseminar notícias falsas, contestar a confiabilidade da mídia e das instituições democráticas, acirrando a polarização, aumentando a violência política e minando a coesão interna[19]. Na Colômbia, o referendo para a paz em 2016 e as eleições presidenciais em 2018 e em 2022 também envolveram «mentiras estratégicas, falácias, propaganda, fortes apelos à emoção, conspirações ou narrativas de polarização»[20]. Ainda, as eleições na Argentina em 2023 e outros tantos cenários de desinformação e manipulação através das plataformas digitais marcaram a política latino-americana nos últimos anos[21]. Cabe reiterar a complexidade de definir a origem exata dessas campanhas cibernéticas, as quais podem se originar ou serem financiadas por atores externos.

As manipulações que podem surgir como ação de atores externos nesse pleito fazem com que a democracia seja o alvo direto dos recursos cibernéticos utilizados numa lógica não violenta. Logo, a clivagem ideológica que tal ação pode causar promove ruptura social e pode, como afirmam Oliveira e Izycki,

> «ser interpretad[a] como evidência de um ambiente democrático em deterioração ou, pelo menos, de um ecossistema político no qual a violação da privacidade dos cidadãos com o objetivo de direcionar sua assimilação cognitiva da realidade é uma forma aceitável de conduzir os assuntos governamentais»[22].

O fato é que, como já antevê o relatório do Fórum Econômico Mundial de Davos de 2024, a informação falsa e a desinformação serão as principais ameaças securitárias do mundo no curto prazo. Isso porque nos próximos dois anos mais de 97 países, incluindo o mais populoso do mundo – a Índia – e o mais rico do mundo – os Estados Unidos – terão eleições importantes[23].

Todavia, quando se trata de recursos cibernéticos, há a necessidade de se ajustar o foco da segurança e da defesa, abarcando toda a complexidade e sinuosidade dos desafios

que advêm do ciberespaço, já que medidas tradicionais de defesa não são suficientes para esses novos tipos de ameaças. Além disso, Wigell reitera que os meios para se proteger desses novos métodos devem considerar também a defesa dos valores democráticos. Para o autor,

> «os valores democráticos liberais não têm de ser vulnerabilidades em matéria de segurança, mas podem ser transformados em pontos fortes e instrumentos para dissuadir de forma credível os agressores híbridos, tornando simultaneamente as nossas democracias ocidentais mais robustas e resilientes»[24].

Nesse sentido, as estratégias de segurança, defesa e construção de capacidades cibernéticas amplas devem considerar abordagens que envolvam toda a sociedade, abordagens cooperativas entre autoridades do setor público, do setor privado, da academia e demais organizações da sociedade civil[25]. Ou, como alguns autores denominam, uma abordagem em tríplice hélice[26]. Como pondera Wigell, «nesta nova era de política subversiva, em que a dicotomia clássica vestefaliana entre assuntos internos e externos do Estado se esbateu, a dissuasão é mais difícil de alcançar apenas através da ação do Estado»[27].

Nessa direção, tendo em vista a dinâmica transfronteiriça do mundo digital e o disseminado alcance de suas ações, medidas de cooperação interestatais também são fundamentais para promover segurança, bem como para a promoção de um processo de governança cibernética internacional que deve ser consolidado de forma ampla. Nesse sentido, analisando os diversos desafios enfrentados pelos países sul-americanos na construção de suas capacidades cibernéticas, conforme mencionado anteriormente, entendemos que o processo de aprofundamento da cooperação estatal é fundamental para a construção de uma resposta efetiva a essas ameaças na região. Essa é a discussão que pretendemos ressaltar na seção seguinte.

COOPERAÇÃO PARA A CONSTRUÇÃO DE CAPACIDADES CIBERNÉTICAS: BUSCANDO SUPERAR DESAFIOS PROVENIENTES DO CIBERESPAÇO

Apesar de iniciativas cooperativas estarem tomando forma, estudos que discutam profundamente a cooperação internacional ainda não estão no centro da discussão quando o assunto é segurança e defesa cibernética, sobretudo por tratar de temas sensíveis e que envolvem a construção da confiança entre os atores[28]. A lógica dominante dá ênfase à securitização e, mesmo, militarização do ciberespaço, abordando-o como um novo domínio para realização de guerras; discute-se, portanto, conflitos, armas cibernéticas, dissuasão militar cibernética e possibilidade de uma corrida armamentista cibernética se desenvolver[29]. Esse contexto deixaria pouco espaço para medidas cooperativas, já que ressalta um ambiente de competição onde a construção da confiança torna-se uma missão quase impossível.

Entretanto, novas perspectivas sobre a temática vêm tomando forma, ressaltando a necessidade de propor alternativas para a construção de capacidades cibernéticas que ultrapassem a lógica militarizada, atentando para o fato que a era digital demanda respostas diferenciadas[30]. Essas visões apontam para dinâmicas cooperativas, o desenvolvimento da diplomacia cibernética e de ações coordenadas entre atores estatais, não estatais e os diversos setores da sociedade. Justifica-se o caráter transnacional dessa esfera, a interligação dos sistemas, a interdependência entre os atores e as características intrínsecas desse ambiente para fortalecer temáticas relacionadas à governança da internet, a construção da confiança entre os atores e o estabelecimento de acordos bilaterais e multilaterais no setor[31].

Conforme Mikser[32], pensar a construção de capacidades cibernéticas desde uma perspectiva cooperativa regional pode melhorar a condição 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.

Diante disso, pode-se observar iniciativas cooperativas tomando forma em organizações internacionais, como na Organização do Tratado do Atlântico Norte, na União Europeia, na Associação das Nações do Sudeste Asiático, na Organização dos Estados Americanos, no Mercosul e nos fóruns existentes no âmbito das Nações Unidas e na União Internacional de Telecomunicações, como as reuniões do Group of Governmental Experts e do Open-Ended Working Group[33].

