UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Jéssica Maria Grassi

A construção de capacidades cibernéticas e os processos cooperativos no contexto geopolítico sul-americano: políticas e estratégias de Argentina, Brasil e Colômbia

Florianópolis
2023

Jéssica Maria Grassi

A construção de capacidades cibernéticas e os processos cooperativos no contexto geopolítico sul-americano: políticas e estratégias de Argentina, Brasil e Colômbia

Tese apresentada ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Doutora em Relações Internacionais.

Orientador: Profª. Drª. Danielle Jacon Ayres Pinto

Florianópolis
2023

Grassi, Jéssica Maria
A construção de capacidades cibernéticas e os processos cooperativos no contexto geopolítico sul-americano : políticas e estratégias de Argentina, Brasil e Colômbia / Jéssica Maria Grassi ; orientadora, Danielle Jacon Ayres Pinto, 2023.
251 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Programa de Pós-Graduação em Relações Internacionais, Florianópolis, 2023.

Inclui referências.

1. Relações Internacionais. 2. Capacidade cibernética. 3. Geopolítica cibernética. 4. Diplomacia cibernética. 5. Cooperação sul-americana. I. Ayres Pinto, Danielle Jacon. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

Jéssica Maria Grassi

A construção de capacidades cibernéticas e os processos cooperativos no contexto geopolítico sul-americano: políticas e estratégias de Argentina, Brasil e Colômbia

O presente trabalho em nível de Doutorado foi avaliado e aprovado, em 24 de novembro de 2023, pela banca examinadora composta pelos seguintes membros:

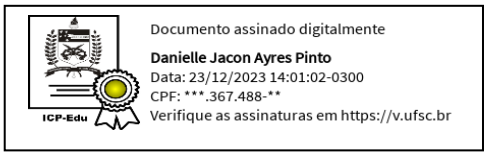
Prof.ª Dr.ª Graciela de Conti Pagliari
Universidade Federal de Santa Catarina (UFSC)

Prof.ª Dr.ª Cristina Soreanu Pecequilo
Universidade Federal de São Paulo (UNIFESP)

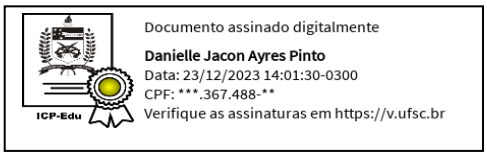
Prof.ª Dr.ª Selma Lúcia de Moura Gonzales
Escola Superior de Defesa (ESD)

Prof.ª Dr.ª Sabrina Evangelista Medeiros
Universidade Lusófona de Lisboa

Certificamos que esta é a versão original e final da tese que foi julgada adequada para obtenção do título de Doutora em Relações Internacionais.



Coordenação do Programa de Pós-Graduação



Prof.ª Dr.ª Danielle Jacon Ayres Pinto
Orientador(a)

Florianópolis, 2023

Aos meus pais,
Natalia Szidloski Grassi e Ozires Grassi,
por seu apoio incondicional.

AGRADECIMENTOS

Agradeço, mais que tudo, aos meus pais, Natália e Ozires, pelo apoio em todas as minhas decisões e pelo incentivo para que sempre perseguisse meus sonhos. Graças a vocês pude chegar até aqui! Vocês são minha base, minha maior inspiração!

Agradeço imensamente ao meu noivo, Everton, por enfrentar comigo esse desafio, pelo companheirismo, apoio, paciência e compreensão em todos os momentos desta jornada. Você é fundamental para as minhas conquistas!

Sou (muito) grata a minha orientadora, Profa. Danielle, pela amizade construída, pelos ensinamentos e conselhos, pelas oportunidades e pela confiança, por sempre acreditar em mim e no meu trabalho. Foi um presente ter sido sua orientanda! Você é uma inspiração!

Agradeço às professoras da Banca, professoras Graciela, Cristina, Selma e Sabrina, por aceitarem fazer parte desse momento tão importante, por ler minha pesquisa com tanta atenção, por compartilhar seus conhecimentos, pelas sugestões e pelas palavras gentis.

Agradeço também a todos(as) os professores e técnicos administrativos do PPGRI e da UFSC que contribuíram para que essa jornada de 4 anos e 9 meses fosse tão rica. Minha passagem pelo PPGRI, pela UFSC e por Florianópolis foi um capítulo lindo da minha vida!

Aos colegas do PPGRI e do GEPPIC, que compartilharam momentos de estudo, pesquisa e construção de conhecimentos, mas também de descontração - principalmente Renata e Janypher - agradeço por tornarem essa caminhada mais leve. A todos(as) os(as) amigos(as) que estiveram presentes, mesmo à distância, agradeço pela torcida e pelo suporte nos momentos mais difíceis.

Da mesma forma, faço um agradecimento aos(as) colegas e aos(as) alunos(as) da FURG quem tive o prazer de conviver e aprender durante os quatro semestres nos quais estive como professora substituta. Um agradecimento especial a Mayra e a Gabriela, pelas conversas, conselhos e pelo auxílio nos momentos em que já estava exausta da jornada dupla (ou tripla). As amizades que construí em Santa Vitória do Palmar tornaram os dois anos finais desse doutorado ainda mais inesquecíveis. Levo cada um de vocês no meu coração!

Agradeço a todos os colegas, professores e alunos que fizeram crescer em mim o amor ao ensino e à pesquisa. Sou muito feliz nesse caminho que escolhi trilhar! Em minha trajetória acadêmica e profissional, até agora, tive o privilégio de passar pela UFSM, UNILA, UFSC e FURG e sou eternamente grata à Universidade Pública, gratuita e de qualidade,

Por fim, sou grata à bolsa de pesquisa concedida a mim pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que tornou possível a construção dessa pesquisa, a qual espero que possa ser uma contribuição significativa à área das Relações Internacionais e áreas afins.

RESUMO

O século XXI trouxe novos desafios e novas demandas para o desenvolvimento socioeconômico, para a segurança e a defesa dos Estados e, na realidade, para o funcionamento da sociedade contemporânea. Isso porque as novas tecnologias e os recursos cibernéticos passaram a moldar todos os aspectos da vida em sociedade e tornaram-se substanciais nas dinâmicas de poder e, portanto, nas Relações Internacionais. Diante disso, a construção de capacidades cibernéticas passa a ser central para a promoção de desenvolvimento, a manutenção da segurança e da defesa e a obtenção de poder no cenário internacional. Contudo, a construção de capacidades cibernéticas é um campo dinâmico, no qual os diversos contextos e realidades sociais, econômicas e políticas dos países devem ser observados. Esta não pode, portanto, ser resumida a questões tecnológicas, uma vez que envolve múltiplos fatores, desde questões legais, técnicas, políticas e diplomáticas, fatores institucionais e organizacionais, assim como os conhecimentos, habilidades e o desenvolvimento científico. Fatores que devem ser fomentados a partir de estratégias coerentes e sustentadas ao longo do tempo. No entanto, países em desenvolvimento, como é o caso dos sul-americanos, enfrentam diversas fragilidades estruturais que dificultam o processo de construção de cibercapacidades e que os deixam ainda mais vulneráveis diante das novas dinâmicas cibernéticas. Frente ao exposto e compreendendo o histórico de cooperação na América do Sul, esta investigação tem como propósito analisar as potencialidades para desenvolvimento de processos de cooperação cibernética na região com vistas à construção de cibercapacidades. Partindo disso, a pergunta central da pesquisa foi delimitada da seguinte forma: Quais as potencialidades para a construção de capacidades cibernéticas na América do Sul por meio de processos cooperativos se analisado o contexto geopolítico regional e, particularmente, se comparadas as políticas e estratégias cibernéticas da região? Diante da delimitação proposta, além da análise do cenário geopolítico regional, foram escolhidos, como objetos para aprofundamento da pesquisa, três países: Argentina, Brasil e Colômbia. Desse modo, será possível analisar suas políticas e estratégias observando elementos de convergências e divergências, além de investigar os níveis de capacitação desses países, explorando elementos de complementariedades. A investigação parte da hipótese de que existem similaridades nos desafios que os países sul-americanos enfrentam e complementariedades no setor cibernético que tornam um processo de cooperação regional um meio viável para a redução das fragilidades individuais na construção de capacidade cibernética. Além disso, observando o cenário regional, acredita-se que as dinâmicas cooperativas entre as nações sul-americanas nas últimas décadas são demonstrativos do potencial da região para a construção de processos cooperativos também na área cibernética. Observam-se complexos obstáculos a serem superados para a implementação efetiva das propostas evidenciadas. Entretanto, contemplam-se também diversas oportunidades para traçarem estratégias cooperativas no campo cibernético, nas quais os países possam somar esforços, compartilhar experiências e conhecimentos e reduzir sua dependência por soluções externas. Isso torna-se crucial para que os Estados possam superar suas lacunas, garantir sua soberania digital e aumentar sua segurança e seu poder cibernético.

Palavras-chave: capacidade cibernética; geopolítica cibernética; poder cibernético. diplomacia cibernética; cooperação sul-americana.

ABSTRACT

The 21st century has brought new challenges and new demands for socioeconomic development, the security and defense of States, and the functioning of contemporary society. This is because new technologies and cyber resources have come to shape all aspects of life in society and have become substantial in power dynamics and, therefore, in International Relations. In view of this, cyber capacity building becomes central to promoting development, maintaining security and defense, and obtaining power in the international system. Cyber capacity building, however, is a dynamic field, in which the different social, economic, and political contexts and realities of countries must be observed. This cannot, therefore, be merely summarized as technological issues, as it involves multiple factors, including legal, technical, political and diplomatic issues, institutional and organizational factors, as well as knowledge, skills and scientific development. Moreover, these factors must be encouraged through coherent and sustained strategies over time. However, developing countries, such those in South America, face several structural weaknesses that complicate the processes of building cyber capabilities and leave them even more vulnerable in the face of new cyber dynamics. Considering the above and understanding the history of cooperation in South America, this investigation aims to analyze the potential for developing cyber cooperation processes in the region with the goal of building cyber capacity. Based on this, the central research question was established as follows: What are the potentials for building cyber capabilities in South America through cooperative processes if the regional geopolitical context is analyzed and, particularly, if the region's cyber policies and strategies are compared? Given the proposed delimitation, in addition to the analysis of the regional geopolitical scenario, three countries were chosen as objects for further research: Argentina, Brazil and Colombia. In this way, it will be possible to analyze their policies and strategies by observing elements of convergence and divergence, in addition to investigating the level of capacity of these countries, exploring elements of complementarity. The investigation is based on the hypothesis that there are similarities in the challenges that South American countries face and complementarities in the cyber sector that make the process of regional cooperation a viable means of reducing individual weaknesses in building cyber capacity. Furthermore, observing the regional scenario, it is believed that the cooperative dynamics between South American nations in recent decades demonstrate the region's potential for building cooperative processes also in the cyber sector. There are complex obstacles to be overcome by countries in order to effectively implement the proposals highlighted. However, there are also several opportunities to outline cooperative strategies in the cyber field, in which countries can join efforts, share experiences and knowledge, and reduce their dependence on external solutions. This becomes crucial for States to overcome their gaps, guarantee their digital sovereignty, and increase their security and cyber power.

Keywords: cybersecurity capacity; cyber geopolitics; cyber power; cyber diplomacy; south american cooperation.

RESUMEN

El siglo XXI ha traído nuevos desafíos y nuevas demandas para el desarrollo socioeconómico, para la seguridad y defensa de los Estados y, en realidad, para el funcionamiento de la sociedad contemporánea. Esto se debe a que las nuevas tecnologías y los recursos cibernéticos han llegado a moldear todos los aspectos de la vida en sociedad y se han vuelto sustanciales en las dinámicas de poder y, por tanto, en las Relaciones Internacionales. En vista de esto, la construcción de capacidades cibernéticas se vuelve central para promover el desarrollo, mantener la seguridad y la defensa y obtener poder en el escenario internacional. La construcción de capacidades cibernéticas, sin embargo, es un campo dinámico, en el que se deben observar los diferentes contextos y realidades sociales, económicas y políticas de los países. Por lo tanto, esto no puede resumirse en cuestiones tecnológicas, ya que implica múltiples factores, entre ellos cuestiones jurídicas, técnicas, políticas y diplomáticas, factores institucionales y organizativos, así como conocimientos, capacidades y desarrollo científico. Factores que deben ser incentivados a través de estrategias coherentes y sostenidas en el tiempo. Sin embargo, los países en desarrollo, como los sudamericanos, enfrentan varias debilidades estructurales que complican el proceso de creación de capacidades cibernéticas y los dejan aún más vulnerables frente a las nuevas dinámicas cibernéticas. Teniendo en cuenta lo anterior y entendiendo la historia de la cooperación en América del Sur, esta investigación tiene como objetivo analizar el potencial para desarrollar procesos de cooperación en la región con la intención de construir cibercapacidades. Con base en esto, la pregunta central de investigación quedó delimitada de la siguiente manera: ¿Cuáles son las posibilidades de construir capacidades cibernéticas en América del Sur a través de procesos cooperativos si se analiza el contexto geopolítico regional y, particularmente, si se comparan las políticas y estrategias cibernéticas de la región? Dada la delimitación propuesta, además del análisis del escenario geopolítico regional, se eligieron tres países como objetos para profundizar la investigación: Argentina, Brasil y Colombia. De esta manera, será posible analizar sus políticas y estrategias observando elementos de convergencia y divergencia, además de investigar los niveles de capacitación en estos países, explorando elementos de complementariedad. La investigación se basa en la hipótesis de que existen similitudes en los desafíos que enfrentan los países sudamericanos y complementariedades en el sector cibernético que hacen que un proceso de cooperación regional sea un medio viable para reducir las debilidades individuales en el desarrollo de capacidades cibernéticas. Además, observando el escenario regional, se cree que las dinámicas cooperativas entre las naciones sudamericanas en las últimas décadas demuestran el potencial de la región para construir procesos cooperativos también en el área cibernética. Hay obstáculos complejos que los países deben superar para implementar efectivamente las propuestas destacadas. Sin embargo, también existen varias oportunidades para delinear estrategias de cooperación en el campo cibernético, en las que los países puedan unir esfuerzos, compartir experiencias y conocimientos y reducir su dependencia de soluciones externas. Esto se vuelve crucial para que los Estados avancen hacia la superación de sus brechas, garantizando su soberanía digital y aumentando su seguridad y su poder cibernético.

Palabras-clave: cibercapacidades; geopolítica cibernética; poder cibernético; ciberdiplomacia; cooperación sudamericana.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

APF	Administração Pública Federal
ALALC	Associação Latino-americana de Livre Comércio
ALADI	Associação Latino-Americana de Integração
ALBA	Aliança Bolivariana para os Povos de Nossa América
ASEAN	Associação das Nações do Sudeste Asiático
BID	Banco Interamericano de Desenvolvimento
BRICS	Brasi, Rússia, Índia, China, África do Sul
CAN	Comunidade Andina de Nações
CASA/CSN	Comunidade Sul-Americana de Nações
CCDCoE	*Cooperative Cyber Defence Centre of Excellence*
CCMM	*Cybersecurity Capacity Maturity Model for Nations*
CCCD	Comando Conjunto de Ciberdefesa de Argentina
CCOC	Comando Conjunto Cibernético de Colombia
CDC	Comitê de Defesa Cibernética da OTAN
CDCiber	Centro de Defesa Cibernética
CDMB	Conselho de Administração de Defesa Cibernética da OTAN
CDS	Conselho de Defesa Sul-Americano
CE	Conselho da Europa
CEAP	Plano de Ação para a Educação em Cibersegurança
CEED	Centro de Estudos Estratégicos de Defesa
CELAC	Comunidade dos Estados Latino-Americanos e Caribenhos
CERT	*Computer Emergency Response Team*
C&T	Ciência & Tecnologia
CGSIC	Coordenação-Geral de Segurança das Infraestruturas Críticas
CONPES	Conselho Nacional de Política Econômica e Social
CSIRT	*Computer Security Incident Response Team*
CCP	Centro Cibernético Policial de Colombia
ColCERT	Grupo de Resposta a Emergências Cibernéticas de Colombia
ComDCiber	Comando de Defesa Cibernética
DDL	Nível de Desenvolvimento Digital

DDoS	Distributed Denial-of-Service Attack
DMDC	Doutrina Militar de Defesa Cibernética
DNP	Departamento Nacional de Planejamento de Colombia
DCI	Departamento de Segurança Cibernética
DSI	Departamento de Segurança da Informação
E-Ciber	Estratégia Nacional de Segurança Cibernética
eGA	e-Governance Academy
EMCFA	Estado-Maior Conjunto das Forças Armadas
ENaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
ESUDE	Escola Sul-Americana de Defesa
EUA	Estados Unidos da América
FOCEM	Fundo para a Convergência Estrutural do Mercosul
GCI	Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum on Cyber Expertise
GGE	Group of Governmental Experts
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IA	Inteligência Artificial
IC	Infraestruturas Críticas
IoT	Internet of Things
IIRSA	Iniciativa para a Integração da Infraestrutura Sul-Americana
INTERPOL	Organização Internacional de Polícia Criminal
JID	Junta Interamericana de Defesa
LBDN	Livro Branco de Defesa Nacional
LGPD	Lei Geral de Proteção de Dados
MD	Ministério da Defesa
MERCOSUL	Mercado Comum do Sul
MinTIC	Ministério das Tecnologias de Informação e Telecomunicações de Colômbia
NSA	National Security Agency
NCSI	National Cyber Security Index
OCDE	Organização para a Cooperação e Desenvolvimento Econômico

OCS	Organização de Cooperação de Shangai
OEA	Organização dos Estados Americanos
OEWG	Open-Ended Working Group
OND	Objetivos Nacionais de Defesa
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
OTCA	Organização do Tratado de Cooperação Amazônica
PCD	Política Cibernética de Defesa
PCSD	Política Comum de Segurança e Defesa
P&D	Pesquisa & Desenvolvimento
PD&I	Pesquisa, Desenvolvimento & Inovação
PEA	População Economicamente Ativa
PIB	Produto Interno Bruto
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
PSI	Política de Segurança da Informação
PTT	Pontos de Troca de Internet
SAGAE	Secretaria de Acompanhamento e Gestão de Assuntos Estratégicos
SCADA	Supervisory Control and Data Acquisition
SENA	Serviço Nacional de Aprendizagem de Colômbia
SENAI	Serviço Nacional de Aprendizagem Industrial
SMDC	Sistema Militar de Defesa Cibernética
SSIC	Secretaria de Segurança Informática e Cibernética
STD	Soberania Tecnológica Digital
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TCU	Tribunal de Contas da União
TIAR	Tratado Interamericano de Assistência Recíproca
TI	Tecnologias de Informação
TICs	Tecnologias de Informação e Comunicação
UE	União Europeia
UIT	União Internacional de Telecomunicações
UNASUL	União das Nações Sul-Americanas

SUMÁRIO

1 INTRODUÇÃO

Nas dinâmicas contemporâneas, capacidades cibernéticas bem desenvolvidas são fundamentais para que os países progridam e se desenvolvam em todas as esferas, uma vez que o ciberespaço impacta a maioria dos aspectos da economia, da segurança e da defesa, da política nacional, regional e global, assim como traz importantes impactos sociais. A interconectividade dos sistemas e a baixa 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. Os contínuos avanços em termos de ameaças cibernéticas levam ao aumento de sua potencialidade de afetar diretamente as infraestruturas críticas (IC) dos Estados e o cotidiano da população.

Essa conjuntura e a potencialidade dos danos que essas ações podem causar provocam cenários desestabilizadores particularmente importantes nos países em desenvolvimento, como é o caso dos países da América do Sul. Tais países possuem fragilidades estruturais que os deixam mais vulneráveis diante de ataques e dificultam sua capacitação em termos de segurança e defesa cibernética. Além disso, diante do acirramento da competição estratégica entre as principais potências mundiais, as regiões periféricas passam a sofrer significativos impactos geopolíticos. A América do Sul, por sua importância estratégica para os Estados Unidos, assim como para Rússia e China, permanece em uma posição central frente a esses processos (AGUIRRE; CHAVEZ; ROBLEDO, 2020; TEIXEIRA Jr., 2020b; MORAIS DA SILVA; GRASSI, 2022).

Se por um lado, há o aumento das ameaças e das incertezas para os Estados, por outro lado, os recursos cibernéticos têm se tornado centrais nas dinâmicas de poder no século XXI, tendo a particularidade de serem mais baratos se comparados com os tradicionais recursos cinéticos de poder (como os armamentos nucleares), o que os torna particularmente importantes para países em desenvolvidos. Tais países podem ver no ciberespaço alternativas para seu processo de desenvolvimento e para melhorar seu posicionamento nas dinâmicas de poder internacionais. Porém, a construção efetiva de tais capacidades exige a restruturação do pensamento estratégico visando elencar suas prioridades e estabelecer novos moldes de atuação.

Frente a esse cenário, tem-se observado dois grandes direcionamentos no que diz respeito à construção de capacidade cibernética (no inglês CCB, *Cyber Capacity Building*) pelos atores estatais. Ressalta-se, entretanto, que esses direcionamentos não são mutuamente

excludentes, nem necessariamente divergentes, mas podem ser complementares. Um deles reflete a construção de capacidades perseguida de modo individualizado – podendo ser competitiva e conflitiva - pelos países, demarcada pelas incertezas e desconfianças que o ciberespaço aflora e sua potencialidade de causar danos efetivamente sérios aos Estados e a sua população. Nessa lógica, mais presente nos estudos sobre a temática, aborda-se a securitização e militarização do ciberespaço, reforçando este espaço como um novo domínio para realização de guerras e frequentemente relacionando as capacidades cibernéticas com a ótica securitária tradicional. Nesse direcionamento, discute-se sobre conflitos, armas cibernéticas, dissuasão cibernética e até mesmo sobre as possibilidades de uma corrida armamentista cibernética vir a se desenvolver (LIBICKI, 2009; RID, 2012; LIFF, 2012; CARNEIRO, 2012; POOL, 2013; STONE, 2013; SINGER; FRIEDMAN, 2014).

Por outro lado, outras perspectivas têm tomado forma, ressaltando a necessidade de propor novas alternativas para a construção de capacidades cibernéticas, principalmente refletindo sobre os países menos desenvolvidos, atentando que a era digital demanda múltiplas e diferenciadas respostas (GADY; AUSTIN, 2010; CALDERARO; CRAIG, 2020). Diante disso, destacam-se visões que apontam para dinâmicas cooperativas, desenvolvimento de parcerias, ações coordenadas entre os atores (estatais e não estatais) e os diversos setores da sociedade, bem como o desenvolvimento da diplomacia cibernética. Justifica-se o caráter transnacional dessa esfera, a interdependência entre os atores e as características intrínsecas desse ambiente para fortalecer temáticas relacionadas à governança cibernética, a construção da confiança entre os atores e o desenvolvimento de processos cooperativos (MULLER, 2015; PAWLAK, 2016; BARRINHA; RENARD, 2017; PAWLAK; BARMPALIOU, 2017; SCHIA, 2018; CALDERARO; CRAIG, 2020; GRASSI; AYRES PINTO, 2022a).

Partindo dessas constatações e 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), um marco regional, e as novas agendas postas no Mercosul nas últimas duas décadas -, os avanços que tais processos proporcionaram no auge de seus funcionamentos e pensando nas fragilidades que os Estados sul-americanos precisam superar para avançar na construção de capacidades, entende-se que a segunda abordagem proposta pode se apresentar como um caminho para a construção de capacidades cibernéticas na região. Cooperando, tais países conseguem somar esforços, compartilhar conhecimentos e experiências e diminuir os custos dos processos

envolvidos, aumentando suas possibilidades para a construção de capacidades e, consequentemente, ampliando seu poder no cenário cibernético internacional, algo que isoladamente torna-se mais complexo diante das dificuldades que possuem.

Importa mencionar que houve diálogos sobre segurança e defesa cibernética no âmbito dessas instituições de cooperação e integração na América do Sul, que buscaram possibilidades de coordenar posições e estabelecer políticas e mecanismos regionais para combater as ameaças cibernéticas. Ademais, há uma percepção de que não existem disputas de poder no domínio cibernético entre os países da região (JUSTRIBÓ, 2014; OLIVEIRA et al., 2017; GONZALES; PORTELA, 2018). Apesar disso, o andamento das conversações e as tentativas de coordenação entre os países sul-americanos foram enfraquecidas ou suspensas. Frente à conjuntura apresentada, pondera-se a necessidade de discutir sobre essa perspectiva cooperativa para a construção de capacidades cibernéticas e suas potencialidades, avaliar as convergências no setor e as complementariedades que tornariam a cooperação regional um caminho viável para a construção de cibercapacidades. Aos mesmo tempo, investigar fatores que estão relacionados às dificuldades e entraves para os avanços desses processos na América do Sul e que, nessa perspectiva, precisam serem avaliados e resolvidos.

Ainda, apesar da relevância da temática relativa à construção de capacidades cibernéticas, observam-se lacunas sobre esses estudos no Sul Global. Particularmente, quando se trata da América do Sul, são escassas as pesquisas e análises que proponham perspectivas que levem em considerações as demandas e problemáticas próprias desses países, que levem em consideração as dinâmicas regionais e, da mesma forma, que ressaltem cenários cooperativos em vista à construção dessas capacidades. A insuficiência de estudos aplicados sobre o tema pode resultar também em dificuldades para a criação de um quadro estratégico apropriado por esses Estados, no qual os interesses sejam delimitados, as áreas prioritárias sejam identificadas, as debilidades sejam reconhecidas, planos concretos sejam arquitetados, mecanismos e estruturas sejam criados, as vias sejam corretamente traçadas e os recursos sejam mais bem alocados.

Diante disso, a presente pesquisa tem como tema a construção de capacidades cibernéticas na América do Sul. Salienta-se que a temática da construção de capacidades cibernéticas na América do Sul será abordada a partir de uma perspectiva cooperativa e partirá do contexto cibernético interno/nacional e regional dos países. Desse modo, a pergunta de partida da pesquisa foi delimitada da seguinte forma: Quais as potencialidades para a construção de capacidades cibernéticas na América do Sul por meio de processos

cooperativos regionais se analisado o contexto geopolítico regional e, particularmente, se comparadas as políticas e estratégias cibernéticas da região?

A partir da problemática da pesquisa, um questionamento secundário ou auxiliar é proposto: Que obstáculos os países da América do Sul enfrentam – e que precisariam, portanto, serem superados - para o desenvolvimento de processos cooperativos para a construção de capacidades cibernéticas?

A investigação parte da hipótese de que (1) existem similaridades nos desafios que os países sul-americanos enfrentam e complementariedades no setor cibernético que tornam um processo de cooperação regional um meio viável para a redução das fragilidades individuais na construção de capacidade cibernética. Além disso, (2) observando o cenário regional, acredita-se que as dinâmicas cooperativas entre os países sul-americanos nas últimas décadas são demonstrativos do potencial regional para a construção de processos cooperativos também na área cibernética. Nesse sentido, defende-se também que o contexto geopolítico regional aproxima os países sul-americanos. Por outro lado, no entanto, (3) a polarização e as assimetrias regionais e, particularmente, as distinções nos fundamentos das políticas e estratégias cibernéticas dos Estados (que perpassam as percepções estratégicas dos países acerca do espaço cibernético e sua atuação na área) tornam-se entraves no desenvolvimento de processos cooperativos mais amplos entre os países.

A partir do exposto, a presente pesquisa irá investigar e comparar as políticas, estratégias e os estágios dessa construção particularmente em três países sul-americanos (Argentina, Brasil e Colômbia), visando compreender seus pontos de divergências e convergências e comparar seus níveis de capacitação a partir de dimensões e indicadores selecionados. De modo secundário, busca-se relacionar tais elementos com a análise do contexto geopolítico regional, levando em consideração as novas dinâmicas de poder estabelecidas pelo crescente protagonismo do espaço cibernético nas relações internacionais e a sua relevância nas políticas dos Estados no século XXI.

A América do Sul possui dinâmicas geopolíticas e geoeconômicas específicas que demandam que estratégias sobre a construção de capacidades cibernéticas leve em consideração suas particularidades e a conjuntura regional que os países estão inseridos. Nessa mesma perspectiva estão os processos de cooperação e integração na América do Sul, que exigem para sua compreensão a análise da geopolítica regional e dos processos internos dos países – já que os processos regionais sul-americanos sofrem diretamente com os

impactos das políticas domésticas dos Estados. Nessa perspectiva, identificou-se que um estudo direcionado às políticas e estratégias para a construção de capacidades cibernéticas desenvolvidas por países expoentes no setor configura-se como uma forma de observar o direcionamento que tem se dado para esta temática e como isso reflete na região em termos de desenvolvimento de processos cooperativos.

A partir disso, tem-se como intuito identificar as potencialidades para o desenvolvimento de um processo de cooperação na América do Sul no setor cibernético, com vistas à construção de capacidades pelos países da região, assim como os obstáculos ou entraves que devem ser enfrentados para um eficiente processo cooperativo se desenvolva. Isso porque defende-se que uma efetiva estratégia para construção de capacidades cibernéticas pelos países sul-americanos exige, além do fortalecimento e a articulação entre os setores nacionais ligados à segurança e defesa do ciberespaço (setor público, setor privado e academia), a cooperação com seus parceiros regionais. Esse processo traria, entre outros resultados, a melhoria dos níveis de capacitação cibernética dos países - e da região como um todo -, melhorando sua posição de poder frente ao cenário internacional. Ademais, entende-se a importância de que países sul-americanos estabeleçam uma ampla estratégia[1], com suas prioridades e meios claramente definidos para a construção de capacidades cibernéticas.

Para alcançar o objetivo principal desta pesquisa, cinco objetivos mais específicos serão perseguidos no decorrer dos três capítulos que dividem essa tese:

I) Definir os conceitos basilares para o desenvolvimento desta pesquisa, particularmente o de capacidade cibernética, estabelecendo as relações entre capacidade cibernética, poder cibernético e segurança e defesa cibernética, e os de diplomacia cibernética e cooperação cibernética;

II) Investigar as contribuições já realizadas sobre cooperação cibernética e diplomacia cibernética para refletir sobre processos de construção de capacidades cibernéticas na América do Sul.

III) Compreender o contexto geopolítico internacional e sul-americano frente ao crescente protagonismo do ciberespaço nas dinâmicas de poder, analisando as principais

[1] Na concepção contemporânea, Kalout e Degaut (2017, p. 10) explicam a formulação de uma grande estratégia (ou ampla estratégia) como o exercício de "definição e conjugação de meios e fins, de maneira que intenções estejam relacionadas a capacidades, e objetivos estejam relacionados a recursos disponíveis ou alcançáveis". Ou seja, "alinhar os recursos de poder do país com seus interesses e prioridades, orquestrando-se fins, meios e métodos".

ameaças e desafios que perpassam esse ambiente, a inserção dos países sul-americanos no ambiente digital e as oportunidades que os recursos cibernéticos promovem à América do Sul;

IV) Investigar as iniciativas de cooperação e integração regional e os diálogos abrangendo o setor cibernético na América do Sul, principalmente as desenvolvidas no âmbito da Unasul, instituição que pode ser considerada um marco para as relações regionais.

V) Comparar as políticas e estratégias para a construção de capacidades cibernética de Argentina, Brasil e Colômbia, identificando o estágio que se encontram nesse processo, analisando as semelhanças e diferenças, as convergências e divergências em sua atuação e percepções estratégicas para o setor.

Nesse sentido, ao estabelecer as delimitações teórico-conceituais, analisar o contexto geopolítico regional e comparar os países elencados - observando divergências, convergências, similaridades e complementariedades no processo de estabelecimento de políticas e estratégias e na construção de suas cibercapacidades dos três países -, busca-se, finalmente, determinar variáveis e criar um entendimento sobre caminhos possíveis, meios eficientes para a construção de capacidades cibernéticas na América do Sul por meio de processos cooperativos regionais.

Assim, diante dos objetivos e da delimitação proposta para esta tese, foram escolhidos, como objetos para aprofundamento da análise, três países: Argentina, Brasil e Colômbia. De modo geral, tais países foram escolhidos por serem compreendidos como expoentes em termos cibernéticos na região, ao estarem avançando em sua agenda cibernética, mas também pela sua relevância geopolítica no contexto sul-americano, possuindo, assim, maior capacidade de liderar uma agenda regional. Dessa forma, inclusive, seus processos internos podem vir a servir de exemplo para os demais atores estatais da região que buscam avançar no setor. Ademais, acredita-se que a análise desses três países possa servir de exemplo para que novas pesquisas sejam feitas com outros países sul-americanos nos mesmos termos, guardadas as devidas diferenciações que podem existir devido aos diferentes níveis de capacitação na região.

Mais especificamente, no que diz respeito à definição desses três países, tomou-se por base uma série de fatores, desde questões históricas, geopolíticas ou relacionadas aos próprios fatores cibernéticos. Essa definição embasa-se em estudos já realizados, relatórios e dados disponíveis sobre os países – discussão que será aprofundada no segundo e terceiro capítulo desta tese.

Sobre isso, alguns pontos podem ser destacados. Em termos regionais, Brasil e Argentina são, territorialmente, os maiores países da América do Sul e, ao longo da história da região, as relações entre os dois ditou também dinâmicas de cooperação e integração na região. Assim, a parceria estratégica entre Brasil e Argentina, que perpassa uma extensa agenda de cooperação bilateral, é considerada o núcleo duro da integração regional, ficando claro que o avanço de processos cooperativos multilaterais e a construção da América do Sul como um bloco de poder depende da participação dos dois países (GULLO, 2006; GRANATO, 2015; GRASSI, 2019; GRASSI; KERR OLIVEIRA, 2022).