Perspectivas cooperativas são particularmente importantes para os países sul-americanos, os quais enfrentam dificuldades econômicas, carecem de recursos humanos qualificados, de habilidades e conhecimento, de desenvolvimento tecnológico e investimento em ciência nacional. Consequentemente, permanecem dependentes dos países desenvolvidos, importando suas soluções para o setor[34]. Ademais, de modo geral, possuem fragilidades institucionais e fraca estrutura de governança cibernética interna[35].

PAÍSES DO SUL GEOPOLÍTICO, COMO OS PAÍSES SUL-AMERICANOS, ENCONTRAM-SE À MARGEM DA CONSTRUÇÃO DE UMA GOVERNANÇA CIBERNÉTICA INTERNACIONAL.

Adicionalmente, conforme destacam Ceballos, Maisonnave e Londoño:

> «As *fake news* e o *lawfare*, fenômenos plenamente presentes nas disputas latino-americanas, são apenas exemplos do potencial antidemocrático das ferramentas digitais se não houver uma visão estratégica em torno delas. A colonialidade do poder e do saber faz com que, enquanto as grandes potências priorizam sua autonomia digital na América Latina, os avanços neoliberais desfazem as políticas estatais de desenvolvimento nacional. Desta forma, a formação de profissionais em tecnologia é negligenciada, estes são flexíveis à estrangeirização dos nossos sistemas tecnológicos e de gestão da informação e, do ponto de vista de uma integração tecnológica regional essencial, carecem de projetos sustentáveis»[36].

Cabe ressaltar que a interconectividade dos sistemas e a carência de regulamentação no ciberespaço facilitam ataques que possam promover rupturas políticas e militares. Assim, em um contexto de acirramento da competição geopolítica internacional, para esse grupo de países torna-se particularmente fundamental a construção de capacidades cibernéticas para que sejam capazes de proteger suas instituições políticas, econômicas e militares, inclusive frente às interferências híbridas mencionadas[37].

Ainda, países do Sul Geopolítico, como os países sul-americanos, encontram-se à margem da construção de uma governança cibernética internacional, sendo insuficientemente representados nas instâncias internacionais de tomada de decisão, de formulação de políticas e de desenvolvimento de mecanismos para o futuro do ciberespaço. Analisando por essa perspectiva, constata-se, portanto, que a estrutura global do ciberespaço perpetua a divisão Norte-Sul[38].

Desse modo, reitera-se a importância de processos de cooperação Sul-Sul para que esses países possam articular ações para a promoção de medidas de segurança, defesa e resiliência no espaço cibernético, desenvolvendo mecanismos de compartilhamento de informações, conhecimentos e experiências, iniciativas conjuntas para treinamento, capacitação e resolução de desafios comuns, trabalhando conjuntamente para a construção de suas capacidades cibernéticas, diminuindo os custos envolvidos, e buscando romper com sua dependência em relação aos países desenvolvidos. Ademais, processos cooperativos são fundamentais para que esses países possam coordenar posições visando aumentar seu poder de decisão e de barganha, para que tenham seus interesses atendidos nos espaços de governança internacional[39].

Como aponta Herz:

> «o debate público sobre segurança cibernética precisa ser promovido em base local, nacional, regional e internacional. Diferentes órgãos e setores do aparato estatal, organizações da sociedade civil, comunidade técnica, setor privado, academia e entidades internacionais precisam ser ouvidos e precisam ter participação nas formas de coordenação. Este processo diz respeito à saúde das instituições democráticas, mas também à necessidade de informação da população sobre as regras e processos relativos à Quarta Revolução Industrial»[40].

Assim, refletindo sobre o histórico das iniciativas de cooperação e integração na América do Sul – principalmente considerando a criação do Conselho de Defesa Sul-Americano (CDS) da Unasul e as novas agendas postas no Mercosul nas últimas duas décadas –, bem como os avanços que tais processos proporcionaram no auge de seus funcionamentos[41], percebe-se o potencial para medidas cooperativas na região também para o âmbito cibernético. Ainda, observando o cenário regional, não há percepções sobre disputas de poder no domínio cibernético entre os países sul-americanos e os países que já projetaram e desenvolveram iniciativas de cooperação cibernética[42]. Desse

modo, a próxima seção buscará compreender como foi e está sendo encaminhada uma agenda de cooperação multilateral na área cibernética.

COOPERAÇÃO CIBERNÉTICA NA AMÉRICA DO SUL: AVANÇOS E RETROCESSOS

A América do Sul é uma região consideravelmente heterogênea, onde se observam notáveis assimetrias em questões econômicas, políticas, sociais e securitárias. Apesar das inúmeras diferenças entre os Estados da região, o contexto geopolítico internacional os une, já que, por um ângulo distinto, tais países também enfrentam inúmeros desafios políticos, econômicos, sociais e securitários que os aproximam para além do aspecto meramente geográfico. Da mesma forma, se observarmos as capacidades cibernéticas desses Estados, encontraremos situações substancialmente diferenciadas e, por outro lado, desafios que têm o potencial de os aproximar, já que os diferentes estágios em que os países se encontram nessa área podem ser analisados a partir de uma perspectiva de complementaridade, na qual os países podem cooperar e contribuir para a construção de capacidades regionais a partir de suas experiências e avanços individuais[43].

Do ponto de vista da cooperação multilateral, os países sul-americanos iniciaram um importante diálogo no âmbito do CDS da Unasul. Em 2012, os Estados-Membros criaram um plano de trabalho buscando oportunidades de coordenar posições e de estabelecer políticas e mecanismos regionais para combater as ameaças cibernéticas e informáticas. Os Estados estabeleceram a criação de um Grupo de Trabalho em Ciberdefesa e entenderam, como um primeiro passo, a necessidade de definir conceitos comuns na área. A partir disso, seriam avaliadas as possibilidades de avanços com a criação de políticas e mecanismos para lidar com tais ameaças cibernéticas. Entre outras coisas, também previram que buscariam diagnosticar as situações enfrentadas pelos países, identificar os principais atores, instituições e protocolos de cada país, propor programas de educação e exercícios de capacitação conjuntos[44].

Após os escândalos de espionagem norte-americana, houve um fortalecimento das iniciativas no âmbito da Unasul, com ênfase à defesa cibernética. Em 2013, em declaração conjunta, os países estabeleceram, inclusive, a intenção de promover o desenvolvimento de tecnologias regionais e de instituir iniciativas conjuntas entre Mercosul e Unasul[45]. Ainda, nesse período, chegaram a propor a construção e conexão das redes de fibra ótica dos países, visando tornar as telecomunicações mais seguras[46].

APÓS OS ESCÂNDALOS DE ESPIONAGEM NORTE-AMERICANA, HOUVE UM FORTALECIMENTO DAS INICIATIVAS NO ÂMBITO DA UNASUL, COM ÊNFASE À DEFESA CIBERNÉTICA.

Da mesma forma, após esses vazamentos, algumas conversações no âmbito do Mercosul também tomaram forma, essas mais voltadas à segurança da informação e das comunicações. Cria-se, a partir disso, um grupo de trabalho com especialistas sobre o tema, os quais chegaram a esboçar linhas de ação que perpassavam discussões sobre regulamentações, desenvolvimento de *softwares*, intercâmbio de informação, capacitação

e desenvolvimento tecnológico. O grupo, no entanto, não obteve resultados concretos e deixou de se reunir após 2015[47].

Já no âmbito da Unasul, em 2014, na X Reunião da Instância Executiva do Conselho de Defesa Sul-Americano, os países-membros estabeleceram, entre seus objetivos: produzir e sistematizar uma ampla reflexão sobre as definições conceituais da defesa e segurança cibernética, de modo a unificá-las no nível regional; criar um grupo de trabalho e uma rede de contatos entre as autoridades competentes para troca de conhecimentos, de procedimentos e de soluções no âmbito da defesa cibernética[48]. Os planos de ação de 2015, 2016 e 2017 previram a continuação das atividades do Grupo de Trabalho de Ciberdefesa, a coordenação de ações com o Conselho de Infraestrutura e Planejamento (Cosiplan) e a realização de um seminário sobre o tema, além da necessidade de repensar o cronograma do plano de trabalho da instituição[49].

No âmbito do Mercosul, também foi criado o Grupo Agenda Digital em 2017. Este se voltou, principalmente, ao tema da economia digital. Os planos do Grupo discutem, entre outros tópicos, aspectos técnicos e regulatórios sobre governo eletrônico, infraestrutura digital e conectividade, segurança e confiança do ambiente digital, bem como habilidades digitais[50].

Desafortunadamente, não se constatou significativos progressos nas discussões. Observa-se que os países não conseguiram avançar nem no sentido de homogeneizar os termos e desenvolver conceitualizações comuns, muito menos avançaram na proposição de políticas e estratégias conjuntas para o setor[51]. Entre os principais agravantes para esse cenário estão a polarização política, as crises internas enfrentadas pelos países e as interferências externas à região, as quais resultaram no processo de desmantelamento da Unasul a partir de 2016 e a consequente paralização dos direcionamentos que vinham sendo dados no âmbito do CDS, bem como a relativa estagnação nas conversações no âmbito do Mercosul[52].

Ainda, o cenário da cooperação e da integração na região já enfrentava diversos problemas estruturais, que perpassam, por exemplo, a fraca institucionalidade dos processos de integração, a falta de recursos e as debilidades internas dos Estados que travam o prosseguimento de vários projetos. Ademais, diante da polarização e das heterogeneidades regionais, seja em termos políticos, econômicos, sociais ou securitários, as decisões por consenso tornam-se complexas[53].

Assim, conforme pondera Justribó, os países sul-americanos apresentam marcos legislativos, políticos e doutrinários diferentes, o que resulta em avanços heterogêneos[54]. Isso tudo dificulta posicionamentos e avanços conjuntos em processos cooperativos na América do Sul, além de deixar a região em mais um cenário de dependência dos atores hegemônicos do sistema e vulnerável diante das inúmeras ameaças cibernéticas mencionadas na primeira seção deste artigo. Para Herz, o desmantelamento da Unasul, especificamente do CDS, representou uma oportunidade perdida, diante da viabilidade de, regionalmente, harmonizar as legislações, criar

regras e articular políticas, criar mecanismos de gestão de crises e coordenar posições em fóruns internacionais[55].

Diante do enfraquecimento dos processos cooperativos no âmbito sul-americano, ampliou-se o espaço para a atuação em mecanismos no nível continental, já que os países alargaram o diálogo sobre tais temas na Junta Interamericana de Defesa OEA. A OEA adotou ainda em 2004 uma estratégia conjunta para segurança cibernética e vem avançando com a proposição de medidas de confiança, realizando investigações nos países-membros, desenvolvendo informes e propondo treinamentos, simulações e capacitações conjuntas[56]. Cabe mencionar, entretanto, que a instituição é sediada nos Estados Unidos – sendo este também seu principal financiador – e tem sido, historicamente, um espaço para a propagação da agenda securitária da potência do Norte, sendo, portanto, um símbolo da ordem norte-americana na América Latina. Para mais, essa situação deixa a América do Sul novamente dependente de mecanismos externos para a resolução de problemáticas regionais[57].

Não obstante, alguns consensos parecem persistir na região. Entre eles estão a defensa da necessidade de normas mais específicas e vinculativas no nível internacional, a construção de confiança entre os atores e o estabelecimento da Organização das Nações Unidas como plataforma para diálogos sobre a paz, a segurança e a estabilidade internacional do ciberespaço[58]. Partindo de consensos já estabelecidos e buscando novas agendas, os Estados podem unir forças para fazer frente em processos de governança internacional, aumentar seus níveis de segurança cibernética e combater os desafios que ameaçam as democracias sul-americanas.