Enquanto Argentina e Brasil são atores centrais no Cone Sul, a Colômbia também tem papel crucial nas dinâmicas geopolítica e securitárias da região andina e sofre com a dependência e as interferências norte-americanas, principalmente no âmbito da denominada política de combate ao narcotráfico, que impacta toda a região. Sobre isso, cabe destacar que a Colômbia se configura com um território muito privilegiado, além das reservas de recursos estratégicos e de ser um país amazônico rico em biodiversidade, conta com acesso ao Mar do Caribe e ao Oceano Pacífico e faz fronteira com dois país sobre os quais Estados Unidos também direcionam uma atenção especial na região, Equador e Venezuela (OLIVEIRA; CÁCERES, 2014). Nesse sentido, também é interessante observar a localização das instalações militares norte-americanas nessa região, as quais se encontram justamente em áreas ricas com recursos considerados estratégicos (OLIVEIRA; CÁCERES, 2014; RODRIGUES, 2015).

De modo geral, como poderá ser observado no capítulo 2, os três países são historicamente impactados com as pressões desestabilizadoras dos Estados Unidos. Ademais, os três países são ricos em recursos estratégicos (recursos minerais, energéticos, água, biodiversidade), com destaque para a Argentina com suas grandes reservas de lítio; e Brasil e Colômbia, como países amazônicos, ricos em biodiversidade e no centro das pressões internacionais sobre a proteção e a internacionalização da Amazônia (AMORIM, 2013; OLIVEIRA; CÁCERES, 2014; AMIN, 2015; RODRIGUES, 2015; AGUIRRE; CHAVEZ; ROBLEDO, 2020; PEIXOTO JÚNIOR, 2020). Diante da corrida geopolítica cada vez mais acirrada pelo controle dos recursos estratégicos para a perpetuação das dinâmicas de poder no cenário internacional, tem-se a perspectiva que esses países vão sofrer cada vez com as dinâmicas da competição entre as grandes potências.

Por outra perspectiva, Argentina, Brasil e Colômbia são os três maiores países em população e usuários de internet, consolidando, juntos, 71% da população e dos usuários de

internet da América do Sul (INTERNET WORLD STATS, 2022). Além disso, estão entre os Estados da região que mais sofrem ataques cibernéticos e entre os países que mais utilizam os sistemas SCADA (Sistemas de Supervisão e Aquisição de Dados, do inglês *Supervisory Control and Data Acquisition*), sistema utilizado em processos industriais e nas infraestruturas críticas nacionais - sendo que a Argentina é o país com maior número desses sistemas (OLIVEIRA et al., 2017). Também, acabam estando entre os países que mais sofrem com crimes cibernéticos, principalmente se observados os dados relacionados aos incidentes de cibersegurança. Somados, Argentina, Brasil e Colômbia correspondem a mais de 40% das infecções de malware e dos ataques de *phishing* na América Latina (ESET, 2021). Isso os torna particularmente vulneráveis no ambiente cibernético e evidencia a necessidade de estratégias coesas e eficientes para a construção de capacidades - já que quanto mais conectado mais vulnerável um país está.

Por outro lado, olhando para os índices internacionais que medem a capacitação cibernética dos países, observa-se que os três países estão entre os que possuem melhores pontuações em pelo menos um dos rankings analisados. No Global Cybersecurity Index, o Brasil ficou como primeiro colocado na América do Sul. No National Cybersecurity Index, a Argentina se configurou na segunda colocação (atrás do Paraguai). No relatório da OEA que se baseia no Modelo de Maturidade de Cibersegurança, a Colômbia ficou na segunda posição, seguida de Brasil na terceira colocação (ambos atrás de Uruguai). Além disso, observando as dimensões apresentadas no relatório da OEA, a Colômbia foi destaque em "Política e Estratégia de Cibersegurança" e o Brasil foi o que melhor se posicionou na dimensão "Marcos Legais e Regulatórios". Ainda, a Argentina foi o primeiro país da América do Sul a promulgar um marco regulatório para a proteção de dados, em 2000.

Ademais, é importante ressaltar que Brasil, Argentina e Colômbia foram países que incentivaram o início das discussões sobre defesa cibernética na Unasul, por serem precursores ao pensar essas dinâmicas internamente em seus países.

O fato da América do Sul não ser um bloco homogêneo e sim uma região consideravelmente assimétrica não é desconsiderado nesta pesquisa. Entretanto, a América do Sul, como uma região geopolítica distinta da América Latina (COSTA, 2009), possui perspectivas e enfrenta desafios políticos, econômicos, sociais e securitários que aproximam os países para além do aspecto meramente geográfico. Ademais, o período de auge dos processos de cooperação e integração regional demonstrou o potencial da região em avançar

na proposição de medidas conjuntas em diversas áreas, inclusive em defesa, e solucionar controvérsias regionalmente (SAINT-PIERRE; PALACIOS Jr., 2014; FUCCILLE 2015; PAGLIARI, 2015; SOUZA, 2015; GONÇALVES; BRAGATTI, 2018; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021).

Ressalta-se também que, apesar da construção de capacidades e das dinâmicas de poder no ciberespaço perpassarem também atores não estatais, nesta pesquisa o foco analítico serão os atores estatais e suas interações, uma vez que se entende que o Estado segue sendo o ator central e que este possui um papel de coordenação nas dinâmicas de governança cibernética. Isso, no entanto, não significa que os demais atores e setores serão desconsiderados na investigação.

Em relação aos procedimentos metodológicos, a pesquisa adotará o método de abordagem hipotético-dedutivo e o método de procedimento principal será o comparativo. Adicionalmente, serão utilizados os aportes da geopolítica para compreender esse novo espaço de atuação, as dinâmicas de poder envolvidas, as percepções de ameaças e a região diante desse novo contexto. Sobre o campo de análise, este pode ser definido a partir de três fatores: espaço geográfico, campo de análise ou unidade de observação e período de análise (QUIVY; CAMPENHOUDT, 1998). Nessa perspectiva, delimita-se:

a) Espaço geográfico: América do Sul;

b) Unidade de observação: países que representam componentes típicos ou unidades características dentro do espaço geográfico proposto para aprofundar a temática - Argentina, Brasil e Colômbia;

c) Período: essencialmente o período compreendido entre 2008-2022. Em 2008, a Unasul foi criada, instituição que congregou em sua dinâmica iniciativas para cooperação no setor cibernético, principalmente a partir do CDS. Além disso, nesse ano, o Brasil introduziu em seus documentos de defesa o setor cibernético como estratégico, configurando-se como o primeiro da região.

Para construir essa pesquisa, pretende-se voltar a atenção para os documentos de políticas e estratégias desenvolvidos pelos Estados nas áreas de cibersegurança e ciberdefesa e para dados disponíveis na literatura especializada, em índices internacionais sobre capacidades cibernéticas, em relatórios internacionais, como o Relatório de Cibersegurança da Organização dos Estados Americanos (OEA) e outros recursos disponíveis. A revisão de literatura especializada da área buscará, primordialmente, compreender: i) as definições propostas e os avanços que a academia tem obtido em relação aos objetos fixados nesta

pesquisa; e ii) as dinâmicas geopolíticas sul-americanas, principalmente em relação às percepções securitárias e ameaças cibernéticas, obstáculos existentes e os avanços no que diz respeito à construção de capacidades e em termos de processos de cooperação.

Além disso, serão analisados índices que têm buscado medir a maturidade das capacidades dos países ou seus níveis de cibersegurança, são estes: I) o *Global Cybersecurity Index* (GCI), da União Internacional de Telecomunicações (UIT) da Organizações das Nações Unidas (ONU); II) o *National Cyber Security Index* (NCSI), do *think tank* e-Governance Academy, da Estônia; e III) o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (CCMM, do inglês *Cybersecurity Capacity Maturity Model*), desenvolvido pelo *Global Cyber Security Capacity Centre* (GCSCC) da Universidade de Oxford, do Reino Unido. Este último foi o modelo base para relatório sobre cibersegurança na América Latina e o Caribe, realizado pelo *Observatorio de Ciberseguridad* da OEA e, portanto, destaca-se na presente pesquisa por permitir uma análise mais detalhada a partir da região. Esses índices foram escolhidos por possibilitarem fazer comparações entre os países elegidos nesta pesquisa. Para além desses, outros relatórios, bancos de dados e centros de pesquisa serão utilizados para construir o entendimento sobre o contexto sul-americano e, particularmente, o cenário no qual estão inseridos os três países analisados, como o *Internet World Stats* e a *Red Iberoamericana de Indicadores de Ciencia y Tecnología* (RICYT).

Por fim, esta tese está dividida em três capítulos, além desta introdução e das considerações finais. O primeiro terá por intuito delinear os principais conceitos e discussões teóricas que envolvem a cibernética nas relações internacionais, os quais servirão de base para a pesquisa. Apresentará análises geopolíticas que permeiam o ciberespaço, trazendo perspectivas sobre ameaças, dinâmicas ofensivas e defensivas e como os países do Sul Global se inserem nessa discussão. Neste capítulo também serão apresentados os três índices mencionados, visando compreender suas estruturas e metodologias para, posteriormente, poder analisar os dados levantados por esses institutos de pesquisa. Além disso, será feito um levantamento das contribuições acadêmicas já realizadas sobre construção de capacidades cibernéticas, de modo a construir um entendimento sobre sua conceitualização e sua importância no cenário doméstico dos Estados e na política internacional. Essas questões devem serem definidas neste primeiro momento de modo a delinear os aspectos teóricos-conceituais que sustentam o processo de investigação a ser desenvolvido.

O segundo capítulo iniciará discutindo cooperação cibernética e diplomacia cibernética, visando apontar as potencialidades desse campo de estudo e o direcionamento que tem se dado à questão. Após, direcionará a atenção para o contexto geopolítico sul-americano, buscando compreender como a região se insere nas novas dinâmicas securitárias determinadas pelo ciberespaço, analisar as principais ameaças que enfrentam em termos cibernéticos e as principais fragilidades regionais diante desse cenário. O capítulo procurará traçar um panorama regional, buscando dados da região e analisando a importância dos recursos cibernéticos para os países. Além disso, buscará resgatar os processos cooperativos regionais que foram desenvolvidos a partir da Unasul e do seu Conselho de Defesa, bem como do Mercosul – bloco composto pelos dois maiores países da América do Sul, Argentina e Brasil, e no qual Colômbia é membro associado –, e os avanços e entraves que puderam ser observados em relação à cooperação na região, principalmente em relação ao setor cibernético.

Por fim, o último capítulo buscará traçar o panorama regional especificamente em relação à construção de capacidades cibernéticas e debruçar-se-á nas dinâmicas dos países elegidos e em suas políticas e estratégias cibernéticas, buscando comparar alguns indicadores e compreender os principais avanços que estes países têm obtido e os desafios ainda a superar. Esse estágio da investigação será essencial para constatar elementos de convergência e divergência entre os países, de modo a analisar, posteriormente, possibilidades para atuações coordenadas entre os Estados. Tais países, como já explicitado anteriormente, são considerados expoentes cibernéticos na região e possuem potencial para liderarem agendas em processos cooperativos regionais no setor.

Para a investigação sobre os três países, alguns elementos são elencados para uma análise mais aprofundada, são estes:

I) As principais temáticas abordadas em suas legislações - de modo a entender as áreas e assuntos que estão sendo priorizados pelos países.

II) Com explicitam os principais conceitos da área – tendo em vista que os conceitos que contornam o ciberespaço não possuem definições universalmente aceitas e suas definições por parte dos Estados tem muito a dizer sobre seu entendimento e perspectivas de atuação nesse ambiente.

III) A estrutura institucional, observando os órgãos responsáveis e a criação de organismos específicos para o setor, bem como a delimitação da responsabilização civil e militar.

IV) Como entendem o ciberespaço, os recursos e as ameaças cibernéticas em suas estratégias de segurança e defesa – por exemplo, se enfatizam a dimensão dos conflitos nesse espaço, se identificam tais recursos como novas oportunidades para o desenvolvimento, aumento de poder e de ascensão internacional e, principalmente, se ou como sinalizam para possibilidades de cooperação no setor, particularmente com o entorno geográfico da América do Sul, e que significância essas estratégias cooperativas têm para os países.

V) As dimensões da construção de capacidades em que se destacam e as que possuem maiores debilidades, identificando similaridades e complementariedades entre os países.

VI) O papel atribuído à pesquisa e à ciência nacional, à educação cibernética e a formação de recursos humanos qualificados, bem como os avanços nessa direção – levando em consideração que este é fator considerado crucial na construção de capacidades cibernéticas.

Seguindo essa estruturação e discutindo os tópicos elencados, espera-se ser capaz de responder os questionamentos e testar as hipóteses das quais essa investigação parte. Finalmente, espera-se, que a presente pesquisa possa servir de base para trabalhos futuros na área, visto a baixa produção acadêmica nacional (e regional) no que diz respeito à diplomacia cibernética e à construção de capacidades cibernéticas, da mesma forma que ainda carecem as discussões sobre as possibilidades de cooperação cibernética na América do Sul, aplicando análises geopolíticas que observem a realidade regional e as problemáticas cibernéticas próprias desse grupo de países.

2 GEOPOLÍTICA NO CIBERESPAÇO E PERSPECTIVAS TEÓRICO-CONCEITUAIS: AMEAÇAS, CAPACIDADE E PODER CIBERNÉTICO

Ao longo das duas primeiras décadas do século XXI, tem se discutido que as características e possibilidades de atuação advindas com o desenvolvimento do ciberespaço - particularmente, a transcendência de fronteiras físicas e a redução das noções de tempo e espaço, a possibilidade de atuar anonimamente e a digitalização das relações sociais e políticas -, tornariam irrelevante o cenário geográfico e a geopolítica clássica (SHELDON, 2014). Nesse mesmo sentido, inclusive, tomaram forma algumas discussões que questionavam a relevância de ideais ligados ao regionalismo e à regionalidade[2] na atuação dos atores diante da ascensão do ciberespaço, pois este estaria abolindo as noções clássicas de espaço, território e fronteira. Com isso, também se problematizou a relevância da geografia e da geopolítica diante do ciberespaço (DOUZET, 2014; SHELDON, 2014).

Diante disso, articulou-se sobre o papel do poder cibernético na discussão geopolítica tradicional, demostrando que "tanto a geografia quanto a geopolítica exercem enorme influência sobre o ciberespaço e que, por sua vez, o poder cibernético – o efeito estratégico gerado a partir do ciberespaço – tem significado geográfico e geopolítico."[3] (SHELDON, 2014, p. 292, tradução própria). Essa discussão ultrapassa a lógica das implicações geográficas e geopolíticas das infraestruturas físicas que tornam possível a existência do ciberespaço e adentra disputas tecnológicas e pelo controle dessas ferramentas e da informação gerada através delas, bem como o enquadramento geográfico e o significado geopolítico dos principais alvos de ataques cibernéticos (SHELDON, 2014). Nessa direção, é ampla a discussão sobre o papel dos recursos cibernéticos, de modo geral, e da informação, particularmente, na política internacional, na revolução dos assuntos militares e nos novos formatos dos conflitos.

---

[2] A regionalidade é definida como "a propriedade ou qualidade do 'ser' regional", assim, "envolveria a criação concomitante da 'realidade' e das representações regionais, sem que elas possam ser dissociadas ou que uma se coloque, a priori, sob o comando da outra [...]" (HAESBAERT, 2010, p. 8). Por sua vez, regionalismo, para Mariano e Ribeiro (2016), está ligado à ideia de pertencimento a um espaço geográfico e envolve uma articulação a partir desse referencial territorial, envolvendo formas de cooperação entre atores estatais e não estatais.

[3] "[...] *both geography and geopolitics exert tremendous influence on cyberspace and that, in turn, cyber power—the strategic effect generated from cyberspace—has geographical and geopolitical meaning*." (SHELDON, 2014, p. 292)

Ainda, a geopolítica é essencial para uma análise substancial sobre as perspectivas cooperativas diante do cenário cibernético. As lentes geopolíticas auxiliam na compreensão, por exemplo, do cenário desigual no processo de construção de capacidades nos países do Sul Geopolítico[4], na manutenção da dependência desses países em relação ao Norte Global e nas dificuldades que esses países enfrentam nas discussões em relação à governança cibernética internacional. Nesse sentido, é uma base crucial para debater o contexto internacional e regional atual na perspectiva aqui proposta.

Partindo disso, este capítulo tem por intuito discutir a geopolítica cibernética, introduzindo tópicos que permeiam esse tema e que são importantes para a compreensão do objeto desta pesquisa. A geopolítica auxilia a compreender o que há por traz dos conflitos no ciberespaço - ou que ocorrem por meio do ciberespaço -, mas também serve para analisar as possibilidades de cooperação e governança coletiva. Portanto, a discussão geopolítica transpassa todos os capítulos dessa tese.

Neste capítulo, serão delineados também os principais conceitos que se relacionam à cibernética nas relações internacionais, particularmente os conceitos considerados centrais para essa pesquisa, entre eles poder cibernético e capacidade cibernética. Ressalta-se que, no que se refere à dimensão cibernética, existe uma ampla e complexa lista de definições, sem existir consenso ou conceitos universalmente aceitos. Essa situação, como será observado adiante, pode dificultar o entendimento e a cooperação entre os Estados nesta área e, por outro lado, torna possível a manipulação desses termos pelos Estados para atender seus interesses particulares. Ressalta-se que, ao final desta tese, como anexo, elaborou-se um quadro conceitual para que o leitor possa recorrer ao longo da leitura, visando facilitar a compreensão das discussões propostas ao longo dessa pesquisa.

[4] 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 e delimita os países do Sul Global como "os outros", a oposição ao Norte Global. Além disso, propaga uma visão enviesada do que é o Norte e o que é o Sul do globo. Por sua vez, "o Sul Geopolítico tem sua definição baseada em atores que constroem suas posturas política e identitária no plano sistêmico, politizando suas posições (desfavoráveis) na hierarquia internacional, a partir de uma leitura histórica das assimetrias, que se perpetuam e se cristalizam em estruturas de poder." O uso do termo 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 adjetivo 'geopolítico' tem valor informativo, uma vez que traz sentido e qualifica o substantivo 'sul'. [...] 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" (COSTA; DUARTE, 2023).

Ainda, serão analisadas as dimensões e indicadores de três índices internacionais que propõem classificar os países diante de suas capacidades cibernéticas. Esses índices contribuem também para o entendimento sobre o que abrange capacidade cibernética, fornecem dados para a compreensão do nível de maturidade cibernética dos Estados e auxiliam na identificação dos fatores que devem ser perseguidos para a construção de suas capacidades nesse âmbito. Ademais, eles serão utilizados mais à frente na contextualização da região e dos países investigados nesta pesquisa.

2.1 A DIMENSÃO CIBERNÉTICA: GEOPOLÍTICA, PODER E CONTROLE DOS RECURSOS CIBERNÉTICOS

A geopolítica está relacionada ao exercício de poder ou as relações de poder em relação a determinado espaço ou território. Assim, desde sua criação, esse campo de estudos discute a necessidade de o Estado obter espaço para garantir sua sobrevivência no cenário internacional. No entanto, essa busca por espaço não pode ser entendida como um fim em si mesma, já que tem como motivação essencial a obtenção de recursos estratégicos que garantam o aumento e a perpetuação do poder dos Estados (PORTELA, 2018). Assim, ao longo da história, o imperialismo e as disputas entre as nações foram marcados pela conquista de povos e territórios a fim de garantir recursos de poder de modo a transformá-los em poder concreto.

Nas relações internacionais, poder é definido pelos recursos que, por meio de estratégias bem delimitadas e de capacidade de liderança, possibilitam os resultados pretendidos (NYE, 2011). Poder, nesse sentido, não pode ser simplesmente definido pelos recursos do ator, uma vez que são necessárias estratégias e mecanismos para transformá-los em poder concreto. Ainda, os recursos de poder são "as matérias-primas tangíveis e intangíveis ou veículos que fundamentam as relações de poder, e se um determinado conjunto de recursos produz resultados preferidos ou não depende do comportamento no contexto."[5] (NYE, 2011, p. 9, tradução própria).

Em uma segunda definição, poder se relaciona à capacidade de impactar comportamentos visando alcançar os resultados pretendidos pelo ator, seja por meio da

[5] "[…] *the tangible and intangible raw materials or vehicles that underlie power relationships, and whether a given set of resources produces preferred outcomes or not depends upon behavior in context*." (NYE, 2011, p. 9)

coerção ou da cooptação, controlando a agenda internacional, influenciando a opinião pública, moldando crenças e preferências (NYE, 2011). Sendo assim, poder pode ser compreendido por recursos e por resultados comportamentais. No entanto, não é fácil definir nem mensurar poder nas relações internacionais, já que este é um conceito contestado, existindo diferentes perspectivas. O poder estatal, entretanto, não pode mais ser mensurado apenas levando em conta seus recursos tradicionais (relacionadas, principalmente, aos recursos militares, ou sua capacidade de fazer a guerra, e aos recursos financeiros e econômicos).

Diante disso, Nye (2011) expõe duas formas de projeção de poder: o poder duro (*hard power*), baseado em recursos tradicionais e que possibilitam, essencialmente, a coerção ou dissuasão; e o poder brando (*soft power*), que diz respeito aos recursos que produzem a cooperação, garantindo que os demais atores se adequem aos seus interesses e expectativas e compartilhem seus valores e ideologias. Partindo disso, o autor propõe uma terceira forma de projeção de poder, o poder inteligente (*smart power*). O poder inteligente, conforme Nye (2011, p. 209, tradução própria), diz respeito "a encontrar maneiras de combinar recursos em estratégias bem-sucedidas no novo contexto de difusão de poder e na 'ascensão do resto'". Ou, "a inteligente integração e ligação em rede de diplomacia, defesa, desenvolvimento e outras ferramentas dos chamados poderes 'duro e brando'."[6]

Dessa forma, fica claro que o poder opera em diversas dimensões e escalas e é relacional, pois existe em um espaço e em relação a algo ou alguém, e é variável no tempo (GONZALES; PORTELA, 2018). Assim, o exercício do poder passa a envolver diversos fatores, capacidades e recursos, e a revolução dos meios de comunicação e informação trazem uma nova dimensão do poder, além de trazer novos desafios.

Tendo em vista essas considerações iniciais, as seções e subseções seguintes apresentarão aspectos teóricos e conceituais sobre o ciberespaço e o poder procedente desse domínio, bem como abordarão discussões geopolíticas fundamentais para iniciar as análises propostas nessa pesquisa.

2.1.1 Ciberespaço, poder e geopolítica cibernética em discussão

[6] "[…] *to combine resources into successful strategies in the new context of power diffusion and the 'rise of the rest'. [...] the intelligent integration and networking of diplomacy, defense, development, and other tools of so-called 'hard and soft' power*." (NYE, 2011, p. 209)

Dentro do contexto de mudanças na configuração do poder no sistema internacional com o fim da Guerra Fria, o ciberespaço passou a ter destaque e, portanto, posicionou-se como elemento central nas discussões geopolíticas. O espaço cibernético[7] pode ser definido como "os satélites, os drones, os sistemas de identificação por rádio frequência, os computadores - conectados ou não -, e os sistemas industriais informatizados" (VENTRE, 2012, p. 34). Ou, pelas palavras de Kuehl (2009, p. 28), o ciberespaço:

> [...] é um domínio global dentro do ambiente de informação, cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação.[8]

Cabe mencionar, no entanto, que não há definições objetivas e universalmente aceitas para os termos que dizem respeito a essa nova esfera de atuação. Ainda assim, alguns autores se esforçam para determinar elementos concretos para sua definição. Choucri (2012, p. 8, tradução própria), por exemplo, entende que o ciberespaço como hierarquicamente composto por camadas, as quais são classificadas por:

> [...] (1) as bases físicas e infraestruturas que permitem o campo de jogo cibernético, (2) os blocos de construção lógicos que suportam a plataforma física e permitem serviços, (3) o conteúdo da informação armazenado, transmitido ou transformado, e (4) os atores, entidades e usuários com diversos interesses que participam dessa arena em vários papéis.[9]

Por outro lado, Ventre (2011) entende que esse espaço é composto por três camadas:

---

[7] Importa destacar que enquanto o ciberespaço é "um domínio operacional eletrônico / eletromagnético", a internet é a "rede central do domínio operacional baseada em computadores" (LOBATO; KENKEL, 2015, p. 25). O ciberespaço é mais abrangente, a Internet "representa parcelas do espaço cibernético que estão interconectadas" (PORTELA, 2018, p. 142). A existência da internet só passa a ser possível com a criação do ciberespaço. Ou seja, os termos não podem ser admitidos como sinônimos.

[8] "[…] *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).

[9] "[…] *we view cyberspace as a hierarchical contingent system composed of (1) the physical foundations and infrastructures that enable the cyber playing field, (2) the logical building blocks that support the physical platform and enable services, (3) the information content stored, transmitted, or transformed, and (4) the actors, entities and users with various interest who participate in this arena in various roles*." (CHOUCRI, 2012, p. 8)

I) uma estrutural, de caráter físico ou material, formada pelas infraestruturas (cabos, redes, satélites, computadores e demais hardwares) – a qual Douzet (2014) identifica como a espinha dorsal da Internet;

II) a segunda, imaterial, representada pelos softwares, aplicações e similares; e

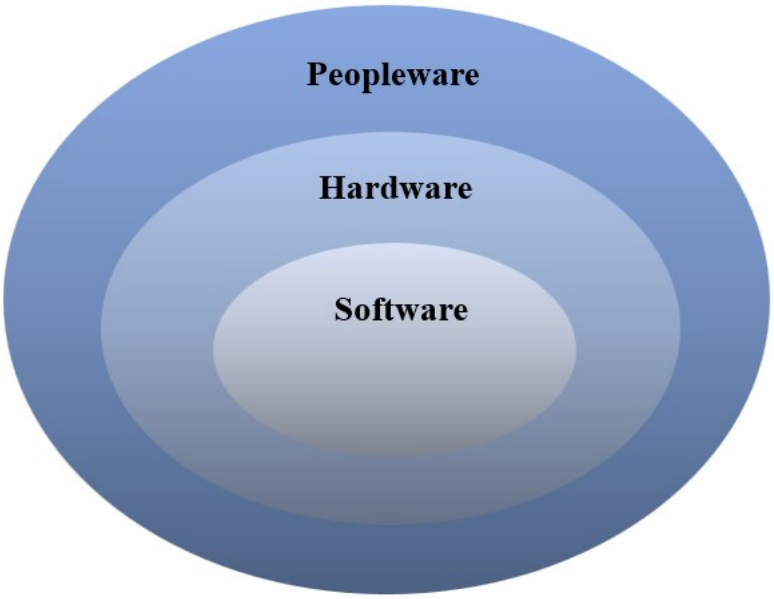
III) a camada superior de caráter cognitivo, que consiste na interação social e no processo mental das pessoas que possibilita a existência desse espaço.

A visão proposta pelo autor coincide com a concepção de especialistas das áreas de sistemas de informação e informática que entendem o ciberespaço a partir de três camadas: o *hardware*, que seriam os componentes do sistema; o *software*, que diz respeito aos sistemas e à programação; e o *peopleware*, que se refere às pessoas que atuam nesse ambiente (FERREIRA NETO, 2014).

A camada cognitiva, ou a *peopleware*, pode ser compreendida como sendo a mais importante ou a base de sustentação do ciberespaço. Isso porque, diferente dos demais espaços geográficos – terrestre, marítimo, aéreo e extra-atmosférico - que existem independente 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. Conforme Portela (2018, p. 148-149), “caso não haja relações sociais na camada *peopleware*, ou seja, a atuação dos operadores e usuários, esse espaço geográfico deixa de existir, já que sua existência não pode ter fim em si mesma”.

Nesse sentido, a figura 1 ilustra, de forma sintética, as camadas do ciberespaço.

Figura 1 - Camadas do ciberespaço

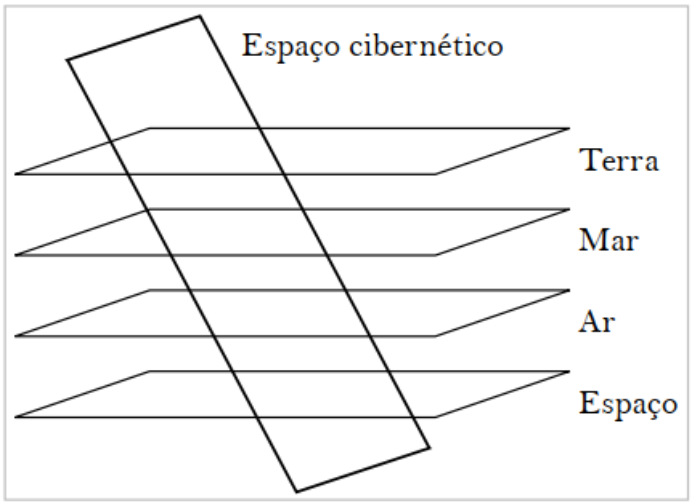


Fonte: elaborado pela autora

Entre as principais características que definem o ciberespaço e demonstram sua relevância na contemporaneidade está o baixo custo da atuação nesse espaço, principalmente se comparado aos recursos tradicionais de poder; a possibilidade do anonimato, o que dificulta antecipar, impedir e mesmo identificar ataques (problema da atribuição); o fato de permitir o aumento do fluxo de informações e a velocidade das ações; e a dificuldade de prever a dimensão e as consequências de ataques efetuados através do ciberespaço (NYE, 2011; DOUZET, 2014; FERREIRA NETO, 2014; FERREIRA, 2017; MEDEIROS; GOLDONI, 2020). Destaca-se também a transcendência de fronteiras físicas. Em outras palavras, a ideia de fronteiras no ciberespaço não se encaixa nas noções tradicionais. A discussão sobre fronteiras cibernéticas não resulta em consensos, sendo que a ideia de ciberfronteiras é ambígua e flexível e, em certa medida, artificial e abstrata (FERREIRA NETO, 2014; PORTELA, 2016; FERREIRA, 2017; MEDEIROS; GOLDONI, 2020).

Outra característica basilar do espaço cibernético é sua transversalidade. Essa particularidade diz respeito a interconexão e o poder de impactar também os demais espaços geográficos, sendo considerado, por isso, uma ferramenta crucial de projeção de poder e de controle para o Estado (FERREIRA NETO, 2014; PORTELA, 2018). A figura 2 ilustra essa marcante característica do ciberespaço.

Figura 2 - Relação entre o espaço cibernético e os demais espaços geográficos



Fonte: Ventre (2012, p. 35)

Desse modo, Ferreira Neto (2014, p. 8) aponta que a cibernética é um "instrumento que vem servindo também para uma (re)territorialização dos espaços tradicionais". Ademais, apresenta uma relação de causalidade: quanto maior a territorialização[10] do ciberespaço, maior é a capacidade de (re)territorializar, isto é, controlar as demais dimensões espaciais (FERREIRA NETO, 2014). Nessa perspectiva, Herrera (2007, p. 68, tradução própria) argumenta que com o advento do ciberespaço, pode-se observar um duplo e simultâneo movimento na política internacional: "a territorialização do ciberespaço e a desterritorialização da segurança do Estado."[11]

Portanto, o ciberespaço é apontado como um espaço em si, ou um fim; um domínio espacial autônomo – local onde o poder é exercido e confrontado. Ao mesmo tempo, a cibernética é compreendida como um recurso de poder, ou um meio (FERREIRA NETO, 2014).

[10] Territorialização é definida como a "tentativa de um indivíduo ou um grupo de atingir, influenciar ou controlar pessoas, fenômenos e relacionamentos, através de delimitação e afirmação do controle sobre uma área geográfica" (SACK, 1986 apud FERREIRA NETO, 2014, p. 8). Ou ainda: "o processo em que o homem age dentro de um território – no caso do Estado, a aplicação da soberania." (PORTELA, 2018, p. 147). A territorialização do ciberespaço é observada a partir da constante "disputa pelo controle de informações e da possibilidade de seu fluxo vem sendo objeto de poder" (FERREIRA NETO, 2014, p. 14). Nessa perspectiva, cabe mencionar, adicionalmente, que dada a criação e estruturação do ciberespaço, este deve ser compreendido como um espaço e, ao mesmo, tempo um território (PORTELA, 2018).

[11] "*I argue that we can observe in international politics today a simultaneous double move: the territorialisation of cyberspace and the deterritorialisation of state security*." (HERRERA, 2007, p. 68)

Entra em cena, portanto, o poder cibernético (*cyber power*) - o qual será retomado nas seções e subseções seguintes. Esta nova dimensão do poder pode ser definida a partir de "um conjunto de recursos relacionados a criação, controle e comunicação da informação eletrônica e computacional – infraestrutura, redes, software e habilidades humanas."[12] (NYE, 2011, p. 123, tradução própria). Ou, em termos comportamentais, ciberpoder:

> [...] é a capacidade de obter resultados preferidos por meio do uso dos recursos de informação eletronicamente interconectados do domínio cibernético. O poder cibernético pode ser usado para produzir resultados preferidos dentro do ciberespaço ou pode usar instrumentos cibernéticos para produzir resultados preferidos em outros domínios fora do ciberespaço.[13] (NYE, 2011, p. 123, tradução própria).

Kuehl (2009, p. 38-39, tradução própria) traz sua definição na mesma direção proposta por Nye (2011). Assim, adiciona:

> Este instrumento de poder é moldado por múltiplos fatores. Enquanto o ciberespaço como um ambiente simplesmente "é", o ciberpoder é sempre uma medida da capacidade de usar esse ambiente. A tecnologia é um fator óbvio, porque a capacidade de "entrar" no ciberespaço é o que possibilita seu uso. [...] Os fatores organizacionais também desempenham um papel importante, porque as organizações que criamos refletem propósitos e objetivos humanos, e suas perspectivas sobre a criação e uso do poder cibernético serão moldadas por sua missão organizacional, seja ela militar, econômica ou política. Todos esses diferentes fatores moldam como empregamos o poder cibernético para impactar e influenciar os elementos do poder. O elemento que está mais intimamente ligado ao poder cibernético é a informação.[14]

A informação é uma arma estratégica para a segurança das nações, assim como um poderoso instrumento a ser utilizado entre grupos rivais em quaisquer esferas (política, ideológica, religiosa, econômica), em nível local, regional ou global (DOUZET, 2014). Importante demarcar também, com bem pondera Nye (2010), que o poder baseado nos

---

[12] "[…] *a set of resources that relate to the creation, control, and communication of electronic and computer-base information – infrastructure, networks, software, human skills*." (NYE, 2011, p. 123)

[13] "*Defined behaviorally, cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace*." (NYE, 2011, p. 123)

[14] *This instrument of power is shaped by multiple factors. While cyberspace as an environment simply "is," cyberpower is always a measure of the ability to use that environment. Technology is one obvious factor, because the ability to "enter" cyberspace is what makes it possible to use it. [...] Organizational factors also play an important role, because the organizations we create reflect human purposes and objectives, and their perspectives on the creation and use of cyberpower will be shaped by their organizational mission, be it military, economic, or political. All of these different factors shape how we employ cyberpower to impact and influence the elements of power. The element that is most closely tied to cyberpower is information* (KUEHL, 2009, p. 38-39).

recursos informacionais não é algo novo nas relações internacionais, já o poder cibernético é e este tornou-se instrumento central para a construção de poder estatal no século XXI.

Diante disso, é indiscutível que "o domínio de informações e dados que trafegam no espaço cibernético pode gerar poder, especialmente Poder Inteligente" (PORTELA, 2018, p. 147). Ainda assim, como os Estados devem lidar com esse novo domínio ainda é bastante discutível e as diversas incertezas e preocupações geradas a partir dessa atuação são justificativas para o aprofundamento de uma geopolítica do espaço cibernético que "norteie a ação dos atores estatais." (PORTELA, 2018, p. 147).

Ao evidenciar os elementos que definem e caracterizam o ciberespaço, percebe-se claramente elementos geográficos e geopolíticos. Como pontua Herrera (2007, p. 74, tradução própria), as tecnologias "são criações humanas e, como tal, sujeitas a moldagem consciente e inconsciente por atores e instituições sociais". Ou seja, "a tecnologia é política".[15] Isso fica nítido, por exemplo, quando observamos as disputas ou contestações políticas em relação a novos sistemas tecnológicos; atores políticos podem discordar "sobre a direção que o desenvolvimento de uma determinada tecnologia deve tomar, ou se uma ou outra das tecnologias concorrentes deve ser escolhida para um determinado propósito."[16] (HERRERA, 2007, p, 74, tradução própria).

Portanto, as características do ambiente digital são consequências de escolhas políticas, não ocorrem simplesmente apesar delas, e nem são somente causas para determinados comportamentos políticos ou geopolíticos. Isso é mais uma evidência de que essas características podem ser moldadas e remodeladas no futuro (HERRERA, 2007). Como fica claro também, as relações internacionais no ciberespaço não estão isoladas ou desvinculadas das demais esferas da política internacional, mas esse novo espaço estabelece novas dinâmicas de interação e de poder entre os atores internacionais (BARRINHA; RENARD, 2020).

Por outro lado, a tecnologia é "conhecimento prático embutido em artefatos materiais, em instituições construídas para gerenciar os artefatos e em sua interface com

[15] "*They are human creations, and as such subject to conscious and unconscious shaping by social actors and institutions. [...] technology is political*" (HERRERA, 2007, p. 74)
[16] "*Political actors disagree about the direction the development of a certain technology should take, or whether one or another of competing technologies should be chosen for a given purpose*." HERRERA, 2007, p. 74)

outras instituições sociais."[17] (HERRERA, 2007, p, 74, tradução própria). Ainda, a geografia física é um componente do ciberespaço:

> [...] onde a tecnologia está localizada é tão importante quanto o que ela é. Embora nossas atividades na Internet possam parecer uma espécie de aventura efêmera e privada, elas estão, na verdade, inseridas em uma infraestrutura complexa (material, logística e regulatória) que, em muitos casos, atravessa várias fronteiras.[18] (BRUNN, 2015, p. 10, tradução própria).

De modo simplificado, o ciberespaço não é algo completamente intangível ou abstrato, foi criado e é manipulado pelo ser humano, é formado por infraestruturas concretas, dispostas geograficamente, com propósitos geopolíticos e consequências políticas, geopolíticas, econômicas, sociais e securitárias. As ações provenientes do ciberespaço, como é notório, têm sérios impactos e consequências no 'mundo físico'. Ao mesmo tempo, ressalta-se que, da mesma forma que nas relações internacionais, de modo geral, há um contexto geopolítico que ajuda a explicar as atuações e interesses dos atores - e as consequências geopolíticas podem ser analisadas diante desse contexto -, as relações internacionais no ciberespaço também possuem tais contextos e implicações, embora estas acabem, por vezes, sendo mitigadas (SHELDON, 2014).

Diante da relevância desse novo espaço de atuação, como pode ser observado, a maior preocupação dos Estados está no domínio de maiores recursos ou acesso a recursos. Em outras palavras, "na atual conjuntura, poder não é estritamente espaço", poder, no século XXI, está vinculado ao controle (PORTELA, 2018, p. 150). Logo, "estudar a geopolítica do espaço cibernético é debruçar-se sobre o controle dos Estados [e demais atores relevantes] nesse novo espaço geográfico." (PORTELA, 2018, p. 153).

Ademais, os recursos e poder advindo do ciberespaço seguem sendo utilizados como ferramenta para controlar e conquistar outros recursos estratégicos para os Estados. Isso porque o espaço cibernético provê um preciso nível de detalhamento "sobre uma região, a dinâmica de um local ou a situação de um país" de forma semelhante ou superior à de um

---

[17] "[…] "*practical knowledge embedded in material artifacts, in institutions built to manage the artifacts, and in their interface with other social institutions*." (HERRERA, 2007, p. 74)

[18] "[…] *physical geography is an essential component of cyberspace: Where technology is located is as important as what it is. While our Internet activities may seem a kind of ephemeral and private adventure, they are in fact embedded in a complex infrastructure (material, logistical, and regulatory) that in many cases crosses several borders*." (BRUNN, 2015, p. 10).

agente em campo, gerando um custo menor e tendo a vantagem do anonimato[19] (PORTELA, 2018, p. 143).

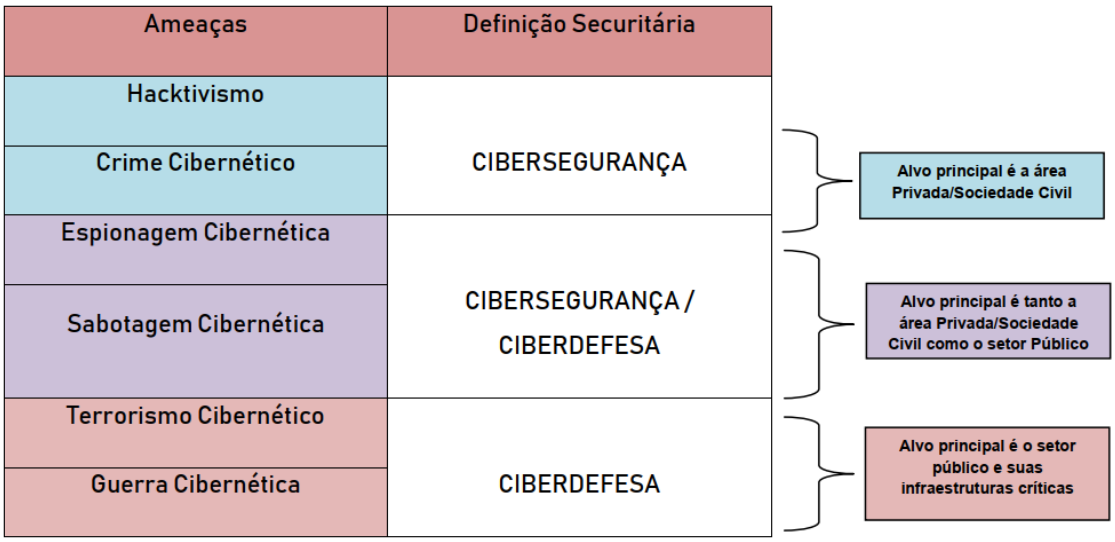
Assim, nas últimas décadas, os Estados têm se utilizado de meios cibernéticos para alcançar seus objetivos nacionais, em uma combinação de ciberespionagem, manipulação da informação, intervenções e econômicas e políticas e sabotagens (WILLETT, 2019). Diante disso, é relevante mencionar, os riscos provenientes dos avanços das capacidades ofensivas no ciberespaço para as infraestruturas críticas dos Estados e as possibilidades de conflitos nesse novo domínio trazerem consequência para os demais domínios.

2.1.2 Geopolítica cibernética: ameaças cibernéticas, ações ofensivas no ciberespaço e seus desdobramentos

Antes de iniciar a discussão aqui proposta, cabe fazer uma ressalva conceitual[20]. Assim como os demais termos que perpassam a cibernética, os conceitos de segurança cibernética e defesa cibernética também possuem diferentes variações nas suas definições, tanto entre os Estados quanto entre os autores especialistas na área. Apesar da linha tênue e frágil que separada as áreas da cibersegurança e da ciberdefesa, a diferenciação delas é necessária. 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). A figura 3 auxilia na compreender a divisão entre essas duas áreas.

[19] Por outro lado, cabe destacar que os recursos tradicionais de poder (como poder econômico, capacidade tecnológica e industrial e população, especificamente recursos humanos qualificados) seguem sendo fundamentais para o desenvolvimento do poder cibernético, como veremos mais adiante.
[20] Para mais conceituações, ver o apêndice A.

Figura 3 - Ameaças cibernéticas e suas definições securitárias



Fonte: Ayres Pinto, Freitas e Pagliari (2018, p. 48)

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 índices internacionais que serão analisados na próxima seção, já que estes vão trazer o termo "cibersegurança" de modo mais geral.

No âmbito da defesa cibernética, as ferramentas do ciberespaço vêm sendo aperfeiçoadas de modo a revolucionar o modo de se fazer a guerra no século XXI. Dessa maneira, o poder cibernético pode se traduzir em diversas vantagens em conflitos. Ataques cibernéticos, como a sabotagem cibernética, podem resultar em um 'efeito cascata' - ou seja, uma operação cibernética contra um sistema específico pode ter repercussões em outros sistemas, paralisando vários serviços essenciais. Se observada a característica da transversalidade – que permite a projeção de poder e seus reflexos nos demais domínios espaciais –, há grande potencial de causar danos sérios às sociedades e aos Estados.

Como aponta Stone (2013, p. 107, tradução própria): "os ataques cibernéticos representam um meio particularmente eficiente de traduzir a força em violência: bastam alguns toques no teclado para iniciar uma sequência de eventos potencialmente muito

violentos."[21] Ou, conforme indica Pool (2013, p. 310, tradução própria), as ferramentas do ciberespaço "podem causar danos por meios indiretos, como a morte de alguém como resultado de uma linha telefônica desconectada de um centro de atendimento de emergência devido a um ataque distribuído de negação de serviço".[22]

O espaço cibernético tornou-se, portanto, palco para a realização de confrontos e os recursos provenientes dele converteram-se em ferramentas poderosas em conflitos geopolíticos. Entretanto, esses conflitos não ocorrem à parte das rivalidades geopolíticas tradicionais, mas são uma nova dimensão dessas rivalidades (DOUZET, 2014). Partindo dessas considerações, a tendência da guerra como um fenômeno híbrido consolida-se como o cenário mais provável no século XXI. Ou seja, as ferramentas cibernéticas sendo utilizadas em operações de guerra (ou em outras campanhas cibernéticas com objetivos diversos) - como já o são - e não necessariamente a concepção de guerras cibernéticas autônomas (RID, 2013).

> A capacidade de coletar, analisar e manipular informações pode oferecer uma vantagem estratégica a um inimigo e lançar dúvidas sobre a confiabilidade das próprias informações. Os ataques cibernéticos podem interromper diretamente as comunicações, confundir o inimigo e até mesmo afetar suas capacidades operacionais, que dependem cada vez mais das redes para sua coordenação e operação.[23] (DOUZET, 2014, p. IX, tradução própria).

A guerra híbrida é definida pelo Balanço Militar de 2015 da Organização do Tratado do Atlântico Norte (OTAN) como "campanhas sofisticadas que combinam operações convencionais e especiais de baixo nível; ações cibernéticas e espaciais ofensivas; e operações psicológicas que usam mídias sociais e tradicionais para influenciar a percepção popular e a opinião internacional."[24] (VACZI, 2016, p. 38, tradução própria). Sendo assim, a guerra híbrida é uma "mistura de táticas convencionais e não tradicionais para alcançar objetivos

---

[21] "[…] *cyber attacks represent a particularly efficient means of translating force into violence: a few key strokes are all that are required to set in train a sequence of potentially very violent events*." (STONE, 2013, p. 107)

[22] "[…] *may cause harm through indirect means, such as someone dying as a result of a phone line being disconnected to an emergency call center due to a distributed denial-of-service attack." (POOL, 2013, p. 310)*

[23] "The capability to collect, analyze, and manipulate information can offer a strategic advantage to an enemy and casts doubt on the reliability of one's own information. Cyberattacks can directly disrupt communications, confuse the enemy, even affect its operational capabilities, which increasingly depend on networks for their coordination and operation" (DOUZET, 2014, p. IX).

[24] "[…] *sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion*." (VACZI 2016, 38).

político-militares."[25] (Charap 2015, p. 51, tradução própria), envolvendo, por exemplo, intervenções na política de outros países, danos financeiros, espionagem, coletas de dados e informações secretas, sabotagem, assim como ataques às infraestruturas estratégicas e essenciais dos Estados. A figura 4 ilustra os elementos da guerra híbrida, conforme Fernandes (2016).

Figura 4 - Imagem representativa dos elementos da guerra híbrida

Fonte: Imagem reproduzida por Fernandes (2016, p. 25).

Dialogando com essas perspectivas, uma das principais discussões que envolvem a geopolítica do ciberespaço está justamente nas suas infraestruturas físicas. Os cabos submarinos, por exemplo, são de importância crucial para o funcionamento do ciberespaço, uma vez que são os responsáveis por mais de 95% do tráfego de informações nesse domínio. Por consequência, o fluxo mundial de informações depende dos cabos submarinos e danos, interrupções ou manipulação desses cabos podem trazer graves prejuízos ao livre fluxo de informações e à logística militar, ao sistema financeiro, ao comércio, à agricultura, à

[25] "[…] *a blending of conventional and non-traditional tactics to achieve political–military objectives* […]" (Charap 2015, 51)

medicina, aos direitos humanos e à segurança nacional (SUNAK, 2017; SHERMAN, 2021; GRASSI, 2022).

Esses cabos, assim como grande parte da infraestrutura física e sistemas que formam o ciberespaço, são, em sua maioria, de propriedade privada[26], de empresas localizadas no Norte Global, as quais possuem interesses próprios que podem não confluir, ou serem divergentes, a interesses políticos, econômicos ou estratégicos de alguns Estados - ou de um grupo de Estados. Da mesma forma, os Estados podem pressionar empresas a agir de acordo com seus interesses. Como atesta Brunn (2015), algumas empresas receberam compensações financeiras para instalar equipamentos de vigilância em suas redes; outras foram secretamente hackeadas, como a Google foi pela *National Security Agency* (NSA); outras, ainda, foram submetidas a pressões estatais (formais ou informais), como ordens judiciais, retenção de licenças de operação ou apelos ao patriotismo.

> Essa forma de pressão do governo sobre o setor privado ilustra a importância da geografia física do ciberespaço. Claro, muitas das corporações que possuem e operam a infraestrutura – empresas como Facebook, Microsoft, Twitter, Apple e Google – estão sediadas nos Estados Unidos. Eles estão sujeitos à lei de segurança nacional dos EUA e, como consequência, permitem que o governo se beneficie de uma vantagem distinta em sua tentativa de "coletar tudo".[27] (BRUNN, 2015, p. 11, tradução própria).

Além disso, por não ser uma infraestrutura formalmente estatal, não há uma proteção robusta no âmbito do direito internacional para esses cabos que atravessam os oceanos e várias jurisdições. A Convenção Internacional para a Proteção de Cabos Submarinos - que consiste em um regime jurídico internacional para proteção e gerenciamento de cabos submarinos e é a base da Convenção das Nações Unidas sobre o Direito do Mar no que diz respeito aos cabos submarinos - pouco evoluiu desde sua criação, em 1884. Ademais, observam-se interesses conflitantes e dificuldades em termos de cooperação entre os Estados

[26] As relações de poder contemporâneas são compostas também por atores não estatais - os quais, inclusive passam a ter um papel crucial. De modo geral, o espaço cibernético possibilita a difusão de poder para atores não-estatais, devido a sua forte acessibilidade e a descentralização do sistema, isso porque os custos para se operar neste espaço são relativamente baixos (NYE, 2011; DOUZET, 2014; PORTELA, 2018).

[27] "*This manner of government pressure on the private sector illustrates the importance of the physical geography of cyberspace. Of course, many of the corporations that own and operate the infrastructure—companies like Facebook, Microsoft, Twitter, Apple, and Google—are headquartered in the United States. They are subject to US national security law and, as a consequence, allow the government to benefit from a distinct homefield advantage in its attempt to "collect it all.*" (BRUNN, 2015, p. 11).

e as empresas proprietárias dos cabos (DAVENPORT, 2012; SUNAK, 2017; CARTER; BURNETT, 2018; VICHI; AYRES PINTO; DE SÁ, 2020; SCOTT, 2021; GRASSI, 2022).

Outras problemáticas que envolvem os cabos submarinos e as demais infraestruturas do ciberespaço diz respeito às possibilidades de sabotagem, atos terroristas, espionagem, interceptação ou manipulação dos dados que trafegam através dessas infraestruturas. Essas ameaças tornam-se cada dia mais problemáticas se levarmos em consideração o crescente volume de dados e informações sensíveis que trafegam pelo meio digital, o que aumentará ainda mais com o avanço da tecnologia 5G (Quinta Geração). A infraestrutura do 5G demandará infraestruturas de cabos rápidas, seguras e resilientes para transportar a enorme quantidade de dados resultantes do grande volume de dispositivos da Internet das Coisas (IoT, do inglês, *Internet of Things*) (SUNAK, 2017; SHERMAN, 2021; GRASSI, 2022). Assim, ações ofensivas, como as mencionadas acima, podem gerar efeitos profundos em toda uma sociedade, prejudicando indivíduos e organizações públicas e privadas, comércio, defesa, transporte e logística e outros setores.

A evolução das tecnologias de informação e comunicação (TICs) atualizou e facilitou, por exemplo, a espionagem, uma prática já muito antiga. A ciberespionagem está entre as mais importantes ameaças provenientes do domínio cibernético e "refere-se à coleta clandestina de inteligência pela interceptação de comunicações entre computadores, bem como pela invasão das redes de computadores de outras pessoas para exfiltrar dados."[28] (RID, 2013, p. 82, tradução própria). Conforme Rid (2012), o principal uso dos recursos cibernéticos pelos Estados é justamente para ações de espionagem e, apesar de não se enquadrar como um ato de guerra ou como uma arma cibernética, é uma séria ameaça aos Estados. A informação é um recurso estratégico, que garante vantagens para a atuação estatal em prol da consecução de seus objetivos.

Inclusive, um dos maiores escândalos envolvendo ações no ciberespaço contornaram as ações de espionagem global e sistemática arquitetadas pelos Estados Unidos, através de suas agências de inteligência e segurança, especialmente a NSA, que foram reveladas em 2013. Entre os alvos diretos dessas espionagens estavam o governo brasileiro e a Petrobrás (OPPERMANN, 2014; TEIXEIRA; DATYSGELD, 2017). Nesse sentido, importa destacar a importância das ferramentas de ciberespionagem para colher informações sensíveis dos

[28] "[…] *cyber espionage, for the purposes of this study, refers to the clandestine collection of intelligence by intercepting communications between computers as well as breaking into somebody else's computer networks in order to exfiltrate data*." (RID, 2013, p. 82).

Estados e perpetuar interferências híbridas em prol de objetivos estratégicos diversos, como pode ser observado nos inúmeros dados e pesquisas que discutiram os objetivos e as consequências do citado esquema de espionagem estadunidense. Ademais, os recursos provenientes do ciberespaço resultam cruciais para que Estados mais desenvolvidos continuem a propagar seu poder e mantenham seu controle sobre países do Sul Geopolítico.

Sobre as interferências híbridas, estas 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 (WIGELL, 2021). Diante disso, tais ferramentas possuem potencial para comprometer valores democráticos e desestabilizar instituições políticas (WIGELL, 2021; OLIVEIRA; IZYCKI 2021). Também podem pressionar organizações econômicas e financeiras de um país, afetar sua moral e moldar o cenário interno, conforme as preferências de determinado grupo ou país.

Elemento central das interferências híbridas é a subversão, citada por Rid (2013), na qual o alvo é a mente humana. 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 (RID, 2013; WIGELL, 2021). 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 - já que é extremante dificultosa identificação da origem exata desse tipo de campanha cibernética - e sem ultrapassar o limiar do conflito. As campanhas de desinformação, manipulação da informação ou as interferências híbridas vêm crescendo e constituindo-se como incidentes extremamente complexos, altamente prejudiciais e de difícil contenção pelo Estado e, por isso, merecem a devida atenção nas estratégias estatais.

Quanto ao terrorismo cibernético, pode-se defini-lo como um “ataque premeditado e politicamente motivado contra as informações, sistemas de computadores, programas de computador e dados que resultam em violência contra alvos não combatentes por parte de

grupos subnacionais ou agentes clandestinos."[29] (CURRAN; CONCANNON; MCKEEVER, 2008, p. 1, tradução própria). As possibilidades de ações terroristas proporcionadas por esse ambiente digital são extensas, direcionando ataques às redes de computadores do governo, às redes financeiras, às usinas de energia, aos sistemas de abastecimento de água, aos hospitais e outros serviços de emergência, etc. Podem visar o roubo, a manipulação ou a corrupção de dados e informações ou, mesmo, a sabotagem de sistemas e infraestruturas (CURRAN; CONCANNON; MCKEEVER, 2008).

Diante de um cenário nebuloso, com várias frentes que podem afetar a segurança e defesa estatal, alguns Estados vêm advogando pela delimitação de sua soberania no que têm pleiteado como seu território nesse novo meio – apesar da complexidade de pensar em definir territórios soberanos no ciberespaço, da característica transnacional das relações e da fluidez dos limites jurisdicionais nesse espaço (DOUZET, 2014; AYRES PINTO; GRASSI, 2020).

Contudo, para Singer e Friedman (2014), da mesma forma que se divide as fronteiras físicas dos países, o ciberespaço também pode ser compreendido a partir da aplicação das noções de nacionalidade, soberania e propriedade. Assim, a ideia do ciberespaço como um "patrimônio global" ou um "bem comum global" é equivocada (SINGER; FRIEDMAN, 2014; SHELDON, 2014; AYRES PINTO; GRASSI, 2020). Desse modo, com a justificativa de garantir a segurança nacional ou a estabilidade econômica, alguns Estados têm ressaltado a necessidade de estabelecer os limites para o controle soberano desse espaço, ou seja, estabelecer pontos de ligação entre o ciberespaço nacional e o ciberespaço internacional, onde ocorrem a entrada e a saída dos dados que trafegam pelas redes, endurecendo, assim, as fronteiras cibernéticas (FERNANDES, 2012b; PORTELA, 2016).

Ferreira Neto (2014) defende que, apesar da propensão em declamar a inexistência de fronteiras no espaço cibernético, o que ocorre, na verdade, é a impossibilidade de pensar essas fronteiras da mesma forma que tradicionalmente se delimitou as fronteiras terrestres. Para esse autor, ainda que não regulamentadas, os Estados já estão se apropriando de parte desse espaço comum global e delimitando seus territórios – por exemplo, de forma mais tangível, ao estabelecer os domínios dos sítios ".br"; ".us"; ".uk", ".mx." etc.

Iniciativas de regulamentação e delimitação de limites e controles no ciberespaço estão ocorrendo pelos Estados individualmente e, em alguns casos, no âmbito de instituições

[29] "*Cyber terrorism is the premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents*." (CURRAN; CONCANNON; MCKEEVER, 2008, p. 1).

internacionais - como nas iniciativas no âmbito da OTAN (DEMCHAK; DOMBROWSKI, 2011; FERNANDES, 2012b, LOBATO; KENKEL 2015). Isso também pode ser observado pela afirmação do então Ministro da Defesa da França, Stéphane Dossé, em 2010: "Assim, parece necessário para os Estados 'plantar a bandeira' nos espaços que ocupam de modo a exercer todas as suas funções soberanas, colonizar espaços virgens, e estar preparado para enfrentar adversários neste espaço"[30] (apud DOUZET, 2014, p. tradução própria).

Não obstante, essas questões que envolvem impor limites, estabelecer fronteiras e proclamar o território soberano dos Estados nesse espaço, geram uma série de questionamentos e críticas, principalmente em torno das implicações resultantes do aumento do controle dos fluxos internos dos países e as possibilidades de uso autoritário por parte dos governos, diante desse maior controle. Isso porque poderiam produzir limites mais rígidos na esfera cibernética, vigilância ou controles de atividades, implantação de filtros e bloqueio de conteúdos, podendo levar a limitações e violações de direitos dos indivíduos e demais agentes internos. Ainda, geram receios sobre as possibilidades de intervenções em territórios que viriam a ser apontados como fontes de ataques cibernéticos, além das críticas acerca da utilização de uma lógica Westfaliana para tratar de questões de uma complexidade que talvez demandassem análises e soluções diferentes das tradicionais (AYRES PINTO; FREITAS; PAGLIARI, 2018; AYRES PINTO; GRASSI, 2020).

Isso, portanto, poderia gerar novas ameaças aos Estados e aos indivíduos, de modo geral. Como aponta Douzet (2014, p. XI, tradução própria), "as estratégias desenvolvidas pelos Estados para defender sua soberania e maximizar seu poder no ciberespaço têm consequências geopolíticas com as quais devemos nos preocupar e que, por sua vez, suscitam sérios questionamentos, até mesmo novas ameaças."[31] Além disso, reitera-se, conforme apontado anteriormente, que as características desse espaço, as quais acabam por ser compreendias como inevitáveis ou "fatalidades tecnológicas" (como o anonimato, a ideia de liberdade e privacidade), na verdade, são decisões políticas, que podem ser alteradas a partir

[30] "*It thus appears necessary for states to 'plant the flag' in the spaces they occupy in order to exercise all their sovereign functions, colonize virgin spaces, and be prepared to confront adversaries in this space"* (DOSSÉ, 2010 apud DOUZET, 2014, p. VII)

[31] "[…] *the strategies developed by states to defend their sovereignty and maximize their power in cyberspace have geopolitical consequences we must be concerned with and that in turn give rise to serious questions, even new threats*." (DOUZET, 2014, p. XI).

do movimento dos atores (FERNANDES, 2012b). Essas discussões sobre fronteiras e soberania no espaço cibernético ilustram bem essa proposição.

Observa-se, consequentemente, que o ciberespaço se tornou um ambiente em os Estados, principalmente os menos desenvolvidos, se deparam com grandes incertezas e aumento de suas fragilidades (PORTELA, 2018). Esse grupo de países, denominados como Sul Global ou Sul Geopolítico, enfrenta uma série de debilidades que se originam desde a falta de recursos financeiros, de recursos humanos qualificados e de desenvolvimento de ciência e tecnologia nacionais, somando-se a isso as fragilidades institucionais e a fraca estrutura de governança interna (MULLER, 2015; PAWLAK, 2016; PAWLAK; BARMPALIOU, 2017; SCHIA, 2018; CALDERARO; CRAIG, 2020). Essa situação resulta em vantagens e oportunidades de atuação e intervenções de atores mais desenvolvidos nesses países.

Diante do cenário apresentado, particularmente pensando nos países menos desenvolvidos, locais em há ocorrido o maior aumento de usuários de internet nos últimos anos, a construção de capacidades cibernéticas deve estar no centro das discussões. Ainda que o Norte Global siga tendo as maiores taxas de uso da Internet, é no Sul que se tem observado um aumento significativo de usuários nos últimos anos. Entre 2010 e 2017, a população com acesso à internet saltou de 4% para quase 18% nesses países. Enquanto isso, nos países com renda mais alta essa taxa aumentou de 72% para pouco mais de 82%. Desse modo, estima-se que, em 2025, 75% dos usuários de internet viverão no Sul Global (CALDERARO; CRAIG, 2020; GRASSI; AYRES PINTO, 2022a).

Apesar da crescente expansão do acesso ao ambiente digital, o fosso digital entre países do Sul e do Norte Global é enorme. Como frisa Chenou e Fuerte (2018, p. 49, tradução própria),

> Esta lacuna pode ser quantificada em termos de infraestruturas de Internet, acesso a novas tecnologias, banda larga, velocidade da Internet, Pontos de Troca de Tráfego (PTT), acesso a mercados digitais, novos desenvolvimentos, empreendedorismo digital e a lacuna em termos das muitas empresas no Norte que lideram o mundo da Internet e as poucas empresas do Sul que lutam por um espaço na web.[32]

[32] "*This gap can be quantified in terms of Internet infrastructure, access to new technology, broadband, Internet speed, Internet eXchange Points (IXP), access to digital markets, new developments, digital entrepreneurship and the gap in terms of the many companies in the North, that lead the world of the Internet and the few companies in the South, that struggle for a space on the web*." (CHENOU; FUERTE, 2018, p. 49)

A título de exemplo, a maioria dos Pontos de Troca de Tráfego (PTT, ou IXP, do inglês *Internet eXchange Points*)[33], os quais possibilitam o aumento da velocidade da internet e diminuição dos custos da mesma, está localizada nos países do Norte: 63% dos PTTs do mundo localizados em países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Por exemplo, enquanto a Colômbia, que possui um território de 1.141.749 km², possui apenas um PTT, a Suécia, com uma área de 450.295 km², possui 9. (CHENOU; FUERTE, 2018).

Ainda, mantém-se o desequilíbrio na representação e na participação ativa desses países nas instâncias internacionais de discussões sobre o futuro do ciberespaço, já que esses espaços de discussão e tomada de decisão continuam a ser dominados por atores do Norte Global. Dessa forma, grande parte desses países fica à margem dos processos de governança cibernética internacional, sem terem, portanto, seus interesses atendidos. Essa situação demonstra que os países do Sul Global não foram capazes de romper com a dominação estrutural do Norte (CHENOU; FUERTE, 2018).

Portanto, percebe-se a preocupação em inserir os países do Sul Global no mundo digital, no entanto, as inúmeras vulnerabilidades que acompanham essa inserção também precisam ser priorizadas, já que "a participação do Sul Global na digitalização não é simplesmente uma questão de adesão ao ciberespaço: é uma questão de formas seletivas de ligação global em combinação com a desconexão e a exclusão."[34] (SCHIA, 2018, p. 822, tradução própria).

> Se os sistemas digitais forem adotados sem serem protegidos, os elevados níveis de penetração da Internet poderão, em vez disso, contribuir para desestabilizar os governos, os sistemas eleitorais nacionais, os ambientes mediáticos e o discurso público, perturbando a estabilidade política e democrática.[35] (SCHIA, 2018, p. 822, tradução própria).

---

[33] Os Pontos de Troca de Tráfego, ou Internet Exchanges Points, "são pontos neutros onde diversas organizações estão interligadas para trocar pacotes de dados Internet entre si. Os PTTs são formados por datacenters com equipamentos que permitem a interligação simultânea de centenas de organizações – empresas de streaming de vídeo, sítios de buscas, redes sociais, bancos, universidades, órgãos de governo, entre outras. Essa união de redes permite que a Internet fique mais veloz, eficiente, resistente a falhas e com custo mais baixo." (CGI.br, 2019)

[34] "[…] *the Global South's participation in digitalisation is not simply a matter of joining cyberspace: it is a question of selective forms of global connection in combination with disconnection and exclusion*." (SCHIA, 2018, p. 822)

[35] "*If digital systems are adopted without being secured, high levels of Internet penetration might instead contribute to destabilising governments, national election systems, media environments and public discourse, disrupting political and democratic stability*." (SCHIA, 2018, p. 822).

Aumentar os níveis de conectividade e digitalização, sem manter o um alto nível de preocupação em relação às inúmeras ameaças provenientes desse domínio e sem desenvolver estratégias eficazes para manter os níveis de segurança, torna não só esse grupo de países e seus cidadãos vulneráveis, mas toda a sociedade internacional – principalmente levando em consideração a interconectividade dos sistemas e transnacionalidade do ciberespaço. Deficientes capacidade cibernéticas afetam a estabilidade global no ciberespaço, já que podem impactar na proteção de outros países contra ações cibernéticas maliciosas que podem se originar desses países ou se utilizar das fragilidades desses que carecem de infraestrutura e governança adequadas (HOHMANN; PIRANG; BENNER, 2017; SCHIA, 2018; CALDERARO; CRAIG, 2020; GRASSI; AYRES PINTO, 2022a). Inclusive, essas são questões abrangidas nas discussões internacionais no que se trata da promoção de iniciativas para a construção de capacidades cibernéticas e disseminação de melhores práticas entre os Estados ao redor do mundo.

Por outra perspectiva, os países do Sul Global sofrem os impactos da acirrada competição geoeconômica e geopolítica em curso entre as grandes potências, particularmente entre Estados Unidos, Rússia e China (MORAIS DA SILVA; GRASSI, 2022). Sobretudo, a questão tecnológica é o ponto mais sensível da chamada Guerra Comercial entre Estados Unidos e China e tem como cerne justamente a liderança em relação às infraestruturas de comunicação, que impacta substancialmente, por consequência, as dinâmicas securitárias e implicará no processo de transição sistêmica (PAUTASSO et al., 2021). Essa conjuntura tem levado a cenários desestabilizadores no Sul Global, inclusive, com o emprego das ferramentas provenientes com o ciberespaço, utilizadas para intervenções e ciberataques.