Por fim, apesar dos desafios para a consolidação de uma agenda de cooperação cibernética na América do Sul, o período de auge dos processos de cooperação e integração regional demonstra o potencial da região em avançar na proposição de medidas conjuntas em diversas áreas, inclusive em segurança e defesa, e solucionar controvérsias regionalmente de forma autônoma. Tais iniciativas possibilitaram a maior coesão regional e demonstraram a capacidade de mobilização da região em prol de uma inserção internacional menos dependente[59], processo que, principalmente na esfera cibernética, será fator estratégico em um futuro próximo tanto para o desenvolvimento da região como para sua segurança em âmbito coletivo.

CONSIDERAÇÕES FINAIS

Esta pesquisa visou, em um primeiro momento, analisar as ameaças cibernéticas e os desafios que estas oferecem à estabilidade democrática. A partir disso, discutiu-se as abordagens cooperativas no setor cibernético e a construção de processos de cooperação na América do Sul, observando o cenário geopolítico sul-americano e ponderando sobre os efeitos dessas medidas para a proteção dos pilares democráticos. Defendemos que a busca por uma solução para as demandas dos países perpassa pelo processo de aprofundamento da cooperação regional, uma vez que estratégias de política externa

são fundamentais para construção de uma resposta efetiva a essas novas ameaças à segurança e defesa dos Estados. Além disso, argumentamos que as ameaças cibernéticas demandam abordagens diferenciadas e mais abrangentes que abarquem toda a complexidade e sinuosidade dos desafios estabelecidos com o espaço cibernético.

Partindo dessa perspectiva, retomando as discussões propostas, além de todas as ameaças originadas no ciberespaço já amplamente discutidas, esse ambiente traz novas ferramentas que atuam também de forma mais sutil e que possuem a capacidade de acelerar polarizações, minar a coesão interna e, principalmente, desestruturar os sistemas democráticos. Essas ferramentas estão sendo empregadas em interferências híbridas em diversos Estados, utilizando, frequentemente, atores locais para tais ações. Diante disso, abordagens que ultrapassem a lógica militarizada, que abranjam medidas cooperativas multissetoriais, envolvendo os setores público e privado bem como a sociedade civil, e medidas de cooperação interestatais estão sendo discutidas pela academia. Compreende-se que tais ameaças necessitam de respostas mais abrangentes, que melhorem as condições dos países se desenvolverem no setor e auxiliem no desenvolvimento de mecanismos mais eficientes para enfrentar os desafios emergentes. Essas discussões têm especial relevância para os países do Sul Geopolítico, que enfrentam desafios econômicos, tecnológicos, fragilidades institucionais e grande dependência em relação às potências do Norte.

Muito embora os desafios à cooperação entre os países da região apontados neste trabalho permaneçam, a percepção desses acerca da importância de normas multilaterais internacionais construtoras da confiança demonstra que há consenso no que diz respeito à necessidade de criação de normas de governança cibernética. Este é um ponto fundamental para sustentar o argumento de que os países devem buscar respostas que ultrapassem as tradicionais reações securitárias, voltando seus esforços também para ações multilaterais centradas no nível regional, desenvolvendo estratégias conjuntas na região. Como apontado, isso configuraria um caminho promissor, de modo a fazer frente às ameaças digitais que vêm desestabilizando suas democracias nos últimos anos.

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Jéssica Maria Grassi Investigadora associada do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD). Doutora em Relações Internacionais pela Universidade Federal de Santa Catarina (UFSC).

> Centro Socioeconômico – CSE UFSC, R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | jessicamgrassi@gmail.com

Danielle Jacon Ayres Pinto Investigadora sénior do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD). Doutora em Ciência Política pela Universidade Estadual de Campinas (UNICAMP). Professora no Curso de Relações Internacionais e coordenadora do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC).
> Centro Socioeconômico – CSE UFSC, R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | danielle.ayres@ufsc.br

Graciela de Conti Pagliari Professora no Departamento de Economia e Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). Coordenadora e investigadora sénior do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD).Doutora em Relações Internacionais pela Universidade de Brasília (UNB).
> Centro Socioeconômico – CSE UFSC. R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | graciela.pagliari@gmail.com

NOTAS

1 BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. University of Oxford, Computational Propaganda Research Project, working paper, report n.º 19, 2019; AYRES PINTO, Danielle Jacon; MORAES, Isabela – «As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit». In *Revista de Estudios Sociales*. Bogotá. N.º 74, outubro-dezembro de 2020, pp. 71-82.

2 As *fake news* são compreendidas como uma das formas que apresentam as campanhas de desinformação. Se caracterizam por informações falsas, inventadas ou distorcidas, visando enganar ou manipular a opinião pública e distorcer o debate político. Ver: CURI JÚNIOR, Aribelco; ALFAYA, Natalia Maria Ventura da Silva – «O impacto das fake news nas eleições presidenciais de 2018 e 2022: prejuízos para a democracia e a sociedade». In *Revista do Instituto de Direito Constitucional e Cidadania*. Paraná. Vol. 8, N.º 1, janeiro-junho de 2023, pp. 1-11.

3 O conceito de capacidade cibernética é particularmente difícil de ser mensurado, não havendo consenso na literatura sobre seus componentes, indicadores ou como efetivamente devem ser avaliadas as capacidades dos Estados. Para uma compreensão mais aprofundada sobre elementos que sustentam a construção de capacidades cibernéticas, ver GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas e os Processos Cooperativos no Contexto Geopolítico Sul-Americano». Universidade Federal de Santa Catarina, Florianópolis, Brasil, 2023. Tese de doutorado em Relações Internacionais.