As capacidades de cibersegurança são também associadas como componentes fundamentais ao desenvolvimento econômico, principalmente se observado que as áreas com maior potencial de crescimento são aquelas onde os riscos associados à cibersegurança são maiores. Desse modo, ao mesmo tempo que a inserção no ambiente digital resulta em diversos riscos, a digitalização e a construção de cibercapacidades para um ambiente digital seguro podem ser considerados elementos-chave para o desenvolvimento econômico e social, bem como para fortalecer as sociedades democráticas (PAWLAK, 2016; PAWLAK; BARMPALIOU, 2017; SCHIA, 2018). Assim, construir capacidade cibernética no Sul Global é crucial para proteger suas instituições políticas, econômicas e sociais (PAWLAK, 2016; SCHIA, 2018; CALDERARO; CRAIG, 2020; GRASSI; AYRES PINTO, 2022a).

Por fim, cabe adicionar também o fato de que, comparativamente aos tradicionais recursos de poder (por exemplo, as armas nucleares), os recursos cibernéticos são considerados mais baratos e mais acessíveis aos países menos desenvolvidos (SCHIA, 2018; CALDERARO; CRAIG, 2020; GRASSI; AYRES PINTO, 2022a). Esse fator deve ser levado em consideração nas perspectivas de construção de capacidades pelo Sul Global, por aumentar suas possibilidades de ganho de poder no sistema internacional.

Partindo disso, a seção seguinte se debruçará em definir capacidade cibernética e compreender a relação entre a construção de capacidades e o desenvolvimento de poder cibernético, avaliando as formas de obtenção e mensuração desses conceitos. Para isso, continua-se resgatando a literatura especializada, ao mesmo tempo que se analisa importantes rankings internacionais e suas dimensões e indicadores, buscando formular uma compreensão sobre os elementos mais relevantes para a construção de capacidade cibernética pelos Estados.

2.2 EM BUSCA DE PODER E SEGURANÇA CIBERNÉTICA: CONSTRUÇÃO DE CAPACIDADES CIBERNÉTICAS E MODELOS PARA AVALIAR A MATURIDADE CIBERNÉTICAS DOS ESTADOS

O espaço cibernético tem desempenhado um papel cada dia mais vital, seja na dimensão econômica, política, diplomática, militar ou social. Como observado na seção anterior, nesse âmbito surgem diversas ameaças para a segurança e a defesa dos Estado e, em realidade, para o simples funcionamento de todos os aspectos da vida na sociedade contemporânea. Assim, desenvolver capacidades cibernéticas e, consequentemente, poder cibernético torna-se essencial.

Poder e segurança no ciberespaço estão intimamente relacionados à construção de capacidades – conjuntamente com uma estratégia adequada para sua utilização. Isso porque, diante do exposto até aqui e como veremos a seguir, a obtenção e a preservação do poder cibernético, bem como a manutenção e incremento da cibersegurança e da ciberdefesa, depende da construção de capacidades cibernéticas, já que tais capacidades criam as condições para um país obter vantagens e produzir resultados no ciberespaço e nos demais ambientes.

Como mencionado na seção anterior, o poder depende do contexto, já que só pode ser dimensionado a partir de uma relação. Contudo, o poder cibernético (assim como o poder

militar, por exemplo) é uma dimensão de poder e depende da posse de recursos, disponíveis a partir do ciberespaço, e da acertada estratégia de utilização desses recursos. De acordo com Nye (2010, p. 3, tradução própria), "poder depende do contexto, e o poder cibernético depende dos recursos que caracterizam o domínio do ciberespaço."[36]

Assim, Kuehl (2009) e Nye (2011) ponderam que esse poder é moldado por múltiplos fatores, que moldam como o ciberpoder é empregado. Entre esses fatores os autores citam os tecnológicos, os informacionais, os organizacionais e os humanos. Já para Klimburg (2011, p. 43, tradução própria) poder cibernético perpassa por três dimensões: "[1] coordenação de aspectos operacionais e políticos em estruturas governamentais, [2] coerência de políticas por meio de alianças internacionais e estruturas legais e [3] cooperação de atores cibernéticos não estatais."[37] O autor frisa que a dimensão mais importante do poder cibernético nas democracias ocidentais é a capacidade de mobilizar seus cidadãos, sendo necessário criar uma abordagem de capacidade nacional integrada, com a cooperação entre os todos os setores – estatal e não estatal (empresas e sociedade civil).

Klimburg (2011) traz o poder cibernético para uma perspectiva mais defensiva, de modo a garantir melhores práticas de segurança cibernética aos Estados que o detém, em contraposição com a lógica ofensiva clássica de poder.

> Essa visão destaca que o poder cibernético e a segurança cibernética estão intrinsecamente ligados. Uma entidade política possui poder cibernético se tiver a capacidade de moldar aspectos do cenário global de segurança cibernética. No entanto, um poder cibernético também precisa ser capaz de 'defender' contra ameaças cibernéticas, ou melhor, gerenciá-las adequadamente. Essas necessidades, ciberresiliência interna e ciberpoder externo, se complementam: nessa visão, não pode haver verdadeiro ciberpoder sem ciberresiliência – e vice-versa.[38] (CAVELTY, 2018, p. 6, tradução própria)

Sobre a importância da adquirir poder cibernético, Sheldon (2014, p. 292, tradução própria) frisa:

---

[36] "*Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace*." (NYE, 2010, p. 3)

[37] […] "*coordination of operational and policy aspects across governmental structures, coherency of policy through international alliances and legal frameworks, and cooperation of non-state cyber actors."* (KLIMBURG, 2011, p. 43)

[38] "*Such a view highlights that cyberpower and cyber-security are intricately linked. A political entity possesses cyber-power if it has the ability to shape aspects of the global cyber-security landscape. However, a cyber-power also needs to be able to 'defend' against cyber-threats, or rather, manage them adequately. These necessities, internal cyber-resilience and external cyber-power, build on each other: in this view, there cannot be any true cyber-power without cyber-resilience – and vice versa*" (CAVELTY, 2018, p. 6)

> O que torna o poder cibernético único na geopolítica é sua influência não apenas como um instrumento de poder em si, mas sua influência direta (assim como indireta) sobre os outros instrumentos de poder mais tradicionais. [...] A influência do poder cibernético, tanto em si quanto em outros instrumentos de poder, é tão profunda que mudou não apenas o caráter da guerra em todos os outros domínios, mas também mudou o caráter da diplomacia, economia e a expressão da cultura, enquanto, ao mesmo tempo, fornece mais uma ferramenta, embora penetrante, com a qual os estados competem uns com os outros em vários locais e sobre uma série de questões.[39]

Fato é que existem diferentes perspectivas sobre poder cibernético e algumas tentativas de medi-lo. Entretanto, conforme defende Cavelty (2018), poder cibernético pode vir de diferentes formas ou a partir de diferentes dimensões. Nesse sentido, sua análise dependerá do contexto, das possibilidades, limites e desafios de cada Estado.

Gradualmente, tem se observado que a temática relativa à construção de capacidades cibernéticas tem se tornando central nos debates sobre a segurança e a defesa cibernética, entrando na agenda de organismos internacionais, como a Organização do Tratado do Atlântico Norte (OTAN), a União Internacional de Telecomunicações (UIT), o Banco Mundial, a União Europeia (UE), a União Africana (UA), a Associação das Nações do Sudeste Asiático (ASEAN), o Conselho da Europa (CE), a Organização de Cooperação de Shangai (OCS) e a Organização dos Estados Americanos (OEA) (PAWLAK, 2016; PAWLAK; BARMPALIOU, 2017). Da mesma forma, instituições de pesquisa têm produzido relatórios, desenvolvido metodologias e índices internacionais nos quais mensuram e classificam os países com base nas suas capacidades em diversas dimensões.

Parte-se então, nessa seção, para o entendimento de capacidade cibernética, o qual é um conceito particularmente difícil de ser mensurado, não havendo consenso na literatura sobre seus componentes, indicadores ou como efetivamente devem ser avaliadas as capacidades dos Estados. Desse modo, serão resgatadas bibliografias que discutem o tema e analisados rankings internacionais que buscam mensurar as capacidades dos Estados, de modo a compreender os pilares centrais e os fatores que devem ser perseguidos em prol do desenvolvimento do poder cibernético e segurança cibernética.

---

[39] "*What makes cyber power unique in geopolitics is its influence not only as an instrument of power in its own right, but its direct (as well as indirect) influence on the other, more traditional, instruments of power. [...] The influence of cyber power, in its own right as well as on other instruments of power, is so profound that it has changed not only the character of warfare in all the other domains, but has also changed the character of diplomacy, economics, and the expression of culture, while, at the same time, providing yet another, albeit pervasive, tool with which states compete with one another in various locations and over any number of issues.*" (SHELDON, 2014, p. 292)

2.2.1 Conceituando capacidade cibernética e compreendendo as vias para sua construção

De forma a chegar a um entendimento sobre os elementos centrais que devem ser considerados para um projeto coeso em vista a construção de capacidades cibernéticas, alguns estudos vêm sendo conduzidos ao redor do globo. De modo amplo, conforme Hurel (2021, p. 9), capacidades cibernéticas são um "conjunto de iniciativas que visa empoderar indivíduos, sociedades e governos para desfrutarem dos benefícios da digitalização". A construção dessas capacidades é entendida como um "processo multidimensional, multicamada e multiator"[40] (PAWLAK; BARMPALIOU, 2017, p. 2, tradução própria).

Assim, Pawlak (2016, p. 84, tradução própria) define a construção de capacidade em termos de "desenvolvimento de recursos humanos, arranjos organizacionais e estruturas legais e institucionais [que] visam, em última análise, uma transformação social e política profunda."[41] De forma mais detalhada, Pawlak e Barmpaliou (2017, p. 2, tradução própria) defendem que a construção de capacidade depende, basicamente, de três dimensões interdependentes que se reforçam mutuamente:

I) capacidades individuais - visando melhorar as habilidades, competências técnicas, conhecimentos e as atitudes no setor cibernético, implementando programas de treinamento, mentoria, bolsas de estudo e planos educativos, de modo geral;

II) estruturas organizacionais – aspirando fortalecer e tornar mais eficientes os processos e redes, as dinâmicas internas, bem como a interligação entre as esferas do Estado. Entre os mecanismos e atividades estariam o desenvolvimento de procedimentos operacionais padrão, medidas administrativas, técnicas e processuais para gestão e proteção das redes, criação de Equipes de Resposta a Incidentes de Segurança Informática (CSIRTs, do inglês, *Computer Security Incident Response Team*), reforço dos procedimentos de coordenação interagências, parcerias público-privada, exercícios de avaliação de risco e apoio de pesquisas sobre segurança cibernética;

III) quadros institucionais, políticos e jurídicos – criando um "ambiente propício" de legislações, políticas e estratégias no setor. Nesse pilar estariam, portanto, a criação de uma

[40] "[…] *a multi-dimensional, multi-layer and multi-actor process* […]" (PAWLAK; BARMPALIOU, 2017, p. 2)
[41] "[…] *human resources development, organisational arrangements and legal and institutional frameworks is ultimately aimed at deep societal and political transformation*." (PAWLAK, 2016, p. 84).

efetiva estratégia nacional de cibersegurança, leis sobre cibercriminalidade e cibersegurança, padrões para aplicações das leis, alocação de recursos orçamentários para a construção de capacidades cibernéticas, campanhas de conscientização e educação no setor e a garantia do respeito pelas liberdades fundamentais[42].

Do mesmo modo, Schia (2018), define que os modelos de construção capacidade cibernética, geralmente, são formados por três categorias fundamentais: recursos tecnológicos, humanos e organizacionais – envolvendo, fatores comportamentais e políticos. Para o autor, a capacitação envolve também a construção de estratégias cibernéticas abrangentes e robustas que sejam capazes não apenas de prevenir incidentes cibernéticos, já que nem todos os incidentes podem ser evitados, mas que possibilitem ao Estado resistir, responder e se recuperar desses incidentes, ou seja, melhorar a resiliência cibernética.

Por seu turno, Muller (2015, p. 2, tradução própria) pondera 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."[43] A autora ressalta a importância da estabilidade institucional, produzir conhecimentos e estruturas legais e educar e conscientizar todas as camadas sociais, assim como aponta para a necessidade de implementar parcerias entre os setores público e privado.

Ademais, Pawlak (2016) ressalta que os esforços para a construção de capacidades cibernéticas não estão desvinculados da agenda política mais ampla, sendo debate fundamental também no âmbito da política externa. Isso porque fazer parte das discussões internacionais sobre a governança cibernética, influenciar na construção das normas e padrões globais e garantir que seus interesses estejam na agenda internacional também tem um papel crítico na promoção da autonomia dos Estados na área, na sua segurança e no desenvolvimento socioeconômico. Além disso, destaca-se que parte dos estudos sobre construção de capacidades cibernéticas definem essa área em termos de colaboração ou apoio

---

[42] Os autores ressaltam a importância de que os projetos para a construção de capacidades cibernéticas estejam integrados num quadro normativo que garantam o equilíbrio e o controle necessário frente à dupla natureza das capacidades cibernéticas, as quais são, por um lado, fonte de desenvolvimento e segurança, mas, por outro, podem resultar em abusos por parte dos Estado, colocando em perigo garantias e direitos fundamentais (PAWLAK; BARMPALIOU, 2017).

[43] "*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).

fornecido principalmente aos países em desenvolvimento ou entre países em desenvolvimento para aumentar o acesso eficiente e seguro ao ciberespaço, mitigando riscos, promovendo um ambiente aberto, estável e pacífico (HOMBURGER, 2019; COLLETT, 2021).

Calderaro e Craig (2020, p. 14, tradução própria), com base em dados e análises feitas a partir de índices cibernéticos internacionais, defendem que "quanto mais pesquisas científicas um país produzir, maior será sua capacidade cibernética, controlando outros fatores", já que o "conhecimento de C&T é um recurso crucial para o desenvolvimento da prontidão para a segurança cibernética".[44] Do mesmo modo, partindo para uma perspectiva mais ampla, reiteram também "o impacto que o conhecimento nacional de C&T tem na capacidade de formulação de políticas dos países."[45] (CALDERARO; CRAIG, 2020, p. 16, tradução própria).

Analisando estudos relacionados à temática, Calderaro e Craig (2020) defendem que os países mais vulneráveis em matéria de segurança cibernética são justamente os que carecem em termos de treinamento e educação. Desse modo, argumentam que iniciativas para promover capacidade cibernética devem ser relacionadas ao acesso do país à ciência e tecnologia. Na direção proposta, a construção de cibercapacidades perpassa a disposição de recursos econômicos direcionados à área, já que países com renda mais alta poderão investir mais em ciência e tecnologia que, por sua vez, levará a maior capacidade cibernética.

Somando-se a esses fatores, a construção de capacidades perpassa a difusão de habilidades técnicas, diplomáticas e de governança, formando, assim, o que Calderaro e Craig (2020) compreendem como os componentes mais robustos para a análise do nível de construção de capacidades cibernéticas. Ademais, os autores ressaltam a relevância de estratégias colaborativas entre os setores, que envolvam governo, indústria e atores da sociedade civil.

Creese et al. (2021) sustenta, em suas análises, que o nível de desenvolvimento econômico de um país molda sua capacidade cibernética, demonstrando que nações mais ricas possuem consideráveis vantagens no setor, o que acaba por reforçar as desigualdades na construção de capacidades cibernéticas e nos seus resultados para os países. No entanto, ressalta que este não é fator determinante, já que países com nível de Produto Interno Bruto

[44] "*The more scientific research a country produces, the higher its cyber capacity is likely to be while controlling for other factors, […] S&T knowledge is a crucial resource for developing cybersecurity readiness*." (CALDERARO; CRAIG, 2020, p. 14).
[45] "[…] *the impact that national S&T knowledge has on countries' policymaking capacity*" (CALDERARO; CRAIG, 2020, p. 16).

(PIB) per capita médio também tem se destacado na construção de capacidades cibernéticas. Diante disso, concorda com Calderaro e Craig (2020) que outros fatores como o desenvolvimento científico e os esforços educacionais têm importante influência no desenvolvimento de capacidades cibernéticas.

Da mesma forma, Pawlak e Barmpaliou (2017) ressaltam que é crucial recursos humanos variados e capacitados presentes nos diferentes setores governamentais, se envolvendo na consolidação de políticas consistentes, atuando de forma interligada, com a troca de informações e realização de consultas, desenvolvendo processos e programas conjuntos e criando um quadro que se reforce mutuamente. Nesse sentido, destacam:

> [...] a necessidade de investimento institucional em 'corretores de conhecimento cibernético' em todos os níveis de governo e em todas as políticas, bem como o desenvolvimento de uma abordagem baseada em princípios para a construção de capacidades no ciberespaço com uma perspectiva sustentável para o fechamento da 'lacuna de capacidade cibernética'.[46] (PAWLAK; BARMPALIOU, 2017, p. 3, tradução própria).

Pawlak e Barmpaliou (2017) reiteram que além das práticas específicas que precisam ser adotadas em cada agência, setor ou organismo estatal, são necessários pontos de contato constante, redes formais e informais que possibilitem a troca de experiências e lições, possibilitando uma atuação conectada, fortalecendo a dimensão organizacional das capacidades cibernéticas. Desse modo, ressaltam:

> Até a data, vários governos investiram na nomeação de 'embaixadores cibernéticos' para representar os seus interesses a nível internacional. No entanto, nos níveis mais baixos do governo, ainda existe uma necessidade premente de estabelecer a cultura de nutrir redes formais e informais de funcionários que lidam diariamente com questões cibernéticas, com recursos humanos e financeiros adequados para manter o seu funcionamento. Estes corretores de conhecimento – servindo como pontos de contato cibernéticos dentro e fora das suas respetivas organizações – representam a forma mais promissora de transposição de lições e experiências. A promoção de tais 'corretores de conhecimento cibernético' que criarão uma massa real de conhecimentos locais deverá permitir, em troca, a escalabilidade de iniciativas de capacitação que possam ser contextualizadas nas circunstâncias locais e, portanto, sejam sustentáveis.[47] (PAWLAK; BARMPALIOU, 2017, p. 15, tradução própria).

---

[46] "[...] *the need for institutional investment in 'cyber knowledge brokers' at all levels of government and across policies as well as the development of a principle-based approach to capacity building in cyberspace with a sustainable outlook towards closing the 'cybercapacity gap'*." (PAWLAK; BARMPALIOU, 2017, p. 3).

[47] "*To date, several governments have invested in appointing 'cyber ambassadors' to represent their interest at international level. However, at lower levels of government there is still a pressing need to establish the culture of nourishing formal and informal networks of officials dealing with cyber issues on a day-to-day basis with appropriate human and financial resources to maintain their functioning. These knowledge brokers – serving as cyber contact points within and outside of their respective organisations – represent the most promising way for*

Sobre isso, Choucri (2012) também argumenta que novos parâmetros passam a ser tornar centrais para fundamentar o poder na política internacional, como educação, habilidades, gestão do conhecimento e as mais variadas manifestações de "poder do cérebro".

Ainda, sobre o capital humano, este é identificado o mais importante recurso para contrapor as ameaças cibernéticas (KLIMBURG, 2011; AMIN, 2019). Discute-se também a importância da diversificação da formação dos recursos humanos recrutados para atuar no setor cibernético. Essa diversificação pode possibilitar uma melhor compreensão em relação às ameaças que o país enfrenta e, consequentemente, desenvolver melhores estratégias de atuação. Sobre isso, cabe ressaltar a atuação do Ministério das Forças Armadas da França que vem buscando aumentar e diversificar seu pessoal, recrutando especialistas em tecnologia da informação e redes, mas também linguistas, psicólogos, especialistas em relações internacionais e outras possíveis áreas (CHAPLEAU, 2021; SAMAMA, 2021). Para a então Ministra das Forças Armadas Francesas, Florence Parly, é "essencial [também] ter um conhecimento detalhado dos diferentes ambientes culturais e políticos em que nossos exércitos estão engajados"[48] (*apud* SAMAMA, 2021, s. p., tradução própria).

Sobre a abordagem baseada em princípios, mencionada por Pawlak e Barmpaliou (2017), Hohmann, Pirang e Benner, (2017) também a defendem, sugerindo cinco princípios orientadores:

I) coordenação e cooperação nacional e internacional: coordenação nacional entre os intervenientes de setores-chave, trabalhando conjuntamente com a sociedade civil, o meio acadêmico e o setor privado. Para isso, agências de coordenação devem ser estruturadas. A abordagem global envolve, por um lado, a participação ativa e consistente em fóruns internacionais, visando melhor comunicação, transparência e troca de conhecimentos; por outro, para desenvolvimento de projetos específicos, as organizações regionais são consideradas pelos autores como catalizadores essenciais.

II) integração de conhecimentos especializados em segurança cibernética e desenvolvimento: adoção de uma abordagem integrada, promover esforços conjuntos entre os

---

transposing lessons and experiences. Fostering such 'cyber knowledge brokers' that will create a real mass of local expertise shall allow, in return, the scalability of capacity building initiatives that can be contextualised in the local circumstances, and therefore be sustainable." (PAWLAK; BARMPALIOU, 2017, p. 15)

[48] "[…] *essentiel d'avoir une fine connaissance des différents environnements culturels et politiques où nos armées sont engages*." (SAMAMA 2021)

setores estatais que, apesar de manter projetos separados, devem trabalhar em prol de objetivos semelhantes e aumentar projetos conjuntos, mantendo o diálogo constante.

III) apropriação do país destinatário: desenvolvimento de projetos conjuntos com intervenientes internacionais nos quais as prioridades estratégicas dos países destinatários sejam respeitadas e os esforços sejam adaptados à realidade destes.

IV) sustentabilidade dos esforços: a construção de capacidades é um processo a longo prazo e seus esforços precisam ser sustentados ao longo do tempo. Nesse sentido, torna-se necessário uma explícita visão sobre os propósitos e as finalidades dos esforços empreendidos. Sobre isso, os autores também ressaltam a importância da "formação dos formadores", bem como o papel das universidades que podem estabelecer centros de excelência e difusão de conhecimento.

V) aprendizagem contínua e mútua: sobre quais medidas funcionaram e quais não funcionaram e o porquê. Para isso, é fundamental a transparência e o desenvolvimento de mecanismos de medição, avaliação e de feedback estruturados e contínuos. Os autores ressaltam a importância dos índices de maturidade das capacidades, como os mencionados - que serão especificados na próxima seção -, que podem auxiliar os Estados no acompanhamento de seus progressos.

Diante do exposto, pode-se compreender que as disparidades de conhecimentos e habilidades entre Estados do Norte e do Sul Global seriam uma das principais razões para os distintos níveis de capacidades cibernéticas (PAWLAK; BARMPALIOU, 2017; SCHIA, 2018; CALDERARO; CRAIG, 2020). Isso porque delas se sustentariam os demais pilares da construção de capacidades cibernéticas.

Por fim, cabe mencionar que os relatórios do Grupo de Especialistas Governamentais da ONU (GGE) sobre Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional "destaca[m] a importância de melhorar a segurança da infraestrutura crítica de Tecnologia da Informação e Comunicação (TIC) e desenvolver habilidades técnicas e legislação, estratégias e estruturas regulatórias apropriadas"[49]. Do mesmo modo, "reconhece[m] o papel da capacitação como um mecanismo para ajudar os países em desenvolvimento a fechar a lacuna entre os diferentes níveis de proteção previstos

[49] "*The UN GGE also highlights the importance of improving the security of critical Information and Communications Technology (ICT) infrastructure and developing technical skills and appropriate legislation, strategies and regulatory frameworks*" (PAWLAK; BARMPALIOU, 2017, p. 3)

nas leis e práticas nacionais."[50] (PAWLAK; BARMPALIOU, 2017, p. 3, tradução própria). A construção de capacidade é compreendida como fundamental para a proteção da segurança nacional e internacional, como via necessária para garantir a estabilidade do ciberespaço global (HOMBURGER, 2019).

Os relatórios ressaltam, ademais, a importância de promover medidas de cooperação e a assistência internacional, como um caminho possível para melhorar os níveis de proteção das TICs e garantir o uso pacífico do ciberespaço. Também recomendam "abordagens regionais para o reforço de capacidades que permitam uma abordagem personalizada tendo em conta aspectos culturais, geográficos, políticos, econômicos ou sociais específicos e os incentive a formar iniciativas de cooperação bilateral e multilateral."[51] (PAWLAK; BARMPALIOU, 2017, p. 6, tradução própria).

Um importante desafio para relações cibernéticas internacionais são as incertezas e as desconfianças geradas no ciberespaço, uma vez que é difícil saber se um conhecimento ou tecnologia compartilhado será usado para a proteção do país em questão e não para atacar. Além disso, a facilidade de atuar no anonimato aumenta a insegurança dos atores (MULLER, 2015; MEDEIROS; GOLDONI, 2020). Nessa direção, conforme Pawlak e Barmpaliou (2017, p. 7, tradução própria), "a progressiva militarização do ciberespaço e a dependência de novos sistemas de armas cibernéticas estatais levantaram preocupações sobre uma corrida armamentista cibernética e a competição pela "supremacia digital" que, em última análise, aumenta o risco de escalada e conflito."

Nessa perspectiva, medidas de cooperação, de construção de confiança e aumento da transparência e do diálogo internacional, desenvolvimento de princípios e normas e a construção de capacidades, torna-se cada dia mais importante para a estabilidade do ciberespaço global. Ademais, como mencionado na seção anterior, a construção de capacidades tem especial relevância para os países do Sul Geopolítico, os quais enfrentam maiores desafios no setor. Dessa maneira, Pawlak e Barmpaliou (2017, p. 17, tradução própria), também defendem:

---

[50] "[...] *acknowledge the role of capacity building as a mechanism to assist developing countries in closing the gap between different levels of protection provided for in national laws and practices*." (PAWLAK; BARMPALIOU, 2017, p. 3)

[51] "[…] *to develop regional approaches to capacity building that allow for a tailored approach taking into account specific cultural, geographic, political, economic or social aspects and encourages them to form bilateral and multilateral cooperation initiatives.*" (PAWLAK; BARMPALIOU, 2017, p. 6)

> A cooperação com campeões regionais que tenham algum grau de maturidade e vontade de se envolverem na Cooperação Sul-Sul e Triangular com os seus vizinhos menos desenvolvidos também poderia ser uma modalidade eficaz para enfrentar este desafio, contribuindo para o desenvolvimento de centros locais com alfabetização cibernética.[52]

Chenou e Fuerte (2018) também apontam para a importância do regionalismo e da Cooperação Sul-Sul[53] para melhorar a posição dos países em desenvolvimento e seu poder de decisão e barganha nas instâncias internacionais de discussão e tomada de decisão sobre padrões, normas e processos de governança cibernética. Essas iniciativas são fundamentais no sentido de identificar interesses comuns e definir estratégias conjuntas de inserção internacional.

Da mesma forma, para Calderaro e Craig (2020, p. 2, tradução própria), que discutem a construção de capacidades no Sul Global especificamente trazendo suas análises para Estados que não possuem claros rivais no âmbito militar, as "abordagens baseadas na teoria de RI [Relações Internacionais] para a segurança cibernética, inspiradas por paradigmas militares e de dissuasão, têm pouco impacto observável na capacidade cibernética".[54]

Nessa direção, ressalta-se a perspectiva de que parceiros regionais frequentemente encontram-se em um contexto geopolítico que os aproxima e favorece agendas de cooperação. Ademais, os diferentes níveis de capacidades cibernéticas e as assimetrias que podem existir nas dimensões que formam um projeto de capacitação podem também ser compreendidas como oportunidades de trocas e aprendizagem mútuas, propiciando um ambiente de ganhos recíprocos. Partindo dessas observações, o próximo capítulo focará justamente em trazer perspectivas sobre a diplomacia cibernética, discutindo sobre cooperação cibernética e analisando o cenário sul-americano.

Entretanto, antes disso, serão apresentados, na seguinte subseção, estudos e investigações sobre capacitação cibernética realizados por prestigiados institutos e centros de

---

[52] "*Cooperation with regional champions that will have some degree of maturity and willingness to engage in with their least developed neighbours could also be an effective modality to address this challenge, contributing to the development of cyber-literate local hubs*." (PAWLAK; BARMPALIOU, 2017, p. 17).

[53] Cooperação Sul-Sul pode ser compreendida como um quadro amplo de cooperação, colaboração, diálogo e parceria entre atores do Sul Global, sejam essas relações bilaterais ou multilaterais, na qual os atores envolvidos podem compartilhar conhecimentos, experiências, recursos, coordenar posições, realizar intercâmbio de acadêmicos e especialistas e outras ações e projetos conjuntos em diversas áreas. Pode perpassar questões políticas, sociais, ambientais, culturais, econômico-comerciais, técnicas, científicas e tecnológicas. (AL-KHATIB, 2023; TOSSD, 2023).

[54] "*IR theory-driven approaches to cybersecurity inspired by military and deterrence paradigms have little observable impact on a country's cyber capacity*." (CALDERARO; CRAIG, 2020, p. 2)

pesquisas ao longo dos últimos anos. Espera-se que as análises e definições propostas auxiliem na compreensão dos pilares e fatores fundamentais para a construção de capacidades pelos Estados.

2.2.2 Mensurando e classificando capacitação cibernética: os rankings internacionais

Importantes instituições e centros de pesquisa têm conduzido investigações, publicado relatórios e desenvolvido rankings internacionais nos quais estabelecem parâmetros para avaliar as capacidades de cibersegurança e ciberdefesa dos Estados, ao passo que classificam os países a partir de dimensões e indicadores elencados. Essas dimensões e indicadores também podem servir como um direcionamento para a compreensão dos componentes necessários à construção de capacidades cibernéticas.

Nessa seção três índices são enfatizados. Esses índices serão utilizados nos capítulos posteriores desta pesquisa como uma forma de analisar o subcontinente sul-americano e avaliar as informações referentes aos três países elegidos para o aprofundamento da pesquisa – Argentina, Brasil e Colômbia. São estes:

I) o *Global Cybersecurity Index* (GCI), desenvolvido pela UIT;

II) o *National Cyber Security Index* (NCSI), do *Think Tank e-Governance Academy*, da Estônia; e

III) o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (CCMM, do inglês *Cyber Security Capacity Maturity Model*), construído pelo *Global Cyber Security Capacity Centre* (GCSCC) da Universidade de Oxford, do Reino Unido.

O *Global Cybersecurity Index (GCI),* da União Internacional de Telecomunicações (UIT) das Nações Unidas, teve seu primeiro relatório publicado em 2015 e sua última edição publicada em 2020. Entre os objetivos da formulação e atualização dos relatórios apresentados pela organização estão o de medir a evolução do compromisso dos Estados quanto à segurança cibernética, identificar as lacunas, permitir a autoavaliação dos países e norteá-los para que possam aperfeiçoar suas estratégias no setor (UIT, 2020).

Dos 193 Estados membros das Nações Unidas (mais o Estado da Palestina), o último relatório contou com 150 contribuições, permitindo avaliar de forma mais eficiente as capacidades de cibersegurança desses Estados, os quais responderam as 82 perguntas

formuladas pela equipe responsável pelo GCI. Para os Estados que não responderam (ou se recusaram a responder) aos questionários[55], foram feitas pesquisas em sites, documentos oficiais e outros recursos -contudo, salienta-se que isso dificulta uma precisa classificação devido à dificuldade de acesso às informações. Conforme o próprio relatório, as perguntas e as ponderações dos pesos dos indicadores são atualizadas ao longo dos anos pelos especialistas nomeados pelos países membros da UIT, buscando refletir as mudanças nas preocupações do setor. Essas mudanças, por consequência, podem levar a alterações nas posições dos países (UIT, 2020)

A classificação dos países se dá a partir de 5 pilares e 20 indicadores, conforme quadro 1. As dimensões e indicadores elencados se baseiam na Agenda Global de Segurança Cibernética (GCA, do inglês *Global Cybersecurity Agenda*), lançada em 2007, pela União Internacional de Telecomunicações (UIT, 2020).

[55] Os países que não responderam ao questionário que gerou o relatório de 2020 foram: Estados Unidos, Canadá, Países Baixos, Noruega, Israel, Suíça, Nova Zelândia, América do Sul, Armênia, Burquina Fasso, Liechtenstein, Jamaica, Papua Nova Guiné, Madagascar, Síria, Nauru, Tonga, Iraque, Guiné, Camboja, Tadjiquistão, Congo, El Salvador, Seicheles, São Cristóvão e Neves, São Vicente e Granadinas, Santa Lúcia, Mali, Nicaragua, Tuvalu, Sudão do Sul, Ilhas Marshall, Timor-Leste, Comores, República Centro-Africana, Maldivas, Eritreia, Guiné Equatorial, República Popular Democrática da Coreia.

Quadro 1 - Pilares e indicadores do Global Cybersecurity Index

Pilares	Descrição	Indicadores
1) Medidas legais	"Medidas baseadas na existência de instituições e quadros jurídicos que tratam da segurança cibernética e do crime cibernético." (p. 131)	1.1. Legislação sobre crimes cibernéticos
		1.2. Regulamentação sobre segurança cibernética
2) Medidas técnicas	"Medidas baseadas na existência de instituições técnicas e quadros que tratam da segurança cibernética." (p.131)	2.1. CIRT/CSIRT/CERT Nacionais/Governamentais
		2.2. CIRT/CSIRT/CERT setoriais
		2.3. Quadro nacional para implementação de normas de cibersegurança
		2.4. Proteção infantil on-line
3) Medidas organizacionais	"Medidas baseadas na existência de instituições de coordenação de políticas e estratégias para o desenvolvimento da segurança cibernética a nível nacional." (p. 131)	3.1. Estratégia Nacional de Cibersegurança
		3.2. Agências de segurança cibernética
		3.3. Métricas de segurança cibernética
4) Medidas de desenvolvimento de capacidades	"Medidas baseadas na existência de programas de investigação e desenvolvimento, educação e formação, profissionais certificados e agências do sector público que promovem a capacitação." (p. 132)	4.1. Campanhas públicas de conscientização sobre segurança cibernética
		4.2. Formação para profissionais de segurança cibernética
		4.3. Programas educacionais e currículos acadêmicos sobre segurança cibernética
		4.4. Programas de pesquisa e desenvolvimento em segurança cibernética
		4.5. Indústria nacional de segurança cibernética
		4.6. Mecanismos de incentivo governamental
5) Medidas de cooperação	"Medidas baseadas na existência de parcerias, quadros cooperativos e redes de partilha de informação." (p. 132)	5.1. Acordos bilaterais sobre cooperação em segurança cibernética
		5.2. Participação governamental em mecanismos internacionais
		5.3. Acordos multilaterais de segurança cibernética
		5.4. Parcerias com o setor privado (PPPs)
		5.5. Parcerias entre agências

Fonte: elaboração própria, com base em UIT (2020), com tradução própria.

Este índice pontua os países de 0 a 100, cada pilar equivalendo 20 pontos e cada indicador com peso ponderado a partir da sua importância relativa no grupo. Esse peso ponderado é indicado por especialistas da academia, de *think tanks*, organizações e outros

organismos (UIT, 2020). Dessa forma, são atribuídos aos países seus níveis de capacitação nas cinco categorias, criando-se o ranking dos países considerados mais ou menos capacitados ou seguros ciberneticamente. Além disso, os relatórios publicados também trazem as classificações por regiões (África, América, Estados Árabes, Ásia-Pacífico e Europa), permitindo um olhar mais direcionado a partir das comparações regionais.

O relatório destaca que para promover o desenvolvimento, garantir a segurança e a resiliência das infraestruturas e sistemas, promover inovação, construir capacidades, é fundamental investir em pesquisa nacional e na capacitação dos recursos humanos em todos os níveis, promovendo programas educativos e formação específica, além de ser necessário também promover campanhas de conscientização. Em termos de medidas de cooperação, ressaltam a interconectividade e a transnacionalidade das ameaças para frisar a necessidade cada vez maior da colaboração entre os atores para enfrentar os diversos desafios da cibersegurança, sendo crucial, portanto, medidas de cooperação nacional, regional e internacional (ITU, 2020).

Para além disso, um quadro jurídico e regulamentar é fundamental para proteger a sociedade e promover um ambiente digital mais seguro e deve ser um passo inicial dos esforços nacionais, estabelecendo os comportamentos, os instrumentos processuais, os mecanismos e os procedimentos para garantir a segurança dos usuários desse ambiente. Já as medidas organizacionais observam as políticas e os mecanismos e instituições de governança nacional e coordenação entre os setores envolvidos na segurança cibernética. Por fim, as medidas técnicas avaliam, essencialmente as estruturas e mecanismos para lidar com os riscos e os incidentes (ITU, 2020). Esses pilares também dependem de conhecimentos e recursos humanos qualificados para atuar nos diversos setores e desenvolver as medidas necessárias ao bom funcionamento de todo o sistema nacional de segurança e defesa cibernética.

O *National Cyber Security Index (NCSI),* por outro lado, se destaca pela diferença, em relação aos demais mencionados, na definição e organização das dimensões e indicadores que utiliza para medir as capacidades de cibersegurança dos Estados. Visando medir a preparação dos Estados frente às ameaças cibernéticas e servir como ferramenta para direcionar a construção de capacidades nacionais, esse índice global, do *e-Governance*

Academy Foundation (eGA)[56], sediado em Tallin, na Estônia, faz a coleta, revisão e atualização dos dados em processo contínuo, não divulgando relatórios anuais sobre o ranking especificamente (NCSI, 2023). Portanto, fornece as informações em seu site, o qual permite visualizar os dados e, inclusive, fazer comparações entre os níveis de capacitação de cada um dos países disponíveis no banco de dados da plataforma. Ademais, o *Think Tank* também possui um repositório onde é possível encontrar outros relatórios e publicações de pesquisas realizadas e projetos finalizados e em curso.

Quanto à organização do Índice, este está estruturado em 12 dimensões de capacidades e 46 indicadores (conforme disposto no quadro 2). Cabe ressaltar que recentemente, em 2022, foi lançado o relatório "*Upgrading National Cyber Resilience*", o qual apresenta o NCSI 3.0, com atualizações em relação às dimensões e indicadores do Índice, mas que ainda não são visualizados nas pesquisas dos países apresentados no site do instituto.

> O NCSI 3.0 inclui novos indicadores de liderança política, compromisso com o direito internacional no ciberespaço e investigação e desenvolvimento em cibersegurança (pilar estratégico); cibersegurança dos serviços em nuvem e da cadeia de abastecimento, e coordenação da sensibilização para a cibersegurança (pilar preventivo); e ferramentas de notificação de incidentes cibernéticos, participação na cooperação internacional de resposta a incidentes, direito processual e doutrina cibernética militar (pilar responsivo). O NCSI 3.0 fundiu a proteção dos serviços digitais e essenciais numa única área de capacidade e fundiu ainda alguns indicadores para identidade eletrônica e serviços de confiança, ao mesmo tempo que omitiu indicadores relativos a organizações internacionais de cibersegurança hospedadas por países e à participação em exercícios cibernéticos (militares) internacionais. [...] O NCSI atualizado também inclui pontuações e pesos de indicadores revisados que refletem a importância do aspecto específico no sistema nacional de segurança cibernética.[57] (KASKA, 2022, p.12, tradução própria).

[56] O NCSI é um dos programas do *think tank* eGA. O eGA foi criado ainda em 2002, como uma iniciativa conjunta entre o Governo da Estônia, *Open Society Institute* e o Programa das Nações Unidas para o Desenvolvimento (PNUD), buscando auxiliar na transição digital do setor público e de organizações da sociedade civil, através de consultorias, treinamentos, parcerias e desenvolvimento de pesquisas (NCSI, 2023).

[57] "*NCSI 3.0 includes new indicators for political leadership, commitment to international law in cyberspace, and cybersecurity research and development (Strategic pillar); cybersecurity of cloud services and the supply chain, and cybersecurity awareness raising coordination (Preventive pillar); and cyber incident reporting tools, participation in international incident response cooperation, procedural law, and military cyber doctrine (Responsive pillar). The NCSI 3.0 has merged the protection of digital and essential services into a single capacity area and further merged some indicators for electronic identity and trust services, while omitting indicators concerning international cybersecurity organisations hosted by countries and participation in international (military) cyber exercises. [...] The updated NCSI also includes revised indicator scores and weights that reflect the significance of the particular aspect in the national cybersecurity system*." (KASKA, 2022, p.12).

Apesar dessas alterações, será utilizada aqui a estruturação disponível no site do NCSI, pois é a que permite realizar a comparação entre os países nos capítulos seguintes. Acrescenta-se, como pode ser observado a seguir, que as categorias ou dimensões expostas pelo NCSI são mais específicas, se comparadas aos demais índices. O quadro 2 apresenta a estrutura de dimensões e indicadores disponíveis no site do NCSI.

Quadro 2 - Capacidades e indicadores do National Cyber Security Index

Capacidades	Indicadores
1. Desenvolvimento de políticas de segurança cibernética	1.1. Unidade de política de segurança cibernética
	1.2. Formato de coordenação da política de segurança cibernética
	1.3. Estratégia de segurança cibernética
	1.4. Plano de implementação da estratégia de segurança cibernética
2. Análise e informações sobre ameaças cibernéticas	2.1. Unidade de análise de ameaças cibernéticas
	2.2. Relatórios públicos sobre ameaças cibernéticas são publicados anualmente
	2.3. Site de segurança cibernética e proteção
3. Educação e desenvolvimento profissional	3.1. Competências de segurança cibernética no ensino primário ou secundário
	3.2. Programa de segurança cibernética de nível de bacharelado
	3.3. Programa de segurança cibernética de nível de mestrado
	3.4. Programa de segurança cibernética em nível de doutorado
	3.5. Associação Profissional de Segurança Cibernética
4. Contribuição para a segurança cibernética global	4.1. Convenção sobre Crime Cibernético
	4.2. Representação em formatos de cooperação internacional
	4.3. Organização internacional de segurança cibernética sediada pelo país
	4.4 Capacitação em segurança cibernética para outros países
5. Proteção de serviços digitais	5.1. Responsabilidade de segurança cibernética para provedores de serviços digitais
	5.2. Padrão de segurança cibernética para o setor público
	5.3. Autoridade de supervisão competente
6. Proteção de serviços essenciais	6.1. Operadores de serviços essenciais são identificados
	6.2. Requisitos de segurança cibernética para operadores de serviços essenciais
	6.3. Autoridade de supervisão competente
	6.4. Monitoramento regular das medidas de segurança
7. Identificação eletrônica e serviços de confiança	7.1. Identificador persistente exclusivo
	7.2. Requisitos para criptosistemas
	7.3. Identificação eletrônica
	7.4. Assinatura Eletrônica
	7.5. Carimbo de data/hora
	7.6. Serviço de entrega registrada eletrônica
	7.7. Autoridade de supervisão competente
8. Proteção de dados pessoais	8.1. Legislação de proteção de dados pessoais
	8.2. Autoridade de proteção de dados pessoais
9. Resposta a incidentes cibernéticos	9.1. Unidade de resposta a incidentes cibernéticos
	9.2. Responsabilidade de reporte
	9.3. Ponto de contato único para coordenação internacional

[continua...]

[continuação]

10. Gerenciamento de crises cibernéticas	10.1. Plano de gestão de crises cibernéticas
	10.2. Exercício de gestão de crises cibernéticas a nível nacional
	10.3. Participação em exercícios internacionais de crise cibernética
	10.4. Apoio operacional de voluntários em crises cibernéticas
11. Luta contra o crime cibernético	11.1. Crimes cibernéticos são criminalizados
	11.2. Unidade de crimes cibernéticos
	11.3. Unidade forense digital
	11.4. Ponto de contato 24/7 (24 horas por dia, 7 dias por semana) para crimes cibernéticos internacionais
12. Operações cibernéticas militares	12.1. Unidade de operações cibernéticas
	12.2. Exercício de operações cibernéticas
	12.3. Participação em exercícios cibernéticos internacionais

Fonte: elaboração própria com base em NSCI (2023), com tradução própria.

Cada indicador possui uma pontuação, definida a partir da importância deste no índice geral. Os valores são atribuídos pelo grupo de peritos de acordo com a seguinte consideração: 1 ponto – um ato jurídico que regula uma área específica; 2–3 pontos, uma unidade especializada; 2 pontos, um formato oficial de cooperação; 1–3 pontos, um resultado/produto. A atribuição dessas pontuações poderá ser observada mais claramente na análise individualizada dos países.

O NCSI realiza as classificações dos países a partir de dados públicos, disponíveis em legislações, documentos e site oficiais. Sobre a coleta de dados, afirmam que estes podem ser fornecidos por funcionários dos governos, por organizações ou especialistas, ou recolhidos pela própria equipe responsável pelo NCSI a partir dos dados públicos. Busca-se dados mensuráveis como os atos jurídicos implementados pelos governos, as instituições criadas, os comitês, grupos de trabalho e projetos de cooperação em desenvolvimento, e demais resultados como programas, exercícios, tecnologias, etc. Com o recolhimento dos dados, estes são revisados por pelo menos dois especialistas do NCSI e, então, são publicados. A classificação dos países se dá pela porcentagem atribuída em relação a pontuação total dos indicadores (NCSI, 2023).

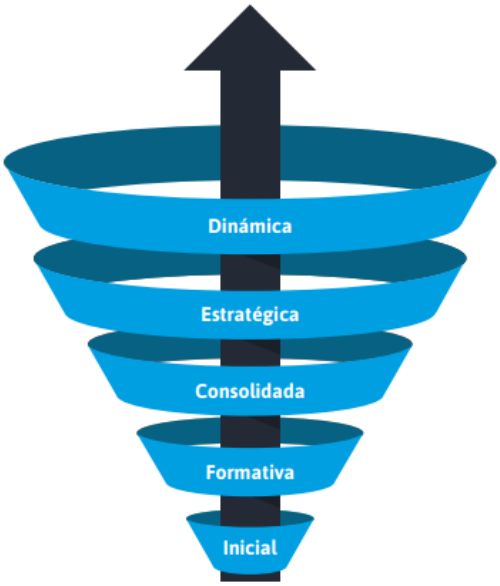
Por fim, cita-se o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (CCMM), desenvolvido *Global Cyber Security Capacity Centre* (GCSCC) da Universidade de Oxford. O trabalho do GCSCC concentra-se no desenvolvimento, implantação e manutenção de uma estrutura em relação à construção de capacidades cibernéticas, buscando entender o que funciona, o que não funciona e por quê. Nesse sentido, pretende fornecer uma base sólida para revisões que podem levar a recomendações sobre políticas e práticas no setor (GCSCC, 2023). Para além disso, ressaltam que:

> Se não garantirmos que a capacidade de segurança cibernética existe em todo o ciberespaço global, inevitavelmente desenvolveremos ciberguetos, locais onde os danos prevalecem e onde os ataques podem ser implantados com sucesso e de onde podem ser lançados com facilidade. Em última análise, a falta de progresso na capacidade de segurança cibernética pode resultar em danos à prosperidade e ao bem-estar dessas economias e nações tão dependentes do ciberespaço – cada vez mais a grande maioria da humanidade.[58] (GCSCC, 2023, s. p., tradução própria).

O modelo estabelece 5 níveis da maturidade cibernética: Inicial, Formativa, Consolidada, Estratégica e Dinâmica. A fase Inicial indica que não existe uma maturidade em matéria de cibersegurança ou que esta está em fase muito embrionária, podendo haver algumas discussões a respeito, mas sem medidas concretas sendo tomadas. A Formativa indica que iniciativas começaram a ser tomadas, mas estas ainda são pontuais, desorganizadas, mal definidas ou ainda muito recentes para serem avaliadas concretamente. Já a Consolidada demonstra que os indicadores avaliados já estão em funcionamento e com evidências de que estão funcionando; contudo, a alocação de recursos ainda é insuficiente, sendo necessário maior comprometimento com o setor. O estágio Estratégico aponta para a importância dada pelo país ao setor, indica que foram feitas escolhas sobre quais aspectos são mais relevantes levando em conta as circunstâncias particulares da nação em questão. Por fim, na fase Dinâmica revela que existem claros mecanismos implementados, sofisticação tecnológica, rápida tomada de decisão, alocação de recursos de forma eficiente, atenção constante ao ambiente e às suas mudanças, bem como percebe-se uma liderança global no setor (GCSCC, 2021).

[58] "*If we do not ensure that cybersecurity capacity exists across the global entirety of cyberspace, we will inevitably develop cyber ghettos, places where harm is prevalent and where attacks can be successfully deployed, and also from where they can be easily launched. Ultimately, a lack of progress on cybersecurity capacity could result in harms to the prosperity and the well-being of those economies and nations so dependent on cyberspace – increasingly the vast majority of humanity*." (GCSCC, 2023, s. p.)

Figura 5 - Os cinco estágios da maturidade da capacidade de segurança cibernética, segundo o CCMM



Fonte: BID; OEA (2020, p. 42).

Os níveis de maturidade são obtidos através da análise de 5 dimensões, as quais são subdivididas em alguns componentes mais específicos, apresentados no quadro 3. Importa mencionar que o relatório disponibilizado pelo Centro detalha cada uma das dimensões e do que eles denominam como fatores, aspectos e indicadores de cada dimensão, explicando o que é necessário para que determinado nível seja atribuído aos países em cada um dos componentes apresentados.

Quadro 3 - Dimensões e fatores do Modelo de Maturidade da Capacidade Cibernética

Dimensão	Descrição	Fatores
1. Políticas e estratégias de cibersegurança	"explora a capacidade do país de desenvolver e fornecer estratégia de segurança cibernética e aumentar sua resiliência de segurança cibernética, melhorando suas capacidades de resposta a incidentes, defesa cibernética e proteção de infraestrutura crítica (CI)."	1.1. Estratégia Nacional de Segurança Cibernética
		1.2. Resposta a incidentes e Gerenciamento de crise
		1.3. Proteção de Infraestrutura Crítica (IC)
		1.4. Defesa cibernética e Segurança Nacional
2. Cultura cibernética e sociedade	"analisa elementos importantes de uma cultura de segurança cibernética responsável, como a compreensão dos riscos cibernéticos na sociedade, o nível de confiança nos serviços de Internet, governo eletrônico e serviços de comércio eletrônico e a compreensão dos usuários sobre a proteção de informações pessoais online. [...] explora a existência de mecanismos de denúncia que funcionam como canais para que os usuários denunciem crimes cibernéticos. [...] analisa o papel da mídia e das mídias sociais na formação de valores, atitudes e comportamentos de segurança cibernética."	2.1. Mentalidade de segurança cibernética
		2.2. Confiança e segurança em serviços online
		2.3. Compreensão do usuário sobre proteção de informações pessoais online
		2.4. Mecanismos de denúncia
		2.5. Mídias e redes sociais
3. Conhecimento e capacitação	"analisa a disponibilidade, qualidade e aceitação de programas para vários grupos de partes interessadas, incluindo o governo, setor privado e a população como um todo, e se relaciona com programas de conscientização sobre segurança cibernética, programas formais de educação em segurança cibernética e programas de treinamento profissional."	3.1. Conscientização sobre segurança cibernética
		3.2. Educação cibernética
		3.3. Formação Profissional em Cibersegurança
		3.4. Pesquisa e inovação em segurança cibernética
4. Marcos legais e regulatórios	"examina a capacidade do governo de elaborar e promulgar legislação nacional direta e indiretamente relacionada à segurança cibernética, com ênfase particular nos tópicos de requisitos regulatórios para segurança cibernética, legislação relacionada ao crime cibernético e legislação relacionada. A capacidade de fazer cumprir essas leis é examinada por meio de aplicação da lei, acusação, órgãos reguladores e capacidades judiciais. [...] observa questões como estruturas formais e informais de cooperação para combater o cibercrime."	4.1. Disposições Legais e Regulatórias
		4.2. Quadro Legislativo Relacionado
		4.3. Capacidades Legais e Regulatórias
		4.4. Estruturas de cooperação formal e informal para combater o cibercrime
5. Padrões e tecnologias	"aborda o uso eficaz e generalizado da tecnologia de segurança cibernética para proteger indivíduos, organizações e infraestrutura nacional. [...] examina especificamente a implementação de padrões e boas práticas de segurança cibernética, a implantação de processos e controles e o desenvolvimento de tecnologias e produtos para reduzir os riscos de segurança cibernética."	5.1. Aderência aos Padrões
		5.2. Controles de segurança
		5.3. Qualidade de software
		5.4. Resiliência de infraestrutura de comunicações e Internet
		5.5. Mercado de segurança cibernética
		5.6. Divulgação responsável

Fonte: elaboração própria, a partir do disponível no site do GCSCC (2023), com tradução própria.

O modelo desenvolvido pelo GCSCC, publicado pela primeira vez em 2014, foi um dos primeiros a apresentar o que seria necessário para os Estados alcançarem os diferentes níveis de capacitação cibernética (CREESE et al., 2021). Este modelo é utilizado como base para diversas pesquisas sobre capacitação cibernética dos Estados e é, inclusive, base para o relatório sobre cibersegurança na América Latina e o Caribe, construído pelo Observatório de Cibersegurança da OEA. A aplicação do modelo nos países latino-americanos foi conduzida pela OEA em colaboração com a Universidade de Oxford. A análise foi feita por meio de um questionário online com uma versão adaptada do CCMM, de modo a se adequar ao contexto regional. Além disso, a aplicação envolveu a realização de workshops para explicação o CCMM aos países, como forma de obter dados mais precisos (CREESE et al., 2021).

> A ferramenta on-line fornecia perguntas a serem respondidas pelos Estados membros da OEA, solicitando ao seu ponto de contato nacional em cada país que distribuísse a pesquisa a especialistas nacionais relevantes com conhecimento para fornecer as informações mais confiáveis sobre segurança cibernética no país, como referências em apoio da sua resposta (incluindo links para websites e documentos). Participaram vários especialistas e funcionários com conhecimentos em cada país, mas o questionário era um questionário de apuramento de factos e não uma amostra de inquérito de opinião. A equipe da OEA revisou as respostas coletadas e recorreu a especialistas na área para pesquisar e completar quaisquer valores incertos ou ausentes nos dados fornecidos. As pontuações geradas foram então enviadas a cada Estado membro para validação adicional e os resultados foram publicados pelo BID e pela OEA e usados para análise da preparação para segurança cibernética.[59] (CREESE et al., 2021, p. 8, tradução própria).

Antes de encerrar a discussão proposta nesta seção, considera-se importante mencionar as contribuições sobre construção de capacidades feitas pelo *Global Forum on Cyber Expertise* (GFCE), uma plataforma de cooperação e governança estabelecida em 2015. O Fórum, diferentemente das demais instituições apresentadas, não cria uma sistemática para classificação dos países em relação às suas capacidades cibernéticas. Seu objetivo central é a troca de conhecimentos e o desenvolvimento de iniciativas visando a construção de capacidades cibernéticas. Ele conta com a parceria de países, organizações internacionais,

[59] "*The online tool provided questions to be completed by OAS member states, asking their national point of contact in each country to distribute the survey to relevant national experts with the knowledge to provide the most reliable information about cybersecurity in the country, such as references in support of their response (including links to websites and documents). Multiple experts and knowledgeable officials in each country participated, but the questionnaire was a fact-finding questionnaire rather than a sample survey of opinion. The OAS team reviewed the responses that were collected and used domain experts to research and complete any uncertain or missing values from the data provided. The generated scores were then sent to each member state for further validation, and the results were published by the IDB and OAS and used for analysis of cybersecurity preparedness*." (CREESE et al., 2021, p. 8)

organizações não governamentais (ONGs), empresas privadas e comunidade acadêmica e técnica (PAWLAK; BARMPALIOU, 2017).

Em 24 de novembro de 2017, divulgaram o Comunicado de Delhi sobre uma Agenda Global da GFCE para a Construção de Capacidade Cibernética, no qual estabeleceram o que consideram pontos de referências para os Estados ou organizações alcançarem o nível desejado de segurança e resiliência cibernética. O quadro a seguir reproduz as informações apresentadas no referido documento.

Quadro 4 - Agenda Global GFCE para Capacitação Cibernética

Tema 1. Política e Estratégia de Segurança Cibernética:

a. Buscar o compromisso de políticas em nível nacional com a segurança cibernética que impulsionam o planejamento estratégico, recursos e implementação.

b. Avaliar as práticas, ameaças e vulnerabilidades nacionais atuais e desenvolver, implementar e evoluir ao longo do tempo, conforme necessário, uma estratégia nacional abrangente de segurança cibernética que considere como essas questões afetam todas as partes interessadas e suas respectivas funções no processo.

Tema 2. Gerenciamento de Incidentes Cibernéticos e Proteção de Infraestrutura Crítica:

a. Desenvolver um sistema nacional de resposta a incidentes para prevenir, detectar, impedir, responder e se recuperar de incidentes cibernéticos.

b. Desenvolver, testar e exercitar planos e procedimentos de resposta a emergências, nacional e internacionalmente, para aumentar a conscientização e garantir que os colaboradores governamentais e não governamentais possam construir confiança, se preparar, coordenar de forma eficaz e lidar com crises.

c. Identificar e proteger os setores de infraestrutura de informação crítica nacional.

Tema 3. Cibercrime:

a. Promulgar e fazer cumprir um conjunto abrangente de leis, diretrizes, políticas e programas relacionados ao cibercrime, de acordo com os padrões internacionais existentes que permitem uma cooperação internacional eficaz, como a Convenção de Budapeste sobre o cibercrime.

b. Modernizar e fortalecer os sistemas internos de justiça criminal para lidar com crimes cibernéticos e crimes envolvendo provas eletrônicas, incluindo a prevenção, detecção, investigação, repressão e julgamento eficazes de tais crimes em todas as suas formas.

Tema 4. Cultura e habilidades de segurança cibernética:

a. Promover a conscientização abrangente de todas as partes interessadas sobre ameaças e vulnerabilidades cibernéticas e capacitá-las com conhecimento, habilidades e senso de responsabilidade compartilhada para praticar comportamentos seguros e informados no uso das TICs.

b. Envolver todas as partes interessadas para criar uma força de trabalho com um conjunto de habilidades de segurança cibernética e conhecimentos exigidos pelos empregadores.

Tema 5. Padrões de Segurança Cibernética:

a. Promover o desenvolvimento e uso de padrões de segurança cibernética globalmente relevantes que são desenvolvidos de forma consensual em órgãos transparentes e abertos à participação de todas as partes interessadas e que permitem alcançar abordagens baseadas em risco para a segurança cibernética.

Fonte: adaptado de GFCE (2017, p. 3), com tradução própria.

Entre as atividades desenvolvidas pelo Fórum está a criação e administração do Cybil Portal, um repositório online que apresenta e divulga projetos, programas, pesquisas e eventos na área, especialmente em relação ao tema da capacitação cibernética. O Portal conta com o suporte de outras organizações como o *Global Cyber Security Capacity Centre*, o *Australian Strategic Policy Institute*, o *Norwegian Institute of International Affairs* e outros (CYBIL PORTAL, 2023).

> É um local onde governos, financiadores e agências implementadoras podem encontrar e partilhar melhores práticas e informações práticas para apoiar a concepção e execução de projetos e atividades de capacitação. A Cybil também atua como fonte de informações sobre segurança cibernética e capacitação em crimes cibernéticos para a sociedade civil, a academia e a comunidade técnica, em linha com o compromisso do GFCE com a transparência e a inclusão. O objetivo geral da Cybil é estabelecer uma plataforma de compartilhamento de conhecimento multissetorial neutra, aberta e de propriedade global que permita: O compartilhamento de dados, informações e resultados dos esforços globais de capacitação cibernética; Garantir o acesso transparente a dados e informações sobre ferramentas de capacitação cibernética com uma interface de usuário simples; A integração dos recursos existentes e da informação que já está disponível; Uma utilização mais eficaz dos recursos de capacitação cibernética (CCB) para a programação de capacitação pela comunidade global da GFCE; A harmonização das iniciativas de reforço da capacidade cibernética e das abordagens de reforço da capacidade. (CYBIL PORTAL, 2023, s.p, tradução própria).

Em suma, percebe-se que tais centros de pesquisa compreendem e apresentam de forma distinta os pilares e/ou dimensões e indicadores que podem nortear a construção de capacidades cibernéticas dos países. Essa situação corrobora com a questão da falta de consenso em torno das conceituações dos termos que envolvem o ciberespaço, o que é ainda mais perceptível no que diz respeito às capacidades cibernéticas. Contudo, esse cenário não surpreende visto a complexidade do ciberespaço e as dificuldades que envolvem as análises que perpassam esse ambiente – como pode ser observado, inclusive, na seção anterior. Ademais, como pondera 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. Essa perspectiva ressalta a necessidade da agenda de pesquisa aqui defendida e implementada, ao buscar compreender o cenário sul-americano e, partir disso, adentrar a investigação em países específicos da região, como caminho para discutir a construção de capacidades cibernéticas.

Ainda, somando às diferentes definições adotadas, as distintas metodologias para coleta e sistematização dos dados dos países analisados, assim como a falta de transparência e de confiança dos Estados para divulgar as suas informações sobre a temática, acabam por

resultar em posições consideravelmente diferentes entre as nações em tais classificações realizadas. Isso, contudo, não anula o extenso trabalho e as contribuições cruciais de tais institutos e centros de pesquisa na compreensão do atual cenário de capacitação cibernética. Inclusive, tais índices são utilizados em diversas pesquisas ao redor do mundo, como conceituadas bases de dados que são.

Dito isso, considera-se que o esforço empreendido por esses centros de pesquisa – assim como demais estudos que vem sendo realizadas no campo - pode auxiliar os Estados na compreensão de suas lacunas e orientar suas políticas e estratégias para construção de capacidades, bem como nortear a alocação de recursos para os setores que precisariam de maior atenção. Novamente constata-se a importância da nítida identificação dessas áreas para os países do Sul Global, que possuem limitados recursos e, portanto, necessitam de planos de ação direcionados que possam gerar os melhores resultados.

Por fim, embora haja diferenças na compreensão sobre as dimensões e indicadores apresentados pelos centros de pesquisa, percebe-se o consenso de que a construção de capacidades vai muito além de competências técnicas. Pode-se constatar que os índices coincidem ao abranger ampla gama de questões, envolvendo temas de segurança nacional, política externa, segurança pública e políticas públicas. Os tópicos propostos incluem a estratégia e a política de segurança cibernética, adequação dos quadros jurídicos e regulamentares, a estrutura institucional e organizacional, as medidas de cooperação e construção de parcerias, os níveis de conhecimento e treinamento, e as inovações científicas e tecnológicas. Isso se dá justamente pela diversificação de componentes envolvidos na construção de capacidades cibernéticas. Adicionalmente, apesar de os modelos serem formados por pilares ou dimensões separadas, estas são estreitamente relacionadas entre si, formando, juntas uma base sólida para a construção de capacidades cibernéticas ao serem implementadas a partir de uma ampla e concisa estratégia estatal.

Diante disso, a partir do apresentado, os dados obtidos por esses centros de pesquisa serão utilizados no terceiro capítulo desta tese, como forma de analisar a posição que os países sul-americanos e, particularmente, dos três países elegidos para uma investigação mais aprofundada. Justamente pelas diferentes metodologias e resultados, optou-se por utilizar três índices nas análises conduzidas no último capítulo desta tese, as quais, acredita-se, pode serem observadas a partir de uma perspectiva de complementariedade.

2.3 CONSIDERAÇÕES PARCIAIS

A construção de capacidades cibernéticas é um campo dinâmico, no qual os múltiplos contextos e realidades sociais, econômicas e políticas dos países devem ser observados. Portanto, não pode ser resumida apenas a um desenvolvimento tecnológico, é um processo muito mais profundo e abrangente. Este deve ser sustentado por políticas e estratégias coesas, devem envolver ampla gama de setores, criando incentivos e parcerias com o setor privado e a academia, fundamentando-se na formação, na educação e no treinamento do capital humano, bem como no investimento em ciência e pesquisa nacional. Nesse sentido, deve envolver capacidades institucionais, organizacionais, políticas, legais e diplomáticas. Tudo isso preservando a população e protegendo seus direitos fundamentais.

Partindo dos elementos examinados neste capítulo, pode-se compreender que a construção de capacidades cibernéticas é fundamental para garantir a segurança, a defesa e a resiliência dos Estados diante de tantas ameaças que se originam nesse ambiente, bem como é base para a obtenção de maior poder e controle no século XXI. Compreender as capacidades cibernéticas de um país perpassa a investigação sobre indicadores de investimentos no setor em si e nas demais áreas que sustentam o desenvolvimento e a proteção do ciberespaço, nas suas estruturas institucionais, na amplitude e a precisão das legislações existentes, na coerência das suas políticas e estratégias para o setor e nos mecanismos e processos desenvolvidos para a segurança e a defesa. Envolve também as capacidades diplomáticas, demonstrando a atuação no país nos diversos fóruns e organizações que discutem as temáticas, a cooperação entre os setores e instituições nacionais, garantindo a integração dos conhecimentos e, principalmente, o investimento no desenvolvimento de pesquisa, ciência e tecnologias nacionais e na capacitação dos recursos humanos, sendo esses considerados a base de todas as dinâmicas cibernéticas.

Observa-se que muitos dos componentes para a construção de capacidades não trazem resultados imediatos, podendo levar tempo considerável para gerarem resultados concretos. Ou seja, a construção de capacidades cibernéticas é um processo de longo prazo que deve tomar forma em camadas e ser sustentada no tempo, inclusive com iniciativas basilares de educação cibernética. Para mais, a estabilidade do Estado e o desenvolvimento de políticas de Estado, não de governo, tornam-se ainda mais cruciais.

Diante das particularidades das dinâmicas que envolvem o ciberespaço e da complexidade que envolve a construção de capacidades cibernéticas emana a importância de

uma ampla estratégia para o setor. Assim, ressalta-se a necessidade de propor alternativas para a construção de capacidades cibernéticas que ultrapassem a lógica militarizada, atentando que a era digital demanda respostas diferenciadas (GADY; AUSTIN, 2010; CALDERARO; CRAIG, 2020). Diante disso, destacam-se visões que apontam para dinâmicas cooperativas, o desenvolvimento da diplomacia cibernética, a construção da confiança entre os atores, o estabelecimento de acordos bilaterais e multilaterais e de ações coordenadas entre atores estatais, não estatais e os diversos setores da sociedade (MULLER, 2015; PAWLAK, 2016; BARRINHA; RENARD, 2017; PAWLAK; BARMPALIOU, 2017; SCHIA, 2018; HERZ, 2019; CALDERARO; CRAIG, 2020).

Como já ressaltado, essa pesquisa se direciona por essa perspectiva, que tem especial relevância para os países do Sul Global devido ao cenário particular enfrentado por esse grupo de países. Assim, medidas de cooperação poderia ser a chave na busca por superar as lacunas tecnológicas e de infraestrutura ou para o estabelecimento de programas de trocas de experiências e informações, treinamento e formação de recursos humanos ou, ainda, para fazer frente e aumentar o poder de influência desse grupo de países no cenário da governança cibernética internacional. Partindo disso, o capítulo seguinte tem por intenção apresentar e analisar as discussões que têm tomado forma acerca da cooperação cibernética, da diplomacia cibernética e sobre os processos de governança cibernética internacional. A partir disso, o estudo se deterá nas análises em relação ao entorno sul-americano.

3 DIPLOMACIA E COOPERAÇÃO CIBERNÉTICA: A AMÉRICA DO SUL FRENTE AOS NOVOS DESAFIOS DO CIBERESPAÇO NA POLÍTICA INTERNACIONAL

Até esse momento, discutiu-se aspectos considerados mais tradicionais nos estudos sobre geopolítica e cibernética e as discussões acerca das diversas ameaças à segurança dos Estados diante da evolução tecnológica e as relações de poder no ciberespaço. Entretanto, os estudos geopolíticos também perpassam as iniciativas de cooperação, regionalismos, alianças, parcerias estratégicas e processos de integração.