4 Conforme Ferreira Neto, o ciberespaço pode ser entendido a partir de três camadas: o *hardware*, que seriam os componentes do sistema; o *software*, que diz respeito aos sistemas e à programação; e a *peopleware*, que se refere às pessoas que atuam nesse ambiente. Ver: FERREIRA NETO, Walfredo Bento – «Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder». In *Revista das Ciências Militares, Coleção Meira Mattos*. Rio de Janeiro. Vol. 1, janeiro-abril de 2014, pp. 7-18. A *peopleware* seria a camada mais importante ou a base de sustentação do ciberespaço, conforme Grassi, já que «diferente dos demais espaços geográficos – terrestre, marítimo, aéreo e extra-atmosférico – que existem independentes da vontade humana, o ciberespaço é produto da ação humana, sua evolução ou transformação ao longo do tempo é devida à atuação do ser humano, que desenvolve e interage com o elemento físico e que, a partir dele, põe em funcionamento todos os seus sistemas» (GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...»).

5 O termo passou a ser utilizado como um substituto de Sul Global por autores que defendem a insuficiência analítica, a imprecisão semântica e a generalização do conceito e compreendem que este reforça as assimetrias e desigualdades da clivagem Norte-Sul. Nesse sentido, o uso do termo «Sul Geopolítico» busca «reforçar a agência dos atores do Sul, na medida em que traz uma imagem autoconstruída, a partir das leituras que eles têm das relações internacionais e de suas inserções». Ainda, «o conceito apresentado busca colocar essas disputas e tensões no centro da análise, convidando a uma leitura histórica das assimetrias, das relações de dominação, da exploração e da humilhação como fatores constitutivos das relações internacionais» (ver COSTA, Hugo Bras Martins da; DUARTE, Rubens de Siqueira – «Sul Global versus Sul Geopolítico: um debate quanto à pertinência analítica dos conceitos». In *Austral: Brazilian Journal of Strategy and International Relation*. Porto Alegre. Vol. 12, N.º 24, 2023, p. 24-25).

6 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

7 OLIVEIRA, Marcos Aurelio Guedes, et al. – *Guia de Defesa Cibernética da América do Sul*. Recife: Ed. UFPE, 2017.

8 AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil». In *Revista Brasileira de Estudos de Defesa*. Vol. 7, N.º 2, julho-dezembro de 2020, pp. 103-131.

9 NYE JR, Joseph S. – *The Future of Power*. Nova Iorque: Public Affairs, 2011; PORTELA, Lucas Soares – «Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI». Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2016. Dissertação de mestrado em Ciências Militares; FERREIRA NETO, Walfredo Bento – «Territorializando o "novo" e (re)territorializando os tradicionais...».

10 AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética...».

11 RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies*. Vol. 35, N.º 1, 2012, pp. 5-32.

12 OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo – «Propaganda computacional na prática: os casos de Estados Unidos,

França, Colômbia e Venezuela». In *XI Encontro Nacional Da Associação Brasileira de Estudos de Defesa* [online]. 2021, pp. 1-18.

13 WIGELL, Mikael – «Democratic deterrence: "how to dissuade hybrid interference». In *Washington Quarterly*. Vol. 44, N.º 1, 2021, pp. 49-67.

14 RID, Thomas – «Cyber war will not take place».

15 BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order…*; AYRES PINTO, Danielle Jacon; MORAES, Isabela – «As mídias digitais como ferramentas de manipulação…».

16 BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order…*.

17 Os atores citam os seguintes países: Austrália, Brasil, Colômbia, República Checa, Finlândia, França, Alemanha, Indonésia, Israel, Itália, Malta, Montenegro, Países Baixos, Macedónia do Norte, Noruega, Singapura, Espanha, Taiwan, Ucrânia e Estados Unidos da América.

18 HANSON, Fergus, et al. – *Hacking Democracies: Cataloguing Cyber-enabled Attacks on Elections*. Australian Strategic Policy Institute, policy brief, report n.º 16, 2019.

19 CURI JÚNIOR, Aribelco; ALFAYA, Natalia Maria Ventura da Silva – «O impacto das fake news nas eleições presidenciais de 2018 e 2022…».

20 GUTIÉRREZ-COBA, Liliana; RODRÍGUEZ-PÉREZ, Carlos – «Estrategias de posverdad y desinformación en las elecciones presidenciales colombianas 2022». In *Revista de Comunicación*. Vol. 22, N.º 2, 2023, pp. 225-242. Tradução livre dos autores.

21 RAULS, Leonie – «How Latin American governments are fighting fake news». In *Americas Quartely*. 19 de outubro de 2021. Consultado em: 12 de outubro de 2023. Disponível em: https://americasquarterly.org/article/how-latin-american-governments-are-fighting-fake-news/; CRIALES, José Pablo – «La inseguridad irrumpe en la campaña electoral argentina aupada por las noticias falsas en redes sociales». In *El País*. Buenos Aires, 11 de agosto de 2023. Consultado em: 12 de outubro de 2023. Disponível em: https://elpais.com/argentina/2023-08-11/la-inseguridad-irrumpe-en-la-campana-electoral-argentina-aupada-por-las-noticias-falsas-en-redes-sociales.html.

22 OLIVEIRA, Marcos Aurelio Guedes, et al. – *Guia de Defesa Cibernética da América do Sul*, p. 4.

23 FÓRUM ECONÔMICO MUNDIAL – *Global Risks Report 2024*. Genebra: Fórum Econômico Mundial, 2024. Consultado em: 28 de fevereiro de 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

24 WIGELL, Mikael – «Democratic deterrence…», p. 50. Tradução livre a partir do original.

25 WIGELL, Mikael – «Democratic deterrence…»; OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo – «Propaganda computacional na prática…»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

26 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 *Defesa Cibernética e Mobilização Nacional*. Recife: Ed. UFPE, 2020, pp. 153-174.

27 WIGELL, Mikael – «Democratic deterrence…», p. 53. Tradução livre a partir do original.

28 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

29 LIBICKI, Martin – *Cyberdeterrence and Cyberwar*. Pittsburgh: RAND Corporation, 2009; LIFF, Adam P. – «Cyberwar: a new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war». In *Journal of Strategic Studies*. Vol. 35, N.º 3, 2012, pp. 401-428; STONE, John – «Cyber war will take place!». In *Journal of Strategic Studies*. Vol. 36, N.º 1, 2013, pp. 101-108; RID, Thomas – «Cyber war will not take place»; AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética…».