No capítulo anterior pode-se observar que países em desenvolvimento enfrentam diversas dificuldades para a construção de capacidades e para desenvolver poder nessa esfera, principalmente levando em consideração os empecilhos que enfrentam no desenvolvimento científico e tecnológico e suas reduzidas capacidades de negociação nos fóruns e organismos internacionais. Essa situação frequentemente os deixa a margem dos processos de governança cibernética ou sem ter uma participação ativa nas tomadas de decisão sobre questões envolvendo a temática cibernética. Ademais, esses países se encontram em situação de grande dependência em relação ao Norte Global e às potências cibernéticas, o que acentua suas vulnerabilidades no setor.

Diante disso, vem tomando forma estudos que enfatizam alternativas cooperativas, visando fortalecer medidas de confiança entre os atores[60], o estabelecimento de acordos bilaterais e multilaterais no setor, o desenvolvimento da diplomacia cibernética em busca de uma efetiva governança internacional que assegure estabilidade e melhores níveis de segurança internacional. Algumas dessas perspectivas têm se debruçado em compreender as possibilidades de construção de parcerias e processos cooperativos entre os países em

[60] Desenvolver processos cooperativos em temas sensíveis para a segurança e para a defesa dos Estados é um desafio nas relações internacionais. Quando se trata de compartilhamento tecnológico, e de capacidades de modo geral, os Estados deparam-se com desconfianças e incertezas sobre as reais intenções dos parceiros internacionais. Nessa perspectiva, a construção de medidas de confiança entre os atores torna-se central para avançar para processos cooperativos mais amplos. Cabe destacar que, segundo Pagliari e Viggiano (2020), medidas de construção e fortalecimento de confiança são iniciativas que visam aumentar a transparência sobre dados, políticas e planejamento estratégico visando possibilitar a consolidação de processos de cooperação e integração e a formação de parcerias e alianças, além de evitar a eclosão de conflitos. Conforme as autoras, "a construção da confiança [...] não implica necessariamente em compartilhar todo o tipo de informação disponível acerca dos assuntos militares (em especial, acerca das capacidades), mas deve atender a demandas específicas dos atores envolvidos, e que represente o que consideram necessário que seja informado ou compartilhado para o fomento da confiança." (PAGLIARI; VIGGIANO, 2020, p. 48).

desenvolvimento, justamente por levar em consideração as disparidades entre os Estados do Norte e do Sul Geopolítico e a grande dependência desses últimos.

Desse modo, o presente capítulo recorrerá a alguns desses estudos para expor a perspectiva adotada nesta pesquisa, apresentando também algumas iniciativas de cooperação internacional na área cibernética. Após, será dada ênfase à América do Sul, objeto desta pesquisa, para compreender o cenário no qual se encontram os países da região e analisar as iniciativas de cooperação multilateral construídas nos últimos 15 anos, a partir da criação da Unasul (2008), uma instituição considerada um marco no cenário sul-americano, por reunir 12 países sul-americanos para dialogar, coordenar ações e cooperar em diversas áreas, inclusive na temática de defesa cibernética.

3.1 COOPERAÇÃO E DIPLOMACIA CIBERNÉTICA: NOVAS PERSPECTIVAS PARA A SEGURANÇA E A CONSTRUÇÃO DE CAPACIDADES

Pelos altos níveis de conectividade internacional do ciberespaço e devido a característica transfronteiriça e transversal desse ambiente, entende-se como fundamental pensar em novas abordagens para a segurança e a defesa cibernética. Diante disso, um dos caminhos para superar os diversos desafios que imperam nessa esfera é justamente deixar de focar excessivamente em termos de conflitos cibernéticos, desenvolver medidas de confiança e fortalecer o campo da diplomacia cibernética (GADY; AUSTIN, 2010; BARRINHA; RENARD, 2017; HOMBURGER, 2019).

Em consonância, Herczynski (2020, p. 26, tradução própria), Diretor Administrativo da PCSD (Política Comum de Segurança e Defesa)[61] e Resposta à Crise do Serviço Europeu de Ação Externa, afirma que "dada a natureza global da ameaça, construir e preservar fortes alianças e parcerias com terceiros países é essencial para a prevenção e dissuasão de ataques cibernéticos, que são cada vez mais críticos para a estabilidade e segurança internacionais."

Conforme Barrinha e Renard (2017, p. 361, tradução própria), "a ciberdiplomacia é para o ciberespaço o que a diplomacia é para as relações internacionais: um pilar fundamental

[61] A PCSD faz parte da Política Externa e de Segurança Comum (PESC) da União Europeia. Trata-se do "principal quadro político através do qual os Estados-Membros podem desenvolver uma cultura estratégica europeia de segurança e defesa, enfrentar conflitos e crises em conjunto, proteger a União e os seus cidadãos e reforçar a paz e a segurança internacionais." (PARLAMENTO EUROPEU, 2023, s. p.)

da sociedade internacional"[62]. Ainda assim, poucos governos vêm pensando sobre a dimensão diplomática da segurança cibernética e, certamente, muito menos vêm desenvolvendo estratégicas nesse âmbito diante das crescentes ameaças cibernéticas que os Estados têm enfrentado. A literatura sobre o tema também é ainda consideravelmente limitada (BARRINHA; RENARD, 2017).

A ciberdiplomacia, ou diplomacia cibernética, pode ser definida como "o uso de recursos diplomáticos e o desempenho de funções diplomáticas para assegurar os interesses nacionais no que diz respeito ao ciberespaço"[63], incluindo em sua agenda a segurança cibernética, crimes cibernéticos, construção de confiança e capacidades, liberdade e governança da Internet (BARRINHA; RENARD, 2017, p. 355). A ciberdiplomacia seria conduzia em todo, ou parte, por diplomatas em espaços de diálogo bilaterais ou multilaterais, interagindo não apenas com atores estatais, mas também com os principais agentes envolvidos no setor, líderes de empresas de Internet (como Facebook, Microsoft e Google), empresários de tecnologia ou organizações da sociedade civil (BARRINHA; RENARD, 2017).

Não se pode, entretanto, confundi-la com a diplomacia digital ou e-diplomacia, a qual se refere ao uso de novas tecnologias e mídias sociais por Chefes de Estado, Chefes de Governo, Ministros e Diplomatas, no contexto de suas atividades tradicionais no âmbito da política externa (BARRINHA; RENARD, 2017).

> [...] as relações cibernéticas internacionais e a governança do ciberespaço são extremamente complexas e frágeis, mas ao mesmo tempo tornam a diplomacia ainda mais necessária, especialmente no que diz respeito (mas não se limitando) aos mecanismos de construção de confiança e ao desenvolvimento de normas internacionais e valores.[64] (BARRINHA; RENARD, 2017, p. 357, tradução própria).

A diplomacia é crucial para que se formem os canais de comunicação necessários entre os Estados, assim como entre os Estados e organizações internacionais, sociedade civil e demais atores não estatais dentro dessa esfera externa. Essa comunicação também é importante para que os Estados estabeleçam parcerias e coordenem sua atuação visando defender suas posições e atender seus interesses. Tendo em vista as aceleradas mudanças, as

---

[62] "[...] *cyber-diplomacy is to cyberspace what diplomacy is to IR: a fundamental pillar of international society*." (BARRINHA; RENARD, 2017, p. 361).
[63] "[...] *the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace*." (BARRINHA; RENARD, 2017, p. 355).
[64] "[…] *international cyber relations and the governance of the cyberspace extremely complex and fragile, but at the same time make diplomacy all the more necessary, particularly with regard (but not limited) to confidence-building mechanisms and the development of international norms and values."* (BARRINHA; RENARD, 2017, p. 357).

visões divergentes e em disputa no processo de construção de governança cibernética internacional, a diplomacia cibernética torna-se basilar para acompanhar e participar ativamente das conversações (BARRINHA; RENARD, 2020).

A China, por exemplo, vem adotando uma diplomacia cibernética mais ativa, apresentando em seus documentos oficiais sobre cibernética diversos pontos sobre sua atuação internacional nesse setor. O país defende a reforma do atual sistema de governança cibernética, baseando-se no diálogo, na cooperação, troca de informações e advoga pelo direito de todos os Estados participarem da construção de uma governança cibernética global e justa. Pleiteia por um modelo de governança cibernética estatal, estando a soberania cibernética entre os elementos centrais da sua proposta e reforça a premissa da não interferência nos assuntos e na organização interna dos países. Em 2017, o país lançou sua Estratégia Internacional para Cooperação no Ciberespaço, importante documento sobre sua ciberdiplomacia, no qual reforça os elementos citados acima e se compromete na construção de uma comunidade internacional no ciberespaço, em promover medidas de construção de confiança e de promoção da paz (BRITO; CASTRO, 2021).

Nessa direção, em 2021, os Estados Unidos divulgaram o *Cyber Diplomacy Act*, propondo o desenvolvimento de uma fundamentada e organizada política para ser implementada na diplomacia cibernética do país, visando fortalecer sua liderança no mundo digital e nos processos de governança cibernética, na proposição de normas, valores e padrões do ciberespaço. O país advoga na direção de promover "uma Internet aberta, interoperável, confiável, sem restrições e segura, regida pelo modelo multissetorial"[65] (U.S., 2021, p. 8, tradução própria).

O documento propõe implementar a política descrita através do diálogo, bilateral e multilateral, com atores externos, incluindo empresas do setor privado, ONGs, acadêmicos e outras partes interessadas. O documento lista uma variedade de questões a serem endereçadas pelo país nessa esfera, entre elas: acesso e a liberdade na Internet, a liberdade de expressão e a privacidade, respeito aos direitos humanos e proteção da democracia, economia digital, crimes cibernéticos, dissuasão e respostas internacionais a ameaças cibernéticas (U.S., 2021).

Ainda propõe a criação de um Escritório de Política Internacional do Ciberespaço (*Bureau of International Cyberspace Policy*), no âmbito do Departamento do Estado, chefiado

[65] […] "*an open, interoperable, reliable, unfettered, and secure Internet governed by the multi-stakeholder model* […] (U.S., 2021, p. 8)

por um oficial com posto de embaixador, o qual deverá ter competências nas áreas de cibersegurança e diplomacia internacional (U.S., 2021). Uma lista de responsabilidades está associada a esse diplomata, entre as quais:

I) Representar, orientar e liderar os esforços diplomáticos norte-americanos nesse setor;

II) Atuar como um elo entre a sociedade civil, setor privado, academia e outras entidades públicas e privadas em questões relevantes do ciberespaço internacional;

III) Desenvolver e executar estratégias para influenciar os tomadores de decisão, em coordenação com outras agências governamentais;

IV) Promover a construção de capacidades cibernética estrangeiras, baseando-se nas prioridades da política cibernética;

V) Promover um ambiente regulatório internacional para as tecnologias relacionadas ao setor que beneficiam os interesses econômicos e securitários estadunidenses (U.S., 2021).

Pawlak e Barmpaliou (2017, p. 6, tradução própria) defendem que:

> Uma abordagem abrangente à ciberdiplomacia abrange uma vasta gama de questões como a promoção e proteção dos direitos humanos online, o reforço do modelo multilateral de governação da Internet, a prevenção de conflitos no ciberespaço e a garantia de maior estabilidade com instrumentos diplomáticos e jurídicos, bem como como a salvaguarda do acesso aberto à Internet como meio de permitir aos cidadãos desfrutarem plenamente dos benefícios sociais, culturais e econômicos do ciberespaço.[66]

A ciberdiplomacia é fundamental para que se possa estabelecer vocabulário e definições conceituais comuns, bem como o desenvolver normas, valores e padrões de comportamento internacionais no âmbito cibernético (MEYER, 2012; BARRINHA; RENARD, 2020). Essa via tem particular importância se levarmos em consideração a ainda incipiente formulação e aplicação do direito internacional nas dinâmicas cibernéticas (GADY; AUSTIN, 2010; MEYER, 2012; AYRES PINTO; GRASSI, 2020; BARRINHA; RENARD, 2020). Esses passos parecem necessários para a construção de confiança e da estabilidade da ordem cibernética internacional, visto as diferentes visões, preferências e definições dos Estados e o uso dos termos de forma a atender seus interesses particulares dos Estados.

---

[66] "*A comprehensive approach to cyber diplomacy embraces a broad range of issues such as promotion and protection of human rights online, strengthening the multi-stakeholder model of internet governance, the prevention of conflict in cyberspace and ensuring greater stability with diplomatic and legal instruments, as well as safeguarding the open access to internet as a means of enabling citizens to thoroughly enjoy the social, cultural and economic benefits of cyberspace*." (PAWLAK; BARMPALIOU, 2017, p. 6)

Diante disso, ao longo dos anos tem-se buscado desenvolver mecanismos de governança cibernética, visando lidar com as mudanças constantes lideradas pelas novas tecnologias, superar lacunas institucionais e normativas, fortalecer medidas de confiança e capacitação (HERZ, 2019). Sobre isso, destaca-se a atuação de atores em fóruns, convenções internacionais, organismos e organizações internacionais.

Em termos de cooperação internacional, a temática mais proeminente é a relativa aos cibercrimes, visto a formulação da Convenção de Budapeste, ou Convenção do Conselho da Europa sobre Cibercrime, firmada em 2001 e que entrou em vigor em 2004, sendo o único tratado vinculante sobre o tema até o momento. Entre os objetivos do tratado estão harmonizar as legislações internacionais sobre o tema, melhorar as técnicas de investigação e estabelecer medidas de cooperação e assistência mútua nos procedimentos relativos aos crimes cibernéticos (CONVENÇÃO DE BUDAPESTE, 2001).

Conforme Gady e Austin (2010, p. 13, tradução própria), o referido Tratado é único em vários aspectos.

> Pela primeira vez, uma convenção aborda atividades e práticas ilegais que surgem em um amplo espectro de ameaças à segurança cibernética. Em segundo lugar, é a primeira tentativa de estabelecer padrões e procedimentos comuns no ciberespaço que sejam juridicamente vinculativos para seus signatários. Em terceiro lugar, a convenção está aberta aos Estados membros do Conselho da Europa e outros, o que significa que pode se tornar um instrumento internacional aceito por mais de um grupo de países. (Por exemplo, os Estados Unidos a assinaram e ratificaram.) Por fim, e de forma mais controversa, a convenção introduz requisitos para o manuseio e acesso de dados, que deram origem a preocupações sobre direitos de privacidade e liberdades civis e, como no caso da Rússia, questões sobre a soberania do Estado.[67]

Dentre as iniciativas tomadas no âmbito das Nações Unidas, destaca-se o papel da União Internacional de Telecomunicações (UIT) e as reuniões do Grupo de Especialistas Governamentais da ONU sobre Comportamento Estatal Responsável no Ciberespaço (GGE, do inglês *Group of Governmental Experts*), e o Grupo de Trabalho de Composição Aberta

[67] "*For the first time, a convention addresses illegal activities and practices that crop up across a broad spectrum of cybersecurity threats. Second, it is the first attempt to establish common standards and procedures in cyberspace that are legally binding on its signatories. Third, the convention is open to Council of Europe member states and others, which means it could become an international instrument accepted by more than one group of countries. (For example, the United States has signed and ratified it.) Finally, and most controversially, the convention introduces requirements for data handling and access, which have given rise to concerns over privacy rights and civil liberties, and, as in the case of Russia, questions about state sovereignty*" (GADY; AUSTIN, 2010, p. 13)

sobre Desenvolvimentos no Campo das Telecomunicações de Informação no Contexto da Segurança Internacional (OEWG, do inglês *Open-Ended Working Group*).

A UIT passou a abranger a cibersegurança entre suas preocupações a partir de 2003, a declarando como questão prioritária em 2006. A partir disso, lançou a Agenda Global de Segurança Cibernética, em 2007, reunindo grupos de especialistas na área. Desde então, cinco Grupos de Especialistas Governamentais no Campo da Informação e Telecomunicações (GGE) se reuniram, estabelecendo discussões e estudos sobre as ameaças que as novas tecnologias trazem à segurança internacional, sugerindo princípios e normas, bem como desenvolvendo propostas tendo em vista as melhores práticas para lidar com os desafios originados do ciberespaço (HERZ, 2019; HOMBURGER, 2019).

Em seus relatórios, recomendaram a cooperação internacional como via para diminuir os riscos à segurança no domínio cibernético, convidaram os países a compartilhar informações sobre as vulnerabilidades e soluções possíveis, bem como apresentaram uma série de recomendações visando estabelecer as melhores práticas e comportamentos, medidas de criação de confiança e capacitação cibernética (PAWLAK, 2016; HOMBURGER, 2019; COLLETT, 2021). O GGE, originalmente, foi formado por especialistas de Estados membros da ONU, incluindo os 5 membros permanentes e respeitando um critério geográfico para a escolha dos demais, e exigindo o consenso para a submissão de seus relatórios à Assembleia Geral da ONU – sem conseguir alcançar esse consenso para o relatório de 2017, no entanto (EFRONY, 2021).

Já o OEWG, criado por proposta do governo russo e com a primeira reunião realizada em 2019, é aberto para a participação de todos os Estados membros e estabelece reuniões juntamente com atores não estatais, como organizações regionais, ONGs, academia e empresas (HERZ, 2019; COLLETT, 2021; EFRONY, 2021). Pensado como um espaço de discussão de ideias e cooperação para a promoção da estabilidade do ciberespaço, atualmente, vem ocorrendo a rodada 2021-2025 de discussões do OEWG. O Grupo visa:

> [...] desenvolver ainda mais as regras, normas e princípios de comportamento responsável dos Estados; considerar iniciativas dos Estados destinadas a garantir a segurança na utilização das tecnologias de informação e comunicação; estabelecer, sob os auspícios das Nações Unidas, um diálogo institucional regular com a ampla participação dos Estados; continuar a estudar, com vista a promover entendimentos comuns, as ameaças existentes e potenciais na esfera da segurança da informação, nomeadamente, a segurança dos dados, e possíveis medidas de cooperação para prevenir e combater tais ameaças, e como o direito internacional se aplica à utilização de tecnologias de informação e comunicação por parte dos Estados, bem como medidas de criação de confiança e de capacitação. (ONU, 2023, s. p.)

No entanto, tais fóruns internacionais não foram capazes de promover regulações ou normas no campo do Direito Internacional que vinculassem os atores, permanecendo na esfera das declarações e recomendações. Observa-se a dificuldade de estabelecer consenso em termos que envolvem o ciberespaço. Isso acaba por acontecer, em grande medida, por se estabelecer uma divisão entre as posições defendidas principalmente por China e Rússia, de um lado; e a descrita "visão Ocidental", defendida por Estados Unidos e União Europeia, do outro (HOMBURGER, 2019). Adicionalmente, percebe-se o não interesse por parte dos Estados em estabelecer normas vinculativas nesse âmbito

Além dessas, outras iniciativas multilaterais e multissetoriais foram desenhadas nesse campo, tais como a Cúpula Mundial sobre a Sociedade da Informação, Comissão Global sobre Estabilidade no Ciberespaço, o Fórum de Governança da Internet (IGF, do inglês *Internet Governance Forum*), a *Paris Call for Trust and Security in Cyber Space* e outros (HOMBURGER, 2019; COLLETT, 2021).

Em relação ao tema da ciberdefesa, tem notoriedade a atuação conjunta dos países na OTAN, a qual reconheceu o ciberespaço como um domínio para suas ações de defesa coletiva ainda em 1999 (ANTONIO, 2020). Em 2008, após uma série de ciberataques sofridos pela Estônia, a Organização aprovou sua primeira Política de Defesa Cibernética. Após esse acontecimento também foi criado o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (CCDCoE - do inglês, *NATO Cooperative Cyber Defence Centre of Excellence*). O CCDCoE é "uma instalação de pesquisa e treinamento credenciada pela OTAN focada em educação, consultoria, lições aprendidas, pesquisa e desenvolvimento em defesa cibernética"[68] (OTAN, 2023, tradução própria).

Conforme o site da OTAN (2023, tradução própria), "a defesa cibernética é tanto sobre pessoas quanto sobre tecnologia" [69], sendo assim, dá atenção à educação, treinamento e realização de exercícios conjuntos – inclusive realizando anualmente o Exercício Anual da Coalizão Cibernética. Sendo assim, além do CCDCoE, possui a Academia de Comunicações e Informação (NCI – do inglês *NATO Communications and Information Academy*), localizada

[68] "[…] *is a NATO-accredited research and training facility focused on cyber defence education, consultation, lessons learned, research and development*." (OTAN, 2023)
[69] "*Cyber defence is as much about people as it is about technology,"* (OTAN, 2023).

em Oeiras, Portugal; a Escola da OTAN, em Oberammergau, na Alemanha; e o Colégio de Defesa da OTAN, em Roma (OTAN, 2023).

Ademais, a Aliança busca desenvolver uma abordagem comum para o desenvolvimento de capacidades entre os membros, definindo metas para a implementação de medidas para capacitação em ciberdefesa. Os países aliados têm se comprometido no compartilhamento de informações, intercâmbio de melhores práticas, desenvolvimento de exercícios conjuntos e assistência mútua para a prevenção, mitigação e recuperação diante de ataques cibernéticos. Além disso, a Organização possui um Comitê de Defesa Cibernética (CDC, do inglês *Cyber Defence Committee*), um Conselho de Administração de Defesa Cibernética (CDMB, do inglês Cyber Defence Management Board), equipes de reação cibernética rápida (*NATO Cyber Rapid Reaction teams*) e um Centro de Operações Ciberespaciais, localizado na Bélgica. Tem buscado também cooperar com a União Europeia, tendo firmado, em fevereiro de 2016, o Acordo Técnico sobre Ciberdefesa.

Ainda sobre a OTAN, não se pode deixar de mencionar a elaboração do Manual de Tallinn. Em 2013, um grupo de especialista em Direito Internacional e cibersegurança, convidados pelo CCDCoE, reuniu-se em Tallinn, na Estônia, e elaboraram o "Manual Tallinn sobre a Lei Internacional Aplicável à Ciberguerra". O Manual delimitou uma série de diretrizes sobre a atuação dos Estados nesse novo domínio, abordando temas como soberania, responsabilidade do Estado, o *jus ad bellum* (direito à guerra), Direito Internacional Humanitário e Direito da Neutralidade (SCHMITT, 2013). Mais tarde, em 2017, publicaram o Manual de Tallinn 2.0, buscando ampliar a discussão em relação a operações cibernéticas. Apesar de não ser um instrumento jurídico vinculativo para os Estados, esse documento tem grande importância devido à participação de mais de 50 especialistas e a contribuição – direta ou indiretamente – de muitos países e organizações internacionais no intento de estabelecer regras de comportamento no ciberespaço (SCHMITT, 2017).

> [o Manual de Tallinn] lida com normas contra ataques a infraestruturas críticas das quais depende o bem-estar das sociedades, com compromissos pela não-proliferação de armas cibernéticas, processos internacionais para lidar com ciberataques direcionados a populações civis e, o mais importante, define o que vem a ser um ciberataque - passo crucial para a construção do direito humanitário neste campo, uma vez que desencadeia o direito de autodefesa de um país no ciberespaço. (HERZ, 2019, p. 13).

Ainda que de modo muito incipiente, organizações do Sul Geopolítico também buscaram desenvolver iniciativas de cooperação cibernética. Como exemplo, a União

Africana estabeleceu, em 2014, a Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais (Convenção de Malabo), a qual visa, inicialmente, estabelecer padrões e procedimentos, impondo o desenvolvimento de medidas legais, políticas e regulatórias para promover a governança da segurança cibernética e controlar o cibercrime, como um passo para promover a estabilidade cibernética na região (ORJI, 2018). A Convenção, no entanto, ainda não entrou em vigor, visto que apenas 14 países a ratificaram.

Além disso, em 2019, ocorreu a primeira reunião do Grupo de Peritos em Cibersegurança da União Africana (AUCSEG). Com o objetivo principal de discutir os desafios relativos ao setor cibernético no continente e visando definir as melhores formas de enfrentá-los. Entre as atribuições do grupo estão:

> Aconselhar a Comissão da União Africana (AUC) sobre questões e políticas de segurança cibernética; Propor soluções para facilitar a ratificação e domesticação da Convenção de Malabo nas leis nacionais Partilhar melhores práticas sobre como mitigar as ameaças atuais e as novas e também sobre a proteção de infraestruturas críticas e sistemas eleitorais; Identificar as áreas de pesquisa necessárias para a formulação de políticas, diretrizes, etc., que podem ser gerais ou específicas do setor; Identificar formas de apoiar a criação e desenvolvimento de Equipes de Resposta a Incidentes de Segurança Informática (CSIRTs); Desenvolver formas de estreita colaboração entre os Estados Membros da UA e as partes interessadas, em Cibersegurança; Propor formas de desenvolver capacidades e aumentar as competências na segurança das TIC e na sua utilização adequada; Apoiar a UA na construção da Posição Africana no processo internacional relacionado com a Cibersegurança, incluindo formas de cooperação com as partes interessadas internacionais.[70] (UNIÃO AFRICANA, 2019, tradução própria).

Além dos mecanismos e organizações mencionados, observou-se também iniciativas de cooperação cibernética no âmbito do BRICS (fórum formado por Brasil, Rússia, Índia, China e África do Sul). Apesar de ter sido formado como um fórum mais focado na governança econômica, as constantes mudanças sistêmicas e as ameaças provenientes dessas mudanças, fez com que os países ampliassem as agendas de diálogo e cooperação. Nessa perspectiva, com as lacunas existentes na governança cibernética internacional e pela crescente insegurança no setor, os países têm também discutido sobre o tema. Desde 2010, os

[70] "*Advising the African Union Commission (AUC) on cyber security issues and policies; Proposing solutions to facilitate the ratification and domestication of the Malabo Convention into national laws; Sharing best practice on how to mitigate current and new threats and on the protection of critical infrastructure and election systems as well; Identifying areas of research needed for the formulation of policies, guidelines, etc., which can be general or sector-specific; Identifying ways to support the establishment and development of Computer Security Incident Response Teams (CSIRTs); Developing ways for close collaboration among AU Member States and stakeholders, on Cybersecurity; Proposing ways to build capacities and to increase skills in ICTs security and their proper use; Supporting AU on building African Position within the international process related to Cybersecurity including ways of cooperation with international stakeholders*." (UNIÃO AFRICANA, 2019)

países vêm desenvolvendo conversações a respeito, intensificadas após as exposições da ciberespionagem norte-americana (WANGLAI, 2018).

Desde então estabeleceram mecanismos de cooperação no setor, entre eles estão a formação de grupos de trabalho e conselhos especializados no tema, visando facilitar o desenvolvimento de parcerias e a cooperação entre as agências técnicas, favorecer consultas e troca de informações bem como promover melhores práticas frente às ameaças e a capacitação conjunta. Criaram também o *BRICS Think Tanks Council* (BTTC), em 2013, visando fortalecer a cooperação com o apoio intelectual, promovendo contribuições mútuas na área. Ademais, a chinesa Huawei Corporation tem ajudado outros países do bloco a aprimorarem suas capacidades de TIC a partir do estabelecimento de centros de treinamentos. Em termos de desenvolvimento de infraestrutura de informação, também deve ser citado o BRICS Cable, um projeto aprovado na cúpula do BRICS de 2013 para o desenvolvimento de cabos de 34.000 quilômetros de extensão, de modo a reduzir em 40% os custos de telecomunicações e aumentar a autonomia dos países, já que, atualmente, estes estão conectados por hubs de cabo localizados nos EUA ou na Europa (WANGLAI, 2018).

Devido à importância desse fórum de países emergentes e as divergências na formulação das regras internacionais em relação à área, Wanglai (2018) defende que o avanço nas conversações no bloco teria o potencial de elevar a voz dos países em desenvolvimento na governança global do ciberespaço e na formação de uma nova ordem cibernética global. Para isso, os países têm advogado por uma governança centrada no âmbito do ONU. Na cúpula de 2016, os países destacaram que juntos trabalhariam para a promoção de regras, normas e princípios para um adequado comportamento dos Estados no ciberespaço (WANGLAI, 2018).

Cabe destacar que, na sua configuração original, os países do BRICS possuem, juntos, mais de 40% da população mundial e são importantes exportadores e importadores de tecnologias de informação e comunicação.

> A China é o maior exportador mundial de produtos eletrônicos, com seus eletrodomésticos ocupando mais de 30% do mercado mundial. A Rússia assume a liderança em serviços de banda larga entre os países do BRICS. O custo de sua internet móvel e comunicações é o segundo mais baixo do mundo, superior apenas ao de Hong Kong. A Índia é um grande exportador de software e sua indústria de informação está a caminho de atingir a meta de US$ 225 bilhões em receita até 2020.4 A África do Sul é líder da indústria de telecomunicações da África e sua operadora de telecomunicações é patrocinadora do BRICS Cable. O Brasil é um hub de dados críticos na América do Sul e implantou 24 servidores espelho de

> geodomínio de primeira classe em seu território.[71] (WANGLAI, 2018, p. 127-128, tradução própria).

Embora o BRICS desafie, em certa medida, a hegemonia dos Estados Unidos no ciberespaço global, os países enfrentam, conforme Wanglai (2018) três grandes desafios em sua cooperação em segurança cibernética. A primeira delas diz respeito ao modelo de governança cibernética, já que há divergências quanto ao modelo multilateral centrado no Estado, defendido por China e Rússia, e um modelo mais inclusivo, defendido por Brasil, Índia e África do Sul. Ademais, restam desconfianças quanto aos interesses nacionais e as pressões exercidas por China e Rússia, o que geram restrições no nível doméstico dos Estado quanto a medidas cooperativas no âmbito do fórum. Por fim, o autor ressalta a influência e pressões ocidentais, especialmente norte-americanas, em relação ao bloco, especificamente em relação ao Brasil, África do Sul e Índia.

No continente americano, a OEA tem grande destaque com iniciativas que tem desenvolvido na área. A Organização adotou, ainda em 2004, a Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética, com vistas a coordenar ações entre os Estados membros - sendo o primeiro órgão regional a adotar tal medida. A estratégica é supervisionada pela Comissão de Segurança Hemisférica e por três comitês que administram a sua implementação: I) o Comitê Interamericano contra o Terrorismo (CICTE); II) a Comissão Interamericana de Telecomunicações (CITEL); e III) o Grupo de Especialistas Governamentais em Crime Cibernético das Reuniões de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas (REMJA) (HERZ, 2019).

Entre os planos de ação, a Estratégia previa a criação de uma rede hemisférica que proporcionasse orientações e apoio técnico e propunha a revisão periódica das estratégias elencadas no documento, progredindo a atuação da Organização ao longo do tempo. Ademais, já delineava a importância de formulações de leis e regulamentos bem como de mecanismos de construção de confiança e cooperação no setor (OEA, 2004).

---

[71] "*China is the world's largest exporter of electronic products, with its household electronic appliances occupying over 30% of the world market. Russia takes lead in broadband services among the BRICS countries. The cost of its mobile internet and communications is the second lowest in the world, only higher than Hong Kong. India is a large software exporter, and its information industry is on track to reach the goal of $225 billion in revenue by 2020. South Africa is the leader of Africa's telecommunications industry and its telecom operator is the sponsor of the BRICS Cable. Brasil is a critical data hub in South America and it has deployed 24 top-class geodomain mirror servers in its territory*." (WANGLAI, 2018, p. 127-128)

Com isso, foi elaborado o Programa de Cibersegurança ainda na primeira década do século XX. Conforme divulgação da própria instituição, o Programa se concentra em três tópicos:

I) Desenvolvimento de políticas - buscando auxiliar os Estados membros a desenvolver suas estratégicas de cibersegurança;

II) Capacitação - ajudando a estabelecer Equipes de Resposta a Incidentes de Segurança de Computadores (CSIRTs) nacionais, oferecendo assistência técnica e oportunidades de treinamento e promovendo a troca de informações, principalmente através da rede CSIRTAmericas;

III) Pesquisa e divulgação – oferecendo relatórios e outras ferramentas para orientar formuladores de política, CSIRTs, organizações públicas e privadas e sociedade civil (OEA, 2023b).

Em 2016, foi criada o CSIRTAmericas Network, no qual fazem parte 41 CSIRTs, 284 especialistas e 21 países. Entre suas ações estão a promoção de trocas de informação sobre ameaças cibernéticas, a assistência técnica e treinamento para os especialistas que atuam nos CSIRTs dos Estados membros (CSIRTAmericas, 2023). Outra iniciativa importante ocorre com o apoio do Banco Interamericano de Desenvolvimento (BID). Juntos, BID e OEA, mantém o Observatório de Cibersegurança na América Latina e o Caribe, que desenvolve estudos sobre os níveis das capacidades nacionais dos países latino-americanos, conhecendo a realidade regional, compreendendo seus principais desafios e publicando informes acerca dos resultados encontrados. No próximo capítulo serão identificadas algumas das análises e considerações apresentadas nesses informes.

Sobre as medidas de construção de confiança, em 2017, foi aprovada a criação de um Grupo de Trabalho sobre Cooperação e Medidas de Fortalecimento da Confiança no Ciberespaço, tendo em vista a necessidade de melhorar a transparência e a cooperação entre os Estados membros da OEA. O referido Grupo realiza reuniões periódicas para discussões e atualizações. As medidas basilares para a construção de confiança em cibersegurança acordadas pelos Estados foram:

> 1.Fornecer informações sobre as políticas nacionais de cibersegurança, como estratégias nacionais, livros brancos, marcos jurídicos e outros documentos que cada Estado membro considere relevantes; 2. Identificar um ponto de contato nacional a nível político para discutir as implicações das ameaças cibernéticas hemisféricas; 3. Designar pontos de contato, caso não existam atualmente, nos Ministérios de Relações Exteriores com o fim de facilitar o trabalho de cooperação e os diálogos internacionais sobre cibersegurança e ciberespaço; 4. Desenvolver e fortalecer o

> desenvolvimento de capacidades através de atividades como seminários, conferências e palestras, para funcionários públicos e privados em matéria de diplomacia cibernética, entre outros; 5. Fomentar a incorporação dos temas de cibersegurança e em relação ao ciberespaço nos cursos de formação básica e nas capacitações de diplomatas e funcionários dos Ministérios de Relações Exteriores e outros entes governamentais; 6. Promover a cooperação e o intercâmbio de boas práticas em matéria de diplomacia cibernética, cibersegurança e ciberespaço, por meio da criação de grupos de trabalho, outras convenções de diálogo e a firma de acordos entre os Estados. (OEA, 2023a, s. p. tradução própria).