30 SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South». In *Third World Quarterly*. Vol. 39, N.º 5, 2018, pp. 821-837; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges and global inequalities in cyber capacity building». In *Third World Quarterly*. Vol. 41, N.º 6, 2020, pp. 917-938.

31 MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*. Norwegian Institute for International Affairs (NUPI), Policy brief n.º 15, 2015, pp. 1-5; PAWLAK, Patryk – «Capacity building in cyberspace as an instrument of foreign policy». In *Global Policy*. Vol. 7, N.º 1, 2016, pp. 83-92; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building: conundrum and opportunity». In *Journal of Cyber Policy*. Vol. 2, N.º 1, 2017, pp. 123-144; BARRINHA, André; RENARD, Thomas – «Cyber-diplomacy: the making of an international society in the digital age». In *Global Affairs*. Vol. 3, N.º 4-5, 2017, pp. 353-364; HERZ, Monica – «Cibersegurança na América Latina». In *Conferência de Segurança Internacional do Forte de Copacabana – A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global*. Fundação Konrad Adenauer; Centro Brasileiro de Relações Internacionais. Coleção de Policy Papers, 2019, pp. 9-19; SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South»; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges…».

32 MIKSER, Sven – «La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: el camino a seguir». In *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, pp. 34-37.

33 PAWLAK, Patryk – «Capacity building in cyberspace as an instrument of foreign policy»; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building…»; HERZ, Monica – «Cibersegurança na América Latina».

34 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

35 MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*; SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South»; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges…»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

36 CEBALLOS, Luis Dario; MAISONNAVE, Marcelo Andrés; LONDOÑO, Carlos Rafael Britto – «Soberanía tecnológica digital en Latinoamérica». In *Revista Propuestas para el Desarrollo*. México. Ano IV, N.º IV, outubro de 2020, p. 152. Tradução livre a partir do original.

37 MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*; SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South»; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building…»; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges…».

38 CHENOU, Jean-Marie; FUERTE, Juan Sebastián Rojas – «The difficult path to the insertion of the Global South in Internet governance». In *Internet Governance in the Global South: History, Theory, and Contemporary Debates*. São Paulo: NUPRI/USP, 2018, pp. 42-73.

39 *Ibidem*; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building…»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

40 HERZ, Monica – «Cibersegurança na América Latina», p. 17.

41 Para aprofundamento sobre as iniciativas de cooperação e integração sul-americanas, recomenda-se: FUCCILLE, Alexandre – «O Brasil e a América do Sul: (re)pensando a segurança e a defesa na região». In *Revista Brasileira de Estudos de Defesa*. Vol. 1, N.º 1, 2014, pp. 112-146; PAGLIARI, Graciela de Conti – «Conselho de Defesa Sul-Americano e a adoção de

medidas de fortalecimento da confiança». In *Carta Internacional*. Belo Horizonte. Vol. 10, N.º 3, 2015, p. 23; TEIXEIRA JÚNIOR, Augusto Wagner Menezes – «Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar». In *Revista Política Hoje*. Vol. 24, N.º 1, 2015, pp. 57-70; BRICEÑO-RUIZ, José – «Da crise da pós-hegemonia ao impacto da covid-19: o impasse do regionalismo latino-americano». In *Revista Cadernos de Campo*. Araraquara. N.º 29, julho-dezembro de 2020, pp. 21-39; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas – «A cooperação em segurança e defesa na América do Sul a partir de 2016: desafios e perspectivas». In *Revista Brasileira de Estudos Estratégicos*. Niterói. Vol. 16, N.º 26, 2021, pp. 25-49; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global: desestabilização e (des)integração sul-americana». In *Conjuntura Austral*. Porto Alegre. Vol. 12, N.º 61, 2022, pp. 33-46.

42 JUSTRIBÓ, Candela – «Ciberdefensa: una visión desde la UNASUR». In *VII Congreso del Instituto de Relaciones Internacionales*. La Plata, 2014, pp. 1-24; GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética?». In *Austral: Revista Brasileira de Estratégia e Relações Internacionais*. Porto Alegre. Vol. 7, N.º 14, julho-dezembro de 2018, pp. 217-241.

43 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

44 JUSTRIBÓ, Candela – «Ciberdefensa...»; OLIVEIRA, Marcos Aurelio Guedes, et al. – *Guia de Defesa Cibernética da América do Sul*; GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano...»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

45 JUSTRIBÓ, Candela – «Ciberdefensa...».

46 VAN RAEMDONCK, Nathalie – *Cyber Diplomacy in Latin America*. UE Cyber Direct, Digital Dialogue, 26 de junho de 2020, pp. 4-37. Consultado em: 6 de agosto de 2023. Disponível em: https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america.

47 SFORZIN, Verónica Elena – «El rol de los organismos regionales: Celac, Mercosur y Alianza del Pacifico, frente a las Tecnologías de la Información y la Comunicación en el periodo del 2005 al 2015». Universidad Nacional de La Plata, Provincia de Buenos Aires, 2020. Tese de doutorado em Comunicação.