Em suma, entre os resultados do Programa estão o desenvolvimento de investigações sobre cibersegurança e ciberdefesa nos países e a publicação de informes, análises, guias e planos de ação, bem como realização de treinamentos, simulações e capacitações, com a realização de exercícios de gestão de crise e de seminários, que contam com a participação de funcionários públicos e privados, bem como estudantes e pesquisadores dos países membros. Além disso, tem buscado construir medidas de confiança entre os Estados e incentivar o compartilhamento de informações e o intercâmbio de melhores práticas na área.

Na América do Sul, do mesmo modo, houve iniciativas para cooperação cibernética, especialmente no âmbito do CDS da Unasul, no qual os países sul-americanos buscaram possibilidades de coordenação de posições e de estabelecimento de políticas e mecanismos regionais para combater as ameaças cibernéticas. Essa discussão, no entanto, será detalhada nas seções seguintes deste capítulo.

Diante do explorado, reitera-se que a ciberdiplomacia é crucial para buscar respostas cooperativas no ciberespaço e garantir que respostas mais ofensivas sejam limitadas e não levem a uma escalada desnecessária, com riscos de ações equivocas (BARRINHA; RENARD, 2020). Como mencionado, a diplomacia torna-se essencial para que os Estados possam coordenar ações desenvolver parcerias e processos cooperativos multilaterais. Desse modo, fortalece a construção de confiança entre os atores que pode resultar em processos mais amplos de cooperação. Por outro lado, processos de cooperação multilateral podem resultar em capacidades diplomáticas fortalecidas diante dos fóruns internacionais de governança cibernética. Nesse sentido, ambos os processos podem se retroalimentar, diante de uma acertada estratégia estatal.

Diante desses aportes, tem-se a perspectiva sobre o potencial de desenvolverem estratégias cooperativas que congreguem os diversos setores e instituições nacionais que possam contribuir no campo - setor público, setor privado e academia, num modelo tríplice hélice (HERZ, 2019; PAGLIARI; AYRES PINTO; VIGGIANO, 2020). Ao mesmo tempo,

ampliar essa cooperação para além de suas fronteiras, estabelecendo processos cooperativos com países ou organizações – especialmente levando em consideração esse grupo de países que enfrentam diversas vulnerabilidades na esfera cibernética -, somando forças e diminuindo as debilidades.

Na lógica proposta, capacidades diplomáticas e desenvolvimento de processos de cooperação são ferramentas para aumentar os níveis de segurança e de poder nas dinâmicas envolvendo o ciberespaço. Assim, argumenta-se que o desenvolvimento dessas capacidades e de processos cooperativos, particularmente cooperação Sul-Sul, é essencial aos países menos desenvolvidos que buscam construir sua capacidade cibernética, de modo a aumentar seu poder e sua segurança, visando participar mais ativamente nas discussões sobre a governança cibernética internacional.

Nessa perspectiva, as seções seguintes analisarão o contexto geopolítico da América do Sul, considerando a evolução dos meios cibernéticos e ocupar-se-ão de discutir as capacidades diplomáticas e os avanços e retrocessos da cooperação e da integração regional[72] sul-americana.

3.2 CONTEXTO GEOPOLÍTICO SUL-AMERICANO E O CIBERESPAÇO: NOVAS AMEAÇAS, NOVAS POSSIBILIDADES

A América do Sul pode ser considerada uma região estratégica na competição geopolítica das grandes potências. Além de ser a área de influência direta dos Estados Unidos e historicamente ter sofrido com as pressões desestabilizadoras da potência do Norte, a presença chinesa e russa na região tem se expandido nos últimos anos, colocando a América do Sul em um quadro central nesse cenário de disputas (AGUIRRE; CHAVEZ; ROBLEDO, 2020; TEIXEIRA Jr., 2020a; TEIXEIRA Jr., 2020b; MORAIS DA SILVA; GRASSI, 2022).

[72] Cooperação regional e integração regional não devem ser compreendidos como sinônimos. Cooperação internacional pode ser entendida como "as relações entre os atores internacionais, estatais ou não estatais, buscando elaborar planos de ação conjuntos visando a paz e o desenvolvimento, podendo envolver as mais diversas áreas. [...] exige um grau de coordenação, a partir da convergência de interesses entre os atores, além da disposição de tomarem decisões conjuntas [...]." Diante disso, a cooperação regional "é a cooperação entre os atores de uma mesma região geográfica, continental ou subcontinental" (GRASSI, 2019, p. 27). A integração "implica redução ou eliminação de restrições à livre troca de bens, serviços, capitais e pessoas e, em alguns casos, delegação de soberania a uma autoridade supranacional" (LIMA, 2013, p. 178). Ou, ainda, integração regional pode ser compreendida, a partir de uma definição mais abrangente, como um "fenômeno social segundo o qual dois ou mais grupos humanos adotam uma regulamentação permanente de determinadas matérias que até esse momento pertenciam a sua exclusiva competência." (PUIG, 1986, p. 41). Nessa perspectiva, ela não estaria associada apenas a um fenômeno econômico, podendo abarcar outras áreas para o desenvolvimento dos países.

Em termos geopolíticos, o subcontinente possui recursos naturais estratégicos que o tornará ainda mais disputado nos próximos anos (AMIN, 2015; RODRIGUES, 2015; AGUIRRE; CHAVEZ; ROBLEDO, 2020). A América do Sul é rica em recursos naturais, sejam estes recursos energéticos, minerais, ambientais (como a água) e biológicos (fauna e flora). Tais recursos são considerados estratégicos pela essencialidade no processo de acumulação capitalista, para sua utilização na indústria, para a geração de energia, para as comunicações e transportes, para o desenvolvimento científico e tecnológico ou simplesmente para a manutenção da vida humana. Ainda, são considerados estratégicos pelas baixas reservas mundiais, ou seja, pela escassez no cenário mundial, o que intensifica a competição internacional para sua obtenção e controle (RODRIGUES, 2015).

A América do Sul representa 12% da superfície terrestre, possui mais de 25% da água doce, 22% das florestas e 40% da biodiversidade do mundo. As estimativas são de que a região possui aproximadamente 20% das reservas de petróleo e cerca de 3,5% das reservas de gás, além de possuir grande potencial para geração de energia, de modo geral - solar, eólica, termelétrica, hidrelétrica etc. Além disso, a região é grande produtora de alimentos, com potencial para se destacar como o celeiro do mundo (AMORIM, 2013; RODRIGUES, 2015; SOUZA, 2015).

A geopolítica da água é fator de destaque no cenário internacional e a América do Sul detém cerca de 30% dos recursos híbridos renováveis do mundo, além de possuir imensa capacidade de reposição de águas superficiais e subterrâneas, o que garante o abastecimento dos seus sistemas aquíferos. Sobre isso, o Aquífero Guarani, que compreende os territórios de Brasil, Paraguai, Argentina e Uruguai, é um dos maiores depósitos de água doce do mundo (RODRIGUES, 2015).

> A maior preocupação na atualidade é conciliar o consumo de água per capita com a escassez em determinadas áreas do planeta. A escassez já tem feito surgir situações de “hidroconflitos internacionais” em várias regiões do planeta. Podem ser mencionados, por exemplo, os casos de Síria, Iraque e Turquia, que há muito tempo vêm tendo desavenças sérias no que diz respeito à utilização das águas dos rios Tigre e Eufrates, cujas nascentes estão em território turco, mas cruzam áreas dos outros dois países (AMIN, 2015, s. p.).

Em relação à biodiversidade, este pode ser visto como um dos recursos mais importantes da região. Conforme Rodrigues (2015, p. 86), “a América do Sul conta com mais de 40% de todas as espécies animais e vegetais existentes do planeta”, sendo que Brasil,

Colômbia, Equador e Peru estão entre os 10 países com maior biodiversidade do globo. Ademais, a bacia amazônica "contém metade das selvas tropicais do planeta, um terço de todos seus mamíferos e de seus répteis, 41% dos pássaros e a metade das plantas". Contudo, a totalidade da fauna e da flora amazônica não é completamente catalogada (PEIXOTO JÚNIOR, 2020).

Além de rica em biodiversidade, a região amazônica (que compreende territórios de 9 países: Brasil, Bolívia, Colômbia, Equador, Guiana, Peru, Suriname, Venezuela e Guiana Francesa) também conta com variedade de reservas minerais, muitas ainda inexploradas ou não explorados de forma intensiva. Essa situação, inclusive, leva ao crescimento da mineração ilegal na região, problema agravado pelas dificuldades de fiscalização e regulação dos países aos quais pertencem o território amazônico. A Bacia Amazônica é também considerada a mais extensa rede hidrográfica do mundo, ou seja, a região também se destaca pelos seus recursos hídricos (AMIN, 2015; PEIXOTO JÚNIOR, 2020).

Como consequência, a Amazônia tem um destaque particular nessa discussão da importância geopolítica da América do Sul, que acentuam os interesses estrangeiros e as interferências externas na região. O interesse internacional em relação à Amazônia não é recente. Em 1992, no artigo "Amazônia – Geopolítica do confronto e geoestratégia da integração", Therezinha de Castro advertia sobre os crescentes interesses internacionais na região: "Neste fim de século, o mundo internacional descobriu que havia um mundo amazônico, enquanto começava a desvendar o mundo antártico" (CASTRO, 1992, p. 71). Assim, a autora ressaltava que se criava, a partir disso, uma retórica internacional em relação à proteção da Amazônia, disseminando um cenário de "mundo primitivo" que "deveria ser conservado para o bem do mundo civilizado, com a Amazônia transformada no patrimônio da humanidade" (CASTRO, 1992, p. 72).

No entanto, o tema está cada vez mais no centro do debate nos fóruns e instituições internacionais. As pressões internacionais com relação à floresta envolvem, por exemplo, a retórica acerca da ineficiência dos Estados na preservação e proteção dessa região frente a atuação de grupos criminosos, biopirataria, mineração ilegal, desmatamento e queimadas. Apontam também para a importância da Amazônia na regulação do clima, discussão que ganha cada vez mais espaço diante do cenário de aquecimento global e mudanças climáticas. Esse discurso, entretanto, mascara também as intenções de potências internacionais de influenciar nas questões internas desses países, diante do grande estoque de recursos estratégicos presentes na região.

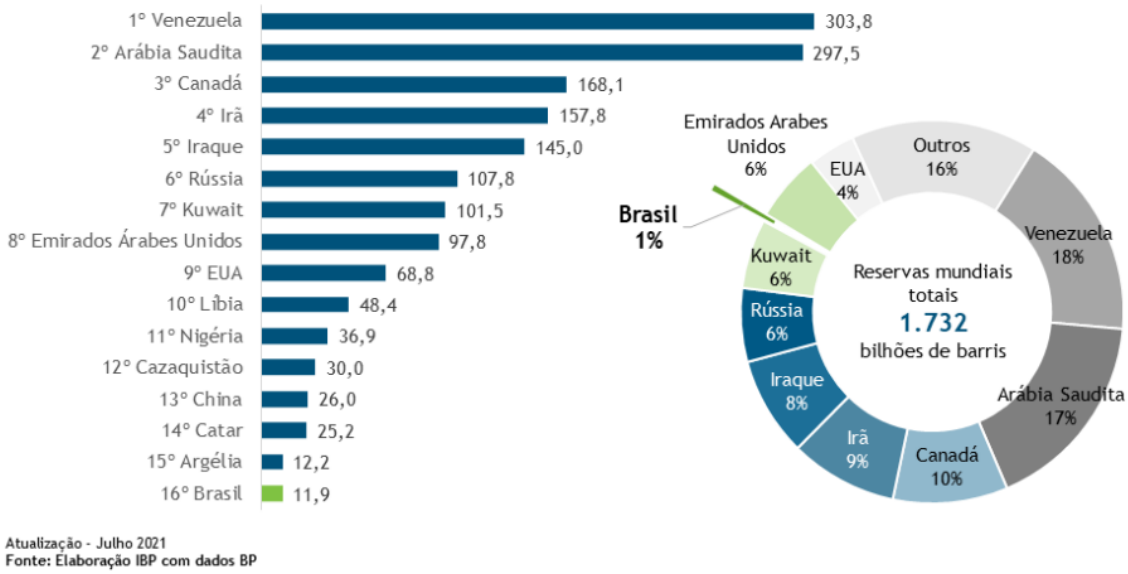
> As diferentes regiões que detêm grande parte dos recursos naturais estratégicos, para as atividades econômicas e produtivas do século XXI, serão os centros determinantes da mobilização de alternativas políticas e estratégias internacionais dirigidas a assumir o controle das reservas de recursos estratégicos. A biodiversidade, os recursos minerais e as grandes reservas de água doce da Amazônia têm exercido, historicamente, enorme interesse de apropriação por parte de vários países e instituições internacionais. Caracterizados pelas forças do mercado internacional como importantes recursos para sobrevivência da humanidade, eles provocam as mais absurdas iniciativas de internacionalização da região Amazônica, desconsiderando completamente a noção da soberania brasileira. (AMIN, 2015, s. p.).

Como exemplo, percebe-se que as bases militares estrangeiras presentes na América do Sul se encontram justamente em áreas ricas com recursos considerados estratégicos. Ademais, cabe destacar, é sintomática a reativação da Quarta Frota dos Estados Unidos em 2008 e a expansão do monitoramento e controle do Comando Sul após as descobertas das reservas de petróleo do Pré-Sal, bem como em um contexto de ampliação da atuação de potências externas na região (RODRIGUES, 2015; RODRIGUES, 2020). Para Pecequilo (2012, p. 53-54):

> A elevação do prestígio brasileiro e as questões energéticas (as reservas do pré-sal brasileiro e no Atlântico Sul) levam à reativação da Quarta Frota do Atlântico Sul, a continuidade do Plano Colômbia e as pressões sobre a Tríplice Fronteira, considerada zona de risco terrorista. A reativação da Quarta Frota responde aos avanços chineses e indianos na América Latina, e ao incremento da cooperação militar entre Venezuela e Rússia (e da aproximação da Venezuela com o Irã).

Além disso, como frisa Moniz Bandeira (2009, p. 20), para que os Estados Unidos possam manter "a posição de potência mundial, que há mais de um século alcançaram, dependem mais e mais de fontes de energia confiáveis, especialmente petróleo [...]". Por essa perspectiva, assegurar o acesso às fontes de materiais estratégicos presentes na região é fundamental para a potência do Norte. Essa realidade continua atual visto, por exemplo, a crise venezuelana, na qual os Estados Unidos têm buscado anular a penetração das potências antagônicas, China e Rússia (TEIXEIRA Jr., 2020a; MORAIS DA SILVA; GRASSI, 2022; PEREIRA DA SILVA et al., 2022). A Venezuela, que ultrapassou a Arábia Saudita, é hoje o país com o maior volume de reservas petrolíferas descobertas, apesar de não ser atualmente o maior produtor.

Gráfico 1 - Maiores reservas provadas de petróleo – em bilhões de barris (2020)



Fonte: IBP (2020)

Sobre os minérios, a América do Sul possui importantes reservas de diversos minerais considerados estratégicos:

> Em termos absolutos, as quinze maiores reservas de recursos minerais da América do Sul correspondem a mais de 15% em relação ao total mundial de cada elemento selecionado. [...] tendo cinco elementos com mais de 35% das reservas mundiais (nióbio, lítio, rênio, cobre e prata), cinco minerais entre 20-35% (selênio, estanho, molibdênio, iodo e minério de ferro) e cinco entre 15-20% (boro, antimônio, tântalo, terras raras e bauxita/alumina). (RODRIGUES, 2015, p. 74).

Particular importância tem as grandes reservas sul-americanas de lítio, já que mais de 50% das reservas mundiais desse minério estão presentes na Bolívia (Salar de Uyuni), no Chile (no Salar de Atacama) e na Argentina (no Salar del Hombre Muerto). O lítio é crucial para o desenvolvimento da indústria tecnológica; por exemplo, para a fabricação de cerâmicas e lentes utilizadas em telescópios e para a produção de pilhas e baterias, utilizadas em celulares, notebooks, carros elétricos ou híbridos – sendo, inclusive, colocado como peça-chave para a transição para uma energia limpa. É também utilizado para fins militares (na construção de armas termonucleares) e na medicina (para tratamento de transtorno bipolar e outras doenças mentais) (RODRIGUES, 2015; JESUS; OLIVEIRA NETO; ARAÚJO SILVA, 2023; USGS, 2023).

Gráfico 2 - Reservas mundiais de lítio (2023)

Fonte: elaboração própria com base em USGS (2023).

Assim, a apropriação e controle desse recurso se torna crucial na disputa geopolítica e geoeconômica internacional, sendo este fundamental para o funcionamento do atual modo de produção capitalista e para garantir a dianteira na competição geopolítica-tecnológica das grandes potências. Na lógica atual da produção capitalista, as empresas de tecnologia precisam acessar as reservas desse minério para que possam assegurar a produção e as inovações no setor. Além disso, o desenvolvimento tecnológico e as inovações nessa área são o sustentáculo para a obtenção e manutenção de poder na contemporaneidade. Diante disso, essa região formada por Argentina, Bolívia e Chile tem sido compreendida como o novo triângulo geopolítico sul-americano, denominada de triângulo geopolítico do lítio (RODRIGUES, 2015; JESUS; OLIVEIRA NETO; ARAÚJO DA SILVA, 2023).

> De acordo com o Banco Mundial, a crescente demanda pelo lítio é impulsionada pela necessidade de transição energética para uma economia de baixo carbono, como os objetivos da Agenda 2030 e o Acordo de Paris. Essa demanda exigirá um aumento de 488% na produção de lítio em relação aos níveis de 2018. (JESUS; OLIVEIRA NETO; ARAÚJO DA SILVA, 2023, p. 6).

Nessa perspectiva, a acirrada disputa geopolítica e tecnológica entre Estados e China[73] ganha destaque e a América do Sul, consequentemente, fica no centro da discussão. Historicamente, a geopolítica norte-americana buscou manter o continente americano sob seu estrito controle, seja empregando elementos de *hard power* ou de *soft power,* ao passo que a mantinha afastada da influência de poderes extrarregionais que pudessem se contrapor aos interesses estadunidenses. Assim, percebem-se períodos nos quais as intervenções norte-americanas foram mais diretas e evidentes e outros períodos nos quais foram mais veladas e indiretas (MONIZ BANDEIRA, 2009; BUSSO, 2016; CARMO; PECEQUILO, 2016; GRASSI, 2019). Como pontua Rodrigues (2015, p.43), "para os Estados Unidos, a América Latina constitui seu *hinterland*, sua área de segurança militar, além de ser depósito de imensos recursos naturais."

Contudo, a China vem expandindo sua influência na região principalmente através de acordos econômicos e investimentos - sobretudo em infraestruturas ao expandir para a América do Sul a Iniciativa do Cinturão e Rota (PECEQUILO, 2012; AGUIRRE; CHAVEZ; ROBLEDO, 2020; TEIXEIRA Jr., 2020a; TEIXEIRA Jr., 2020b). O país se destaca entre os parceiros comerciais sul-americanos, sendo que as relações comerciais do país com a América Latina aumentaram 200% entre 2006 e 2016 – enquanto o comércio com os Estados Unidos aumentou 38% no mesmo período (AGUIRRE; CHAVEZ; ROBLEDO, 2020). Para sustentar seu crescimento econômico – e garantir a subsistência da sua volumosa população - o país asiático necessita acesso às commodities, recursos naturais e insumos estratégicos sul-americanos (PECEQUILO, 2012; RODRIGUES, 2015; BUSSO, 2016; AGUIRRE; CHAVEZ; ROBLEDO, 2020; TEIXEIRA Jr., 2020b; MORAIS DA SILVA; GRASSI, 2022).

Por outro lado, as estratégias geoeconômicas chinesas para a região também refletem a importância da América do Sul na geopolítica chinesa de contraposição aos Estados Unidos no cenário internacional. Com isso, visa também estabelecer parcerias e obter apoio em fóruns e instituições internacionais (AGUIRRE; CHAVEZ; ROBLEDO, 2020; TEIXEIRA Jr., 2020b; MORAIS DA SILVA; GRASSI, 2022).

---

[73] A disputa geopolítica e geoeconômica entre EUA e China tem como ponto focal a liderança no campo tecnológico. Essa competição perpassa as tecnologias de Inteligência Artificial, robótica, a infraestrutura 5G e, consequentemente, o controle dos recursos, como o lítio, e demais insumos essenciais, como os semicondutores[73]. Sobre a tecnologia 5G, esta tem especial relevância, pelas possibilidades de seu uso dual (civil e militar), pois poderá potencializar novas formas de influência e de atuação ofensiva no ciberespaço, através do controle sobre as ferramentas de informação e comunicação, para o ator obter a liderança mundial (PAUTASSO et al., 2021).

Ao discutir o cenário hemisférico, o estrategista norte-americano George Friedman (2012) ressaltava: “historicamente, os Estados Unidos têm negligenciado questões hemisféricas a menos que uma potência global se torne envolvida, ou que elas afetem diretamente seus interesses [...]” (FRIEDMAN, 2012, p. 252). Nessa perspectiva, é possível compreender a retomada de sua agenda de segurança hemisférica para a América Latina nos últimos anos - em contraposição a um período de relativo distanciamento após os acontecimentos do 11 de Setembro, situação que garantiu margens de autonomia para a região -, visto a expansão da atuação de potências extrarregionais na região nos últimos anos.

Especificamente sobre o campo cibernético, a América do Sul segue muito dependente dos EUA. Conforme bem pontua Van Raemdonck (2020), essa dependência inicia pelo fato de a região estar ligada à infraestrutura digital dessa potência desde o início. Desse modo, todo o tráfego internacional da região é encaminhado através dos EUA e grande parte do conteúdo produzido na América do Sul fica hospedado neste país. Sobre isso, as revelações de Snowden, em 2013, deixaram evidente a facilidade estadunidense de vigiar a região. Por outro lado, os EUA é o principal financiador das ações da OEA, tendo sido, portanto, peça-chave nas atividades de construção de capacidades cibernética e nos exercícios conjuntos realizados pela organização.

A China, por sua vez, tem aumentado sua presença buscando financiar e fornecer infraestruturas para a região. Além disso, tem estreitado o diálogo, visando garantir apoio nas discussões sobre a governança cibernética internacional (VAN RAEMDONCK, 2020). Ambos buscam, portanto, exercer influência na região nesse campo, construindo infraestrutura, exportando tecnologia e ideias sobre a construção do ciberespaço global.

Sobre as estratégias para garantir o controle norte-americano na região, Friedman (2012) reitera que a fragmentação regional impossibilita a ascensão de um poder regional, situação que, ressalta, é extremamente conveniente para os Estados Unidos. Nesse sentido, inclusive, o autor frisa a importância do estabelecimento de uma estratégia norte-americana que desestabilize a estreita parceria argentino-brasileira, já que o desmoronamento dessa relação seria uma peça-chave para a fragmentação do subcontinente. No entanto, o autor acrescentava que “os governos da América não podem perceber intromissões dos norte-americanos em suas questões, percepção essa que acirra o sentimento antiamericano, o que pode ser problemático.” (FRIEDMAN, 2012, p. 252).

Observa-se, desse modo, que o país atuou nos últimos anos, para manter sua supremacia na região, difundindo a agenda de liberalização econômica ampla, buscando dominar os recursos e mercados regionais, minando os projetos de cooperação e integração regionais (RODRIGUES, 2020). É nessa perspectiva, portanto, que se discute o papel da disputa entre as potências como desestabilizadoras do cenário político e econômico regional, uma vez que contribuem significativamente para a polarização política na região, o que, por sua vez, acaba por minar as iniciativas de cooperação e integração multilateral na região (MORAIS DA SILVA; GRASSI, 2022).

A atuação dessas potências, que buscam garantir a região na sua área de influência, seja através de fórmulas cooperativas e cooptativas, através de acordos econômico-comerciais ou de parceria estratégicas em diversas áreas, e/ou utilizando-se de meios subversivos, interferências híbridas, ciberespionagem, recorrendo ao arsenal cibernético a disposição dessas potências. Esses recursos se tornam particularmente relevantes diante da sua capacidade de possibilitar interferências sutis, tácitas e indiretas, acentuando polarizações e corroendo a estabilidade interna, moldando os interesses dos demais atores e atraindo-os para sua área de influência. Frequentemente, essas estratégias utilizadas envolvem atores internos como intermediadores e facilitadores das ações disruptivas.

Com esse direcionamento, Rodrigues (2020) pondera que os Estados Unidos têm lançado mão dessas ferramentas para realizar intervenções híbridas com a finalidade de desestabilizar os Estados sul-americanos, seja no nível social, político ou econômico, buscando instaurar seus ideais na região e obter vantagens para a consecução de seus interesses. Essa atuação deteriora os avanços logrados pela região também em termos de cooperação multilateral e afeta a projeção sul-americana no cenário internacional (BUSSO, 2016).

Partindo disso, as campanhas de desinformação e as denominadas interferências híbridas precisam ser mencionadas. Tais ferramentas digitais tornaram-se fundamentais para obter vantagens em períodos eleitorais, 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, tem potencial de acelerar polarizações, interferir ou alterar resultados políticos e desestabilizar os pilares das democracias liberais (BRADSHAW; HOWARD, 2019; AYRES PINTO; MORAES, 2020; OLIVEIRA; IZYCKI, 2021).

Diante disso, pesquisas sobre a utilização dessas ferramentas têm sido realizadas por diversos institutos de pesquisa ao redor do globo. Como exemplo, apontou-se, em estudo do *Computational Propaganda Research Project*, da Universidade de Oxford, publicado em 2019, que, pelo menos, 70 países vêm realizando campanhas cibernéticas com fins políticos (BRADSHAW; HOWARD, 2019). De forma similar, investigações realizadas entre 2016 e 2019 pelo *Australian Strategic Policy Institute*, as quais analisaram 97 eleições nacionais em países livres ou parcialmente livres, identificaram que em 20 países[74] houve claras evidências de interferências estrangeiras. Entre os países citados no estudo estão Brasil e Colômbia, países nos quais as interferências incluíram ações para gerar dúvidas no processo democrático e questionar a legitimidade do processo eleitoral, através, principalmente, de bots no Twitter e no Facebook (HANSON et al., 2019).

Pode-se afirmar que as campanhas de desinformação e manipulação da informação no período eleitoral no Brasil também visaram afastar o país do seu entorno latino-americano ao propagar informações falsas, manipuladas e/ou tendenciosas sobre países vizinhos, sobre os processos de integração regional e em relação à diplomacia dos governos anteriores de Luiz Inácio Lula da Silva. Ademais, os posicionamentos veiculados durante a campanha eleitoral e, posteriormente, durante a Presidência de Jair Bolsonaro tinham o apoio do então Presidente norte-americano Donald Trump e seus aliados (CASARÕES, 2018). Vale ressaltar o papel da grande mídia que pode ressignificar os acontecimentos através do conteúdo veiculado e reforçar um discurso contrário à cooperação e à integração na região (BIDARRA; GRASSI; KERR OLIVEIRA, 2020).

As eleições colombianas também foram marcadas pelo fenômeno das campanhas de desinformação e manipulação da informação. Como ressaltam Gutiérrez-Coba e Rodríguez-Pérez (2023), vários estudos acadêmicos demonstraram que a desinformação – ou o que denominam como "desordem informativo", que envolveria "mentiras estratégicas, falácias, propaganda, forte apelos à emoção, conspirações ou narrativas de polarização" - esteve presente nas campanhas eleitorais de 2018, nas eleições regionais de 2019, mas também no referendo sobre a paz em 2016 e nos protestos nacionais que ocorreram em 2019. Da mesma

[74] Austrália, Brasil, Colômbia, República Tcheca, Finlândia, França, Alemanha, Indonésia, Israel, Itália, Malta, Montenegro, Países Baixos, Macedônia do Norte, Noruega, Cingapura, Espanha, Taiwan, Ucrânia e Estados Unidos.

forma, investigações atestaram interferências estrangeiras nos processos eleitorais, as quais apontaram Rússia e Venezuela como principais perpetradores.

A situação é similar na Argentina que, em 2023, passa por um conturbado período eleitoral. Enfrentando uma crise econômica sem precedentes e com grande polarização interna, as campanhas de desinformação e manipulação da informação também são intensas, ameaçando os pilares da democracia argentina, tendo estado presente, principalmente, nas estratégias eleitorais da extrema direita (CRIALES, 2023; ENRÍQUEZ, 2023; NICAS, 2023). Essas ferramentas, no entanto, já vêm sendo aplicadas a alguns anos. Conforme Clavero (2018, p. 173, tradução própria) "as redes sociais consolidaram-se como 'uma segunda arena' de disputa de posições políticas, onde a geração e propagação de notícias falsas também desempenham um papel na tentativa de despertar predisposições emocionais nos públicos envolvidos". O autor traz com um exemplo as campanhas realizadas durante a reforma previdenciária realizada por Maurício Macri, em 2017, no país (CLAVERO, 2018). Esses cenários de desinformação e manipulação através das plataformas digitais têm marcado a política latino-americana nos últimos anos (RAULS, 2021).

Apesar dessas pesquisas realizadas, é extremamente difícil mensurar a profundidade dessas interferências e definir precisamente as origens de tais campanhas de desinformação e manipulação da informação. Ainda assim, os processos eleitorais na região – tendo como grande exemplo, as eleições de 2018 e 2022 no Brasil - demonstram o potencial de tais ferramentas presentes no espaço cibernético para a incitação da violência, contestação da confiabilidade da mídia e das instituições democráticas, favorecendo a ascensão e difusão de radicalismos de direita e, consequentemente, desencadeando profundas polarizações e desestabilizações das instituições político-democráticas e econômicas de um país. Essa situação coloca a América do Sul, seus regimes democráticos e sua soberania em risco, principalmente frente aos interesses externos nessa rica região geopolítica, interesses para os quais uma América do Sul próspera e unida em um bloco de poder coeso não é conveniente.

Outro tópico relevante de ser mencionado são as revelações da ciberespionagem norte-americanas, as quais demonstraram nitidamente as estratégias de intervenções da potência, em prol de obtenção de vantagens em acordos comerciais e negociações diversas. Apesar de justificarem sua atuação pela sua necessidade de identificar e combater possíveis ações terroristas, observa-se pelos dados divulgados que as ações de espionagem norte-americana no Brasil envolveram a Presidenta Dilma Rousseff e seus assessores, a Petrobrás e o Ministério de Minas e Energia. No que se trata da espionagem ao Ministério de Minas e

Energia e à Petrobrás, os documentos vazados por Snowden demonstraram um claro interesse nos recursos estratégicos nacionais. A NSA obtinha informações privilegiadas sobre as movimentações da empresa estatal e seus documentos internos. Isso demonstra os claros objetivos econômicos e estratégicos por trás da ciberespionagem estadunidense (OPPERMANN, 2014; BERDU, 2016; TEIXEIRA; DATYSGELD, 2017).

Outro exemplo das intenções por trás das práticas de ciberespionagem estadunidense estavam no documento, escrito em 2009 e divulgado na época, no qual o ex-embaixador norte-americano no Brasil, Thomas Shannon:

> [...] agradece à NSA pelas informações repassadas à diplomacia americana antes da 5ª Cúpula das Américas – um encontro entre os chefes de estado do continente para discutir assuntos comerciais e diplomáticos da região. Na carta, Thomas Shannon escreveu que mais de 100 relatórios que eles receberam da NSA deram a eles uma compreensão profunda dos planos e intenções dos outros participantes da cúpula e permitiram que seus diplomatas se preparassem para aconselhar o presidente dos Estados Unidos Barack Obama em como lidar com questões controversas (CERQUEIRA FILHO, 2014, p. 30-31).