48 GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano...».

49 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

50 MERCOSUL – Agenda Digital. Consultado em: 6 de agosto de 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/.

51 JUSTRIBÓ, Candela – «Ciberdefensa...»; GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano...»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

52 NEVES, Bárbara Carvalho; HONÓRIO, Karen – «Latin American regionalism under the new right». In *E-International Relations*. 27 de setembro de 2019, pp. 1-6. Disponível em: https://www.e-ir.info/pdf/80118; BRICEÑO-RUIZ, José – «Da crise da pós-hegemonia ao impacto da covid-19...»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

53 SOUZA, Tamires Aparecida Ferreira – «Cooperação em Defesa e a Região Sul-americana: O Papel do Conselho de Defesa Sul-Americano da UNASUL». Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015. Dissertação de mestrado em Estudos Estratégicos Internacionais; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

54 JUSTRIBÓ, Candela – «Ciberdefensa...».

55 HERZ, Monica – «Cibersegurança na América Latina», p. 17.

56 ORGANIZAÇÃO DOS ESTADOS AMERICANOS – «Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética" Aprobada en la Cuarta Sesión Plenaria, celebrada el 8 de junio de 2004». Washington DC, Estados Unidos de América, 2004. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp; ORGANIZAÇÃO DOS ESTADOS AMERICANOS – Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio, 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oascybercbms.org/es; ORGANIZAÇÃO DOS ESTADOS AMERICANOS – *Programa de Ciberseguridad*. 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp.

57 NEVES, Bárbara Carvalho; HONÓRIO, Karen – «Latin American regionalism under the new right»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

58 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

59 TEIXEIRA JÚNIOR, Augusto Wagner Menezes – «Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas – «A cooperação em segurança e defesa na América do Sul...»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

BIBLIOGRAFIA

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil». In *Revista Brasileira de Estudos de Defesa*. Vol. 7, N.º 2, julho-dezembro de 2020, pp. 103-131. DOI: https://doi.org/10.26792/rbed.v7n2.2020.75178.

AYRES PINTO, Danielle Jacon; MORAES, Isabela – «As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit». In *Revista de Estudios Sociales*. Bogotá. N.º 74, outubro-dezembro de 2020, pp. 71-82. DOI: https://doi.org/10.7440/res74.2020.06.

BARRINHA, André; RENARD, Thomas – «Cyber-diplomacy: the making of an international society in the digital age». In *Global Affairs*. Vol. 3, N.º 4-5, 2017, pp. 353-364. DOI: https://doi.org/10.1080/23340460.2017.1414924.

BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. University of Oxford, Computational Propaganda Research Project, working paper, report n.º 19, 2019.

BRICEÑO-RUIZ, José – «Da crise da pós-

-hegemonia ao impacto da covid-19: o impasse do regionalismo latino-americano». In *Revista Cadernos de Campo*. Araraquara. N.º 29, julho-dezembro de 2020, pp. 21-39. DOI: https://doi.org/10.47284/2359-2419.2020.29.2139.

CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges and global inequalities in cyber capacity building». In *Third World Quarterly*. Vol. 41, N.º 6, 2020, pp. 917-938. DOI: https://doi.org/10.1080/01436597.2020.1729729.

CEBALLOS, Luis Dario; MAISONNAVE, Marcelo Andrés; LONDOÑO, Carlos Rafael Britto – «Soberanía tecnológica digital en Latinoamérica». In *Revista Propuestas para el Desarrollo*. México. Ano IV, N.º IV, outubro de 2020, pp. 151-167.

CHENOU, Jean-Marie; FUERTE, Juan Sebastián Rojas – «The difficult path to the insertion of the Global South in Internet governance». In *Internet Governance in the Global South: History, Theory, and Contemporary Debates*. São Paulo: NUPRI/USP, 2018, pp. 42-73.

COSTA, Hugo Bras Martins da; DUARTE, Rubens de Siqueira – «Sul Global versus Sul Geopolítico: um debate quanto à pertinência analítica dos conceitos». In *Austral: Brazilian Journal of Strategy and International Relation*. Porto Alegre. Vol. 12, N.º 24, 2023, pp. 13-35. DOI: https://doi.org/10.22456/2238-6912.132863.

CRIALES, José Pablo – «La inseguridad irrumpe en la campaña electoral argentina aupada por las noticias falsas en redes sociales». In *El País*. Buenos Aires, 11 de agosto de 2023. Consultado em: 12 de outubro de 2023. Disponível em: https://elpais.com/argentina/2023-08-11/la-inseguridad-irrumpe-en-la-campana-electoral-argentina-aupada-por-las-noticias-falsas-en-redes-sociales.html.

CURI JÚNIOR, Aribelco; ALFAYA, Natalia Maria Ventura da Silva – «O impacto das fake news nas eleições presidenciais de 2018 e 2022: prejuízos para a democracia e a sociedade». In *Revista do Instituto de Direito Constitucional e Cidadania*. Paraná. Vol. 8, N.º 1, janeiro-junho de 2023, pp. 1-11. DOI: https://doi.org/10.48159/revistadoidcc.v8n1.e079.

FERREIRA NETO, Walfredo Bento – «Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder». In *Revista das Ciências Militares, Coleção Meira Mattos*. Rio de Janeiro. Vol. 1, janeiro-abril de 2014, pp. 7-18.

FÓRUM ECONÔMICO MUNDIAL – *Global Risks Report 2024*. Genebra: Fórum Econômico Mundial, 2024. Consultado em: 28 de fevereiro de 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

FUCCILLE, Alexandre – «O Brasil e a América do Sul: (re)pensando a segurança e a defesa na região». In *Revista Brasileira de Estudos de Defesa*. Vol. 1, N.º 1, 2014. pp. 112-146.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética?». In *Austral: Revista Brasileira de Estratégia e Relações Internacionais*. Porto Alegre. Vol. 7, N.º 14, julho-dezembro de 2018, pp. 217-241. DOI: https://doi.org/10.22456/2238-6912.87994.

GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas e os Processos Cooperativos no Contexto Geopolítico Sul-Americano». Universidade Federal de Santa Catarina, Florianópolis, Brasil, 2023. Tese de doutorado em Relações Internacionais.

GUTIÉRREZ-COBA, Liliana; RODRÍGUEZ-PÉREZ, Carlos – «Estrategias de posverdad y desinformación en las elecciones presidenciales colombianas 2022». In *Revista de Comunicación*. Vol. 22, N.º 2, 2023, pp. 225-242. DOI: https://doi.org/10.26441/RC22.2-2023-3270.