Amorim (2013, p. 13-14), em discurso realizado na Argentina, quando ocupava o cargo de Ministro da Defesa, sintetizou um pouco do pensamento aqui debatido:

> Segundo revelações recentes, a América do Sul aparece como uma região sujeita a operações de espionagem em massa. Temos que refletir sobre como cooperar para enfrentar essas novas formas de ataque e intrusão em nossa soberania. [...] Devemos fazer esforços para promover projetos conjuntos em defesa cibernética. Mas é preciso que nos perguntemos também sobre as causas desse grande interesse por esses dados da nossa realidade. A questão das interceptações digitais aponta para uma questão de vital importância: a questão da proteção dos recursos naturais. [...] Especialistas de diferentes fontes destacaram o enorme aumento da demanda por alimentos, água e energia nas próximas duas décadas e, ao mesmo tempo, o potencial de conflito. [...] Se nos lembrarmos dos debates das últimas décadas, pelo menos três tipos de crises já são visíveis nos noticiários: uma crise alimentar, uma crise ambiental e uma crise energética. Na verdade, a América do Sul é uma potência em todas essas três áreas. (AMORIM, 2013, p. 13-14)

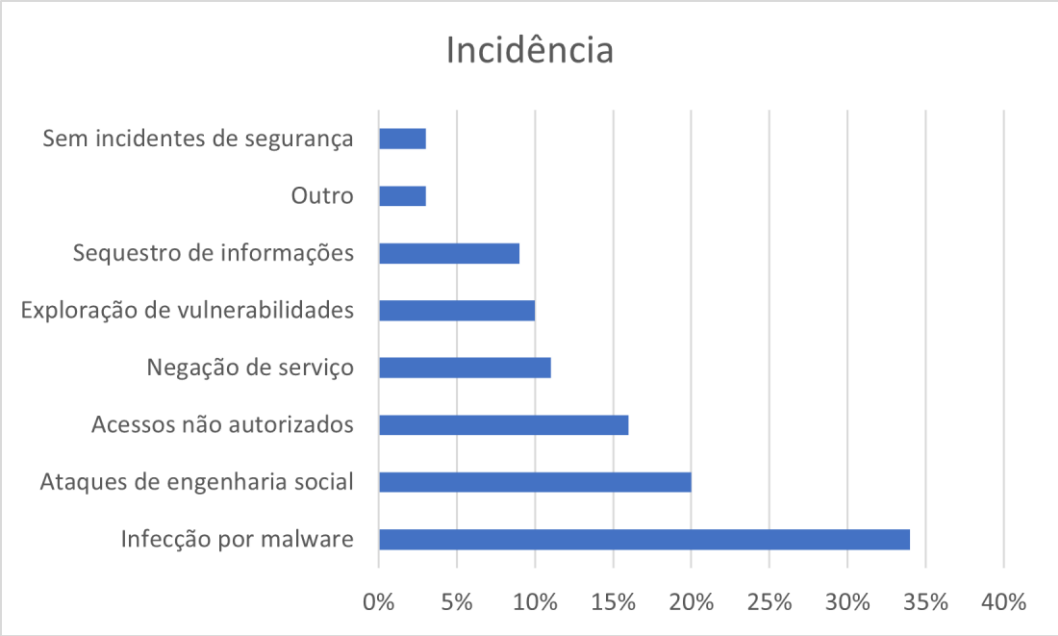
Para mais, entre as principais problemáticas enfrentadas pela região estão os crimes cibernéticos[75], mais relacionados ao campo da segurança cibernética, envolvendo empresas e indivíduos. No entanto, conforme ressalta Oliveira et al (2017, p. 36), os crimes cibernéticos

[75] "[...] são crimes cometidos quando um computador, rede ou qualquer outro meio de tecnologia de informação e comunicação foi usado para cometer um crime. Esses crimes podem incluir uma série de crimes, como crimes económicos, uso indevido da identidade de uma pessoa e download de arquivos ilegais ou pornografia." (Parikh, 2023, p. 61, tradução própria). Para mais conceituações, ver Anexo A.

"também podem atingir a própria defesa cibernética de um país [....] uma categoria de *phishing*, chamada de *skimming*, atinge alvos específicos, civis ou militares." Além disso, a América do Sul possui mais de 3 mil sistemas SCADA/VxWorks (Sistemas de Supervisão e Aquisição de Dados) – sistema utilizado em processos industriais e IC. Os países que mais concentram esses sistemas são Argentina, Peru, Brasil e Colômbia, sendo que a Argentina o país com maior número desses sistemas, concentrando mais 30% destes em seu território (OLIVEIRA et al., 2017). Esses sistemas são constantes alvos de ciberataques por controlar e monitorar os processos de grande parte das infraestruturas críticas nacionais.

No tema da segurança cibernética, conforme dados do ESET Security Report, as principais preocupações das empresas latino-americanas são as infecções com códigos maliciosos, o roubo de dados e o acesso indevido a sistemas. Em termos de incidentes de cibersegurança na América Latina[76], em 2020, o gráfico a seguir traz um panorama, a partir de dados fornecidos pelas empresas consultadas.

Gráfico 3 - Incidentes de Segurança da Informação nas empresas da América Latina (2020)

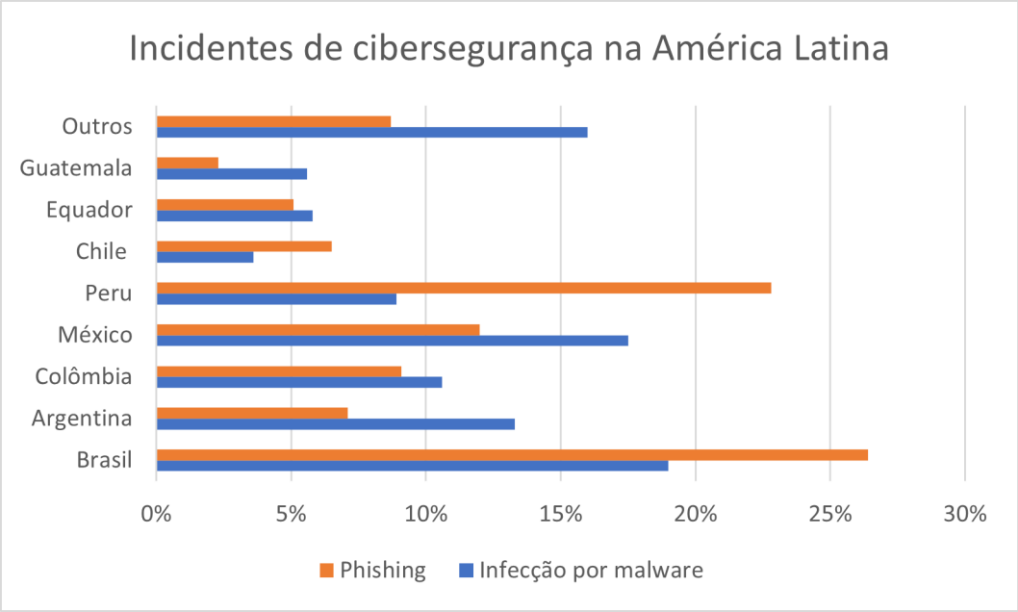


Fonte: elaboração própria com base dos dados de ESET (2021).

[76] Cabe ressaltar que o foco analítico da pesquisa é a América do Sul, no entanto, alguns dados e gráficos apresentados, principalmente nesta seção 3.2 e na seção 4.2, trazem o contexto latino-americano já que não foi possível obter os dados sul-americanos separadamente.

Na América Latina, os países que reportaram mais casos de infecção por malware foram Brasil (19%), México (17,5%), Argentina (13%) e Colômbia (10,6%). Quanto aos ataques de engenharia social, tem-se como caso mais representativo o *phishing* que, geralmente, visa o roubo de informações sensíveis. As empresas brasileiras foram as mais afetadas, com 26,4% das detecções na América Latina no ano de 2020, seguido por Peru (22,8%), México (12%), Colômbia (9,1%) e Argentina (7,1%). Somados, Argentina, Brasil e Colômbia correspondem a mais de 40% das infecções de malware e dos ataques de *phishing* na América Latina (gráfico 4).

Gráfico 4 - Porcentagem de detecção de malware e *phishing* em empresas da América Latina (2020).



Fonte: elaboração própria com dados de ESET (2021)

Além das espionagens, interceptações, crimes cibernéticos, a região enfrenta outros desafios no âmbito cibernético, os quais perpassam os diversas ameaças existentes nesse espaço, conforme exposto no capítulo anterior. Diante disso, assim como os demais países do Sul Geopolítico, a região como um todo sofre com as vulnerabilidades provenientes da falta de recursos orçamentários e dos recursos humanos qualificados, as fragilidades institucionais e organizacionais, a dependência tecnológica em relação aos países mais desenvolvimentos, a baixa produção científica e tecnológica, que perpassa o investimento em pesquisa e pesquisadores, o incentivo insuficiente na produção interdisciplinar e no intercâmbio

acadêmico entre os países da região – ou mesmo em uma perspectiva Sul-Sul. Ademais, os diversos problemas sociais e securitários internos, bem como as crises políticas e econômicas que enfrentam – e que não podem ser desvinculados das dificuldades que enfrentam no âmbito cibernético - geram demandas imediatas e sofrem maiores pressões da sociedade, sendo priorizadas em detrimento das questões de segurança e defesa.

Diante do exposto, pode-se compreender a importância estratégica da região na geopolítica internacional. Diante das características, dos recursos disponíveis e, portanto, da relevância da região, compreende-se a urgência de investir nas múltiplas camadas da segurança e da defesa nacional, diversificar as estratégias e, inclusive, desenvolver projetos conjuntos entre os países, visando também aumentar o poder regional frente às pressões internacionais.

Desse modo, entre as múltiplas camadas da defesa, fundamentais para a proteção desses países frente as diversificadas estratégicas de intervenções estrangeiras na região, está o setor cibernético, que se apresenta - conforme já explorado - como uma nova dimensão para controle e dominação e que possibilita a propagação de uma série de ações, as quais podem ser, inclusive, invisíveis, além de ser extremamente complexas de serem resolvidas.

A partir das considerações levantadas, iniciativas de cooperação foram iniciadas entre os países da região. A seção seguinte centrará na análise dessas iniciativas multilaterais de cooperação e integração que forma levadas a diante pelos países sul-americanos a partir de 2008 – ano que marca a criação da Unasul e o desenvolvimento das primeiras iniciativas de defesa cibernética nos países da região.

3.3 INTEGRAÇÃO NA AMÉRICA DO SUL E OS PROCESSOS COOPERATIVOS EM SEGURANÇA E DEFESA CIBERNÉTICA: DO ÁPICE AO DECLÍNIO (2008-2020)

Os processos multilaterais de cooperação e integração na América Latina não são recentes, já que antes mesmo das independências já se delinearam movimentos integracionistas no subcontinente. Sobre isso, Souza (2012) defende a ideia da existência de ondas da integração, estabelecendo a existência de quatro ondas:

> A primeira corresponde ao período que começa com a independência e conclui na grande crise mundial da primeira metade do século XX – de 1914 a 1945; a segunda inicia com as transformações ocorridas na região durante a grande crise e vai até o esgotamento, em fins dos anos de 1960 e começos dos de 1970, do longo período expansivo de pós-guerra; a terceira corresponde ao declínio dessa onda larga de pós-

> guerra, cobrindo o período que vai da virada da década de 1960 para a de 1970 até o começo da década de 2000; por fim, a quarta e última deflagra-se no início dos anos 2000 e vigora até os dias de hoje. (SOUZA, 2012, p. 88).

Observam-se na região, portanto, que diversas iniciativas tomaram forma ao longo das décadas. Para citar algumas, tem-se a formação da Comunidade Andina de Nações (CAN); da Associação Latino-americana de Livre Comércio (ALALC), que foi substituída pela Associação Latino-Americana de Integração (ALADI); da Organização do Tratado de Cooperação Amazônica (OTCA); do Mercado Comum do Sul (Mercosul); da Iniciativa para a Integração da Infraestrutura Sul-Americana (IIRSA); da Aliança Bolivariana para os Povos de Nossa América (ALBA); da Comunidade Sul-Americana de Nações (CASA/CNS), que foi substituída pela União das Nações Sul-Americanas (Unasul); e da Comunidade dos Estados Latino-Americanos e Caribenhos (CELAC).

Apesar das iniciativas de cooperação e integração que tomaram forma historicamente no cenário latino-americano, observou-se que a América do Sul ganhou maior destaque na política externa dos países dessa região a partir dos anos 1980 e, principalmente, na primeira década do século XXI. Para o avanço das iniciativas sul-americanas, a parceria estratégica entre Brasil e Argentina teve papel crucial. A aproximação dos dois maiores países sul-americanos nos anos 1980, deixando de lado um passado de competição geopolítica regional e iniciando uma relação prioritária bilateral com uma ampla agenda de cooperação, tornou possível a consolidação do Mercosul, em 1991. Para além disso, também estimulou, mais adiante - principalmente durante os governos Lula, no Brasil, e Néstor e Cristina Kirchner, na Argentina - o avanço de outras iniciativas cooperativas na região. As conversações bilaterais nos períodos de maior proximidade, enfatizavam o trabalho conjunto dos dois países em prol da integração sul-americana, visando consolidar a América do Sul como um bloco de poder no sistema internacional. Com isso, convencionou-se afirmar que a parceria estratégia estabelecida entre Brasil e Argentina é o núcleo duro da integração sul-americana, sendo que um processo integracionista no qual um desses dois países não faz parte não poderá se materializar (GRASSI, 2019; GRASSI; KERR OLIVEIRA, 2022).

> A aliança argentino-brasileira é o único caminho real da unificação da América do Sul. Os dois países são o núcleo básico aglutinador. Como foram a França e a Alemanha para a Europa. A unificação da América Latina só pode começar com a unidade da América do Sul, e a unidade da América do Sul só pode ser estruturada a partir da unidade argentino-brasileira. Sem a aliança estratégica entre a Argentina e o Brasil não há unidade sul-americana possível porque, imediatamente, se

> configurariam blocos rivais. Grupos de países mais propensos a apoiar a Argentina e outros o Brasil. O império faria o resto: "Divide e reinarás". (GULLO, 2006, p. 155, grifo do autor).

Ao longo da primeira década do século XXI, observou-se que o direcionamento da política externa dos países sul-americanos os levou a manter certo grau de prioridade para as relações com seu entorno geográfico. Nesse contexto de aproximação entre os países sul-americanos, com a convergência política entre os Estados, a situação econômica favorável, um cenário geopolítico favorável para a região e a busca da autonomia regional, os processos de integração foram impulsionados e as agendas de cooperação foram diversificadas. Esse esforço ultrapassou a tendência de desenvolver projetos de cunho econômico-comercial, passando a abranger temáticas que até então não faziam parte das conversações entre os Estados da região. Assim, os países buscaram resolver seus problemas sem necessitar recorrer a organizações extrarregionais, principalmente as encabeçadas pelos EUA (PECEQUILO, 2012; PAGLIARI, 2015; GRANATO, 2015; CARMO; PECEQUILO, 2016; GRASSI, 2019; PINTO, 2019; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021; PEREIRA DA SILVA et al., 2022; MORAIS DA SILVA; GRASSI, 2022).

Com isso, houve a conformação de um novo modelo integracionista na região, identificados por alguns autores como pós-neoliberal (BRAGATTI; SOUZA, 2016; SANAHUJA, 2012; MARIANO; RIBEIRO, 2016) ou, por outros autores, como pós-hegemônico (RIGGIROZZI; TUSSIE, 2012; BRICEÑO-RUIZ, 2020).

Nesse período, ocorre o revigoramento do Mercosul (Argentina, Brasil, Paraguai e Uruguai), que passa a abranger as dimensões políticas e sociais, inclusive, com a criação do Parlamento do Mercosul e do Fundo para a Convergência Estrutural do Mercosul (Focem), em 2004, e a formação do Instituto Social do Mercosul, em 2006 (GRASSI, 2019; BRICEÑO-RUIZ, 2020; GRASSI; KERR OLIVEIRA, 2022). É nesse contexto que surgem também, em 2004, a ALBA, (liderada pela Venezuela e composta por Cuba, Bolívia, Nicarágua, República Dominicana, Antígua e Barbuda, São Vicente e Granadinas, Santa Lúcia, São Cristóvão e Nevis e Granada), que preconiza uma integração solidária entre os povos, uma proposta anti-imperialista, antineoliberal e anticapitalista (RODRIGUES et al., 2022).

Mais tarde, em 2011, a CELAC se caracterizou como um marco histórico na América Latina por reunir os 33 países latino-americanos pela primeira vez. A CELAC se conformou como um mecanismo de diálogo e concertação política que chegou a ser

apresentada por alguns países como uma alternativa à OEA, simbolizando a tentativa de distanciamento da América Latina do panamericanismo (SOUZA, 2012; BRICEÑO-RUIZ, 2020; PEREIRA DA SILVA et al., 2022).

Contudo, foi a criação da Unasul em 2008 – em substituição à CNS/CASA, constituída em 2004 – que se conformou um marco para a diversificação da cooperação regional, uma vez que a instituição visava criar um espaço de diálogo entre Mercosul e Comunidade Andina, juntando os 12 países sul-americanos para tratar de variados temas. Essa instituição sul-americana se configurou com um espaço de diálogo político e englobou como temas prioritários de sua agenda de cooperação questões de infraestrutura regional, meio-ambiente, democracia, educação, tecnologia, saúde, tráfico de drogas e crime transnacional, inclusão social, justiça social e, inclusive, defesa cibernética[77] (PAGLIARI, 2015; GRANATO, 2015; GRASSI, 2019; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021; MORAIS DA SILVA; GRASSI, 2022). Além do mais, a consolidação da Unasul trouxe a institucionalidade necessária para a região se conformar como uma região geopolítica (COSTA, 2009), tornando-se um 'guarda-chuva' institucional para diversos projetos cooperativos.

Logo após sua constituição, em dezembro de 2008, foi aprovada a criação do Conselho de Defesa Sul-Americano (CDS). Apesar de as iniciativas de cooperação no setor de segurança e defesa no âmbito da Organização dos Estados Americanos remontarem ao século XX, na América do Sul, a Unasul e seu Conselho de Defesa configuraram um ponto de inflexão, no qual os países sul-americanos se propuseram a manter um diálogo multilateral permanente, fortalecer medidas de transparência, ampliando a confiança mútua, e resolver suas problemáticas securitárias sem precisar necessariamente recorrer a mecanismos externos.

> Quando da sua criação, a existência de conflitos sub-regionais e ameaças transnacionais conformavam uma realidade que não mais se coadunava com a anterior ideia de que o continente americano compartilhava somente uma ameaça em termos de segurança. Portanto, o estabelecimento de um mecanismo para discutir e identificar as ameaças à segurança sul-americana surgiu como uma tentativa de

[77] A Unasul era estruturada com 12 Conselhos Setoriais e Ministeriais, os quais demonstravam as prioridades elencadas para a Organização. Era estes: Conselho de Defesa Sul-Americano; Conselho de Saúde Sul-Americano; Conselho Eleitoral da UNASUL; Conselho Energético Sul-Americano; Conselho Sul-Americano de Ciência, Tecnologia e Inovação; Conselho Sul-Americano de Cultura; Conselho de Desenvolvimento Social Sul-Americano; Conselho Sul-Americano de Economia e Finanças; Conselho Sul-Americano de Educação; Conselho Sul-Americano de Infraestrutura e Planejamento; Conselho Sul-Americano sobre o Problema Mundial das Drogas; Conselho Sul-Americano em Matéria de Segurança Cidadã, Justiça e Coordenação de Ações contra o Crime Organizado Transnacional.

> contraponto aos mecanismos coletivos hemisféricos de segurança. (PAGLIARI, 2015, p. 27-28).

Assim, a criação do CDS reflete a preocupação dos países diante da crescente interdependência, da precariedade dos mecanismos interamericanos - como o Tratado Interamericano de Assistência Recíproca (TIAR), a Junta Interamericana de Defesa (JID) e mesmo a OEA - para lidar com as problemáticas sub-regionais. Também reflete as inquietudes acerca do possível transbordamento das novas ameaças securitárias presentes em alguns países, como o caso no narcotráfico colombiano. Visavam, ademais, refrear possíveis desconfianças interestatais, fortalecer o Atlântico Sul como uma zona de paz, garantir a defesa soberana dos recursos naturais e da biodiversidade da região e manter a América do Sul livre da interferência de potências externas (FUCCILLE, 2015; GONÇALVES; BRAGATTI, 2018; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021).

Sobre esse último fator, cabe reiterar que a presença dos Estados Unidos é uma constante na região, apesar de sua interferência ter sido minimizada na primeira década do século XXI, diante do redirecionamento das suas preocupações estratégias para o Oriente Médio no pós-11 de Setembro. Essa situação de relativo distanciamento também possibilitou maiores margens de autonomia regional e favoreceu a reorientação geopolítica dos países (MONIZ BANDEIRA, 2009; PECEQUILO, 2012; CARMO; PECEQUILO, 2016; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021).

O CDS, proposto pelo governo brasileiro, reflete também o esforço do país em prol da estabilidade regional, concretizando-a através da integração sul-americana sob sua liderança, de modo a se firmar como um porta-voz da região, consolidar sua projeção internacional e contribuir para a concretização de seus objetivos geopolíticos (FUCCILLE, 2015; GRASSI, 2019; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021).

O Conselho propôs, portanto, construir uma identidade sul-americana em matéria de defesa, levando em consideração as características e desafios nacionais e sub-regionais, tendo em vista as assimetrias institucionais, econômicas e sociais entre os países da região (FUCCILLE 2015; PAGLIARI 2015; SOUZA 2015). Dentre os objetivos da sua criação também estavam o de promover o diálogo e fomentar o intercâmbio de informações e de análises das ameaças regionais; possibilitar a construção de conceitos e visões compartilhadas em matéria de defesa; organizar posições conjuntas em fóruns internacionais; articular medidas de cooperação na indústria de defesa; compartilhar experiências sobre operações de

manutenção de paz da ONU e sobre os processos de modernização dos Ministérios de Defesa e das Forças Armadas; e oportunizar a capacitação militar e a cooperação acadêmica entre os centros de defesa (SOUZA, 2015).

Para isso, foram estabelecidos quatro linhas de ação (SOUZA, 2015; GONÇALVES; BRAGATTI, 2018; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021):

I) Operações de política de defesa;

II) Cooperação militar, ação humanitária e de paz;

III) Indústria e tecnologia de defesa; e

IV) Formação e capacitação.

Sobre isso, também se menciona a instituição do Centro de Estudos Estratégicos de Defesa (CEED)[78], em Buenos Aires, e da Escola Sul-Americana de Defesa (Esude)[79] para altos estudos, em Quito - respectivamente nos anos de 2009 e 2015. Ambos fortaleceram os esforços em criar um pensamento estratégico sul-americano em matéria de defesa, em consolidar uma política de transparência e intercâmbio de informações e experiências, além de sustentar a capacitação de militares e de civis na área (SAINT-PIERRE; PALÁCIOS Jr., 2014; FUCCILLE 2015; SOUZA, 2015; GONÇALVES; BRAGATTI, 2018; PAGLIARI; VIGGIANO, 2020; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021). A construção de planos de ação e metodologia para a medição de gastos de defesa, exercícios combinados conjuntos, bem como o desenvolvimento de mapas de risco e estudos para a construção de equipamentos militares, visando desenvolver a indústria regional e reduzir sua dependência em relação ao Norte Global, foram outros logros no âmbito da instituição (FUCCILLE 2015; PAGLIARI 2015; SOUZA, 2015; GONÇALVES; BRAGATTI, 2018; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021).

Ainda, a Unasul e o CDS contribuíram para a resolução de controvérsias regionais e crises políticas. Entre elas, pode-se mencionar a discussão acerca de instalações militares norte-americanas na Colômbia em 2009; a tentativa de golpe no Equador, em 2010 - que

[78] O CEED era o responsável pela formulação dos Planos de Ação do CDS e sua criação já é considerada por si uma iniciativa para fortalecimento da confiança. Seu propósito era gerar um pensamento estratégico regional, visando a coordenação e a harmonização das políticas de defesa na América do Sul, estabelecer relações institucionais entre os membros, fomentar o intercâmbio entre os Ministérios de Defesa e atuar como um "centro de documentação para memória institucional da Unasul", tendo como um dos seus produtos a apresentação do Registro de Gastos em Defesa. Assim, a ele incumbia a formulação de "iniciativas consideradas como medidas de construção da confiança a partir dos objetivos definidos pelo CDS" (PAGLIARI; VIGGIANO, 2020, p. 51).

[79] Impulsionada pelos trabalhos conjuntos de Argentina, Brasil e Equador (ARGENTINA, 2015a).

desencadeou a aprovação, meses mais tarde, do Protocolo Adicional ao Tratado Constitutivo da Unasul de compromisso com a democracia; e a crise política venezuelana em 2014 (SAINT-PIERRE; PALÁCIOS Jr., 2014; SOUZA, 2015; GONÇALVES; BRAGATTI, 2018; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021). Assim, observa-se que a instituição atuou de forma ativa, inclusive como um importante instrumento para a resolução de controvérsias regionais e de auxílio em questões internas dos Estados (SOUZA, 2015).

Em matéria de defesa cibernética, a Unasul é considerada pioneira. Ainda em 2012, os países iniciaram um importante diálogo no âmbito do CDS. A iniciativa partiu de países que estavam empreendendo suas políticas e estratégias no âmbito de seus Ministérios da Defesa, como Brasil, Colômbia e Argentina (VAN RAEMDONCK, 2020). Nesse ano, os países sul-americanos deram o primeiro passo ao criar um grupo de trabalho para avaliar as oportunidades de coordenação de posições e estabelecimento de políticas e de mecanismos regionais para combater as ameaças cibernéticas e informáticas que traziam riscos à defesa dos Estados membros (UNASUL, 2012a).

Na primeira reunião do grupo, realizada em 2012, estabeleceram os objetivos do projeto em curso, entre os quais citam-se:

I) Estabelecer uma rede de contato entre as autoridades competentes, visando o intercâmbio de informações e a colaboração permanente;

II) Realizar um diagnóstico da situação da região, incluindo as capacidades de cada país no setor;

III) Definir um esquema metodológico para o desenvolvimento e implementação de uma política regional de cibersegurança;

IV) Definir as capacidades comuns desejáveis em termos de previsão, prevenção, detecção, dissuasão, resposta e recuperação da cibersegurança;

V) Propor terminologia e conceitos comuns;

VI) Propor um programa de educação em segurança da informação;

VII) Avaliar a implementação de uma estrutura organizacional e os níveis de capacitação para seus membros;

VIII) Propor mecanismos de ação frente a incidentes cibernéticos, bem como mecanismos de gerenciamento pós-incidentes, de modo a gerar uma base de conhecimento para situações futuras; e

XIX) Verificar a viabilidade de desenvolver atividades e exercícios conjuntos, visando, principalmente a construção de confiança (UNASUL, 2012b).

Após o escândalo gerado a partir dos vazamentos relativos à espionagem norte-americana, buscou-se um fortalecimento das iniciativas no âmbito da Unasul, com ênfase à defesa cibernética (JUSTRIBÓ, 2014). Cabe mencionar também que 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 (SFORZIN, 2020).

Ainda assim, ressalta-se que na Reunião de Autoridades e Especialistas em Segurança Informática e das Telecomunicações do Mercosul de 2013, chegaram a propor uma iniciativa para a implementação de políticas de segurança da informação por meio do desenvolvimento de centros de dados, pontos de acesso e serviços de informática. Propuseram também a criação do Grupo de Trabalho sobre Governança, Privacidade e Segurança da Informação e Infraestrutura Tecnológica do Mercosul e conceber mecanismos para evitar a espionagem e os delitos cibernéticos nos países membros, incluindo:

> [...] o desenvolvimento e hospedagem de serviços próprios, a fim de tornar nossas telecomunicações mais seguras e reduzir a dependência de tecnologia estrangeira, garantindo a soberania dos povos do MERCOSUL, considerando que atualmente a troca de tráfego de internet entre os países da região transita principalmente através dos Estados Unidos da América (MERCOSUL, 2013).

Além disso, viram como necessário estabelecer posições conjuntas nas instâncias internacionais sobre governança da internet, promover o intercâmbio de informações e experiências, fortalecer a articulação entre os centros de respostas a incidentes cibernéticos e garantir uma coordenação efetiva, harmonizar protocolos e normativas e melhores práticas de segurança entre os membros do Mercosul. Ademais, sugeriram manter iniciativas conjuntas entre o Mercosul e a Unasul (MERCOSUL, 2013).

No âmbito da Unasul, em 2013, os membros estabeleceram também a intenção de promover o desenvolvimento de tecnologias regionais e instituir iniciativas conjuntas entre Mercosul e Unasul (JUSTRIBÓ, 2014). Inclusive, nesse período, chegaram a propor a construção e conexão das redes de fibra ótica dos países, visando tornar as telecomunicações mais seguras (VAN RAEMDONCK, 2020).

> A UNASUL prometeu US$ 1,5 milhão em 2015 para permitir que o Banco de Desenvolvimento da América Latina (CAF) estudasse a viabilidade de uma "Rede de Conectividade Sul-Americana para Integração". Os chefes de estado da UNASUL mencionaram estes esforços na Assembleia Geral da ONU de 2015, dizendo que garantiriam a segurança das redes nacionais de fibra óptica.[80] (VAN RAEMDONCK, 2020, p. 20-21, tradução própria).

No plano de trabalho de 2013, os países da Unasul também determinaram dar seguimento ao Grupo de Trabalho e, assim, buscar estabelecer política e mecanismos regionais necessários para dar seguimento ao projeto de cooperação multilateral (UNASUL, 2013). Seguindo, em 2014, o Plano de Ação previu a realização de um Seminário Regional de Ciberdefesa, como uma plataforma de discussão em vista a enfrentar os desafios cibernéticos e desenvolver capacidades. Previu-se também a coordenação de atividades com o Conselho de Infraestrutura e Planejamento e o Grupo de Trabalho sobre Telecomunicações do Mercosul (UNASUL, 2014).

Ademais, na X Reunião da Instância Executiva do Conselho de Defesa Sul-americano de 2014, ressaltou-se, entre os objetivos, produzir e sistematizar uma ampla reflexão sobre as definições conceituais da defesa e segurança cibernética, de modo a unificá-los no nível regional; e criar um grupo de trabalho e uma rede de contatos entre as autoridades competentes para troca de conhecimentos, procedimentos e soluções no âmbito de defesa cibernética (GONZALES; PORTELA, 2018).

Os planos de ação de 2015 e 2016 apenas previram a continuação das atividades do Grupo de Trabalho de Ciberdefesa e a coordenação desse com o Conselho de Infraestrutura e Planejamento (Cosiplan) para a realização de um seminário (UNASUL, 2015; UNASUL, 2016). Por fim, no Plano de Ação de 2017, observa-se que a temática continuava na agenda de discussão, adicionando a necessidade de estabelecer um novo cronograma para o plano de trabalho sobre ciberdefesa e coordenar ações para assistência mútua conjuntamente com o Cosiplan (UNASUL, 2017).

Em suma, os países membros entenderam, como um primeiro passo, a necessidade de definir conceitos comuns na área e, a partir disso, seriam avaliadas as possibilidades de avanços com a criação de políticas e mecanismos para lidar com as ameaças em termos de

[80] "UNASUR pledged $1.5 million in 2015 to let the development bank of Latin America (CAF) study the feasibility of a 'South American Connectivity Network for Integration'. UNASUR heads of states mentioned these efforts in the 2015 UN General Assembly, saying they would make sure the national fibre optic networks would be secure." (VAN RAEMDONCK, 2020, p. 20-21)

defesa cibernética. Gonzales e Portela (2018) frisam que os membros seguiram ao longo desses anos debatendo sobre a necessidade de definir uma terminologia no nível regional, buscaram diagnosticar as situações enfrentadas pelos países e identificar ameaças, principais atores, instituições e protocolos. Para além disso, buscaram avançar no estabelecimento de políticas regionais de defesa cibernética. No entanto, não se constatou um efetivo progresso nessas discussões.

No âmbito do Mercosul, foi criado, em 2017, o Grupo Agenda Digital voltado, principalmente, ao avanço da economia digital dos países do bloco. Os planos do Grupo discutem, entre outros tópicos, aspectos técnicos e regulatórios, governo eletrônico, infraestrutura digital e conectividade, segurança e confiança do ambiente digital e habilidades digitais, centrados na economia digital (MERCOSUL, 2023).

Todas as iniciativas mencionadas, bem como os demais projetos que tomaram forma na Unasul e, particularmente, no CDS, são exemplos das intenções dos Estados em atuar conjuntamente nessa área, sem que fosse necessário "como no passado, recorrer a outras potências ou colocar-nos sob o manto de organizações onde prevaleçam interesses estrangeiros." (AMORIM, 2013, p. 12). Ademais, demonstrando o otimismo que pairava na região quanto ao papel da instituição nesse período, para o então Ministro da Defesa do Brasil, "poucas pessoas têm dúvidas de que, hoje, os problemas ou diferenças de percepção entre nossos países serão resolvidos com base na diplomacia e no diálogo." (AMORIM, 2013, p. 10). Diante disso, Amorim (2013, p. 10) afirmava: "Em nossa visão estratégica, a UNASUL será progressivamente um dos centros políticos do mundo". No entanto, 3 anos mais tarde, o cenário passou por uma mudança brusca.

Como foi observado, os Estados não foram capazes de avançar nem na consolidação de um quadro conceitual comum em termos de segurança e defesa cibernética. Além disso, os países não têm conseguido estabelecer estratégias concretas de ciberdiplomacia para coordenar seus interesses no nível regional nem para articulações no nível internacional (VAN RAEMDONCK, 2020). Assim, apesar de a Unasul ter tratado da defesa cibernética, o tema foi e continua sendo trabalhado distintamente por cada país. As distinções perpassam questões conceituais e institucionais. De acordo com Oliveira et al. (2017, p. 40-41):

> Os Estados sul-americanos lidam com a defesa cibernética de três formas: alguns atribuem esse assunto à esfera militar; outros, à esfera civil; e alguns trabalham a defesa e a segurança cibernética separadamente. [...] alguns países, como a Colômbia e a Venezuela, têm estruturas militares responsáveis tanto pela defesa

> cibernética quanto pela segurança cibernética. [...] países como Brasil e Argentina [...] têm estruturas civis para lidar com a segurança cibernética e estruturas militares para lidar com a defesa cibernética. Outra questão que deve ser levantada nessa última categoria de países é o limite entre as responsabilidades. Embora em tese cada esfera tenha a sua, em alguns casos ambas as instituições são envolvidas na resolução de um incidente, em um processo de cooperação [...]. No caso da Colômbia, cuja hierarquia militar é responsável pela segurança e defesa cibernética, não há uma distinção entre esses termos, sendo tudo tratado como segurança cibernética.

Apesar dos direcionamentos que vinham sendo dados no âmbito da Unasul e do CDS e das expectativas quanto a atuação das instituições na região, os projetos foram paralisados e a organização esvaziada. As interferências externas, as crises internas e a polarização política na região levaram ao atrofiamento e desmonte dos processos de integração (BIDARRA; GRASSI; KERR OLIVEIRA, 2020; MORAIS DA SILVA; GRASSI, 2022). Consequentemente, os avanços que vinham sendo observados nas conversações a respeito da agenda cibernética se esvaneceram.

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 das assimetrias, da polarização e das heterogeneidades regionais, seja em termos políticos, econômicos, sociais ou securitários, as decisões por consenso tornam-se complexas (SOUZA, 2015; BIDARRA; GRASSI; KERR OLIVEIRA, 2020; MORAIS DA SILVA; GRASSI, 2022).

A formação da Unasul reflete um período histórico