HANSON, Fergus; O'CONNOR, Sara; WALKER, Mali; COURTOIS, Luke – *Hacking Democracies: Cataloguing Cyber-enabled Attacks on Elections*. Australian Strategic Policy Institute, policy brief, report n.º 16, 2019, pp. 3-30.

HERZ, Monica – «Cibersegurança na América Latina». In *Conferência de Segurança Internacional do Forte de Copacabana – A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global*. Fundação Konrad Adenauer; Centro Brasileiro de Relações Internacionais. Coleção de Policy Papers, 2019, pp. 9-19.

JUSTRIBÓ, Candela – «Ciberdefensa: una visión desde la UNASUR». In *VII Congreso del Instituto de Relaciones Internacionales*. La Plata, 2014, pp. 1-24.

LIBICKI, Martin – *Cyberdeterrence and Cyberwar*. Pittsburgh: RAND Corporation, 2009.

LIFF, Adam P. – «Cyberwar: a new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war». In *Journal of Strategic Studies*. Vol. 35, N.º 3, 2012, pp. 401-428. DOI: https://doi.org/10.1080/01402390.2012.663252.

MERCOSUL – Agenda Digital. Consultado em: 6 de agosto de 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/.

MIKSER, Sven – «La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: el camino a seguir». In *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, pp. 34-37.

MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global: desestabilização e (des)integração sul-americana». In *Conjuntura Austral*. Porto Alegre. Vol. 12, N.º 61, 2022, pp. 33-46. DOI: https://doi.org/10.22456/2178-8839.113748.

MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas – «A cooperação em segurança e defesa na América do Sul a partir de 2016: desafios e perspectivas». In *Revista Brasileira de Estudos Estratégicos*. Niterói. Vol. 16, N.º 26, 2021, pp. 25-49. DOI: https://doi.org/10.29327/230731.13.26-2.

MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*. Norwegian Institute for International Affairs (NUPI), Policy brief n.º 15, 2015, pp. 1-5.

NEVES, Bárbara Carvalho; HONÓRIO, Karen – «Latin American regionalism under the new right». In *E-International Relations*. 27 de setembro de 2019. Disponível em: https://www.e-ir.info/pdf/80118.

NYE JR, Joseph S. – *The Future of Power*. Nova Iorque: Public Affairs, 2011.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – «Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética" Aprobada en la Cuarta Sesión Plenaria, celebrada el 8 de junio de 2004». Washington DC, Estados Unidos de América, 2004. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio, 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oascybercbms.org/es.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – *Programa de Ciberseguridad*. 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp.

OLIVEIRA, Marcos Aurélio Guedes; 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.

OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo – «Propaganda computacional na prática: os casos de Estados Unidos, França, Colômbia e Venezuela». In *XI Encontro Nacional Da Associação Brasileira de Estudos de Defesa* [online]. 2021, pp. 1-18.

PAGLIARI, Graciela de Conti – «Conselho de Defesa Sul-Americano e a adoção de medidas de fortalecimento da confiança». In *Carta Internacional*. Belo Horizonte. Vol. 10, N.º 3, 2015, pp. 23-40. DOI: https://doi.org/10.21530/ci.v10n3.2015.307.

PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; VIGGIANO, Juliana – «Mobilização nacional, ameaças ciberné-

ticas e redes de interação num modelo de tríplice hélice estratégica: um estudo prospectivo». In *Defesa Cibernética e Mobilização Nacional*. Recife: Ed. UFPE, 2020, pp. 153-174.

PAWLAK, Patryk – «Capacity building in cyberspace as an instrument of foreign policy». In *Global Policy*. Vol. 7, N.º 1, 2016, pp. 83-92. DOI: https://doi.org/10.1111/1758-5899.12298.

PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building: conundrum and opportunity». In *Journal of Cyber Policy*. Vol. 2, N.º 1, 2017, pp. 123-144. DOI: https://doi.org/10.1080/23738871.2017.1294610.

PORTELA, Lucas Soares – «Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI». Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2016. Dissertação de mestrado em Ciências Militares.

RAULS, Leonie – «How Latin American governments are fighting fake news». In *Americas Quartely*. 19 de outubro de 2021. Consultado em: 12 de outubro de 2023. Disponível em: https://americasquarterly.org/article/how-latin-american-governments-are-fighting-fake-news/.

RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies*. Vol. 35, N.º 1, 2012, pp. 5-32. DOI: https://doi.org/10.1080/01402390.2011.608939.

SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South». In *Third World Quarterly*. Vol. 39, N.º 5, 2018, pp. 821-837. DOI: https://doi.org/10.1080/01436597.2017.1408403.

SFORZIN, Verónica Elena – «El rol de los organismos regionales: Celac, Mercosur y Alianza del Pacifico, frente a las Tecnologías de la Información y la Comunicación en el periodo del 2005 al 2015». Universidad Nacional de La Plata, Provincia de Buenos Aires, 2020. Tese de doutorado em Comunicação.

SOUZA, Tamires Aparecida Ferreira – «Cooperação em Defesa e a Região Sul-americana: O Papel do Conselho de Defesa Sul-Americano da UNASUL». Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015. Dissertação de mestrado em Estudos Estratégicos Internacionais.

STONE, John – «Cyber war will take place!». In *Journal of Strategic Studies*. Vol. 36, N.º 1, 2013, pp. 101-108. DOI: https://doi.org/10.1080/01402390.2012.730485.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes – «Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar». In *Revista Política Hoje*. Vol. 24, N.º 1, 2015, pp. 57-70.

VAN RAEMDONCK, Nathalie – *Cyber Diplomacy in Latin America*. UE Cyber Direct, Digital Dialogue, 26 de junho de 2020, pp. 4-37. Consultado em: 6 de agosto de 2023. Disponível em: https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america.

WIGELL, Mikael – «Democratic deterrence: ¨how to dissuade hybrid interference». In *Washington Quarterly*. Vol. 44, N.º 1, 2021, pp. 49-67. DOI: https://doi.org/10.1080/0163660X.2021.1893027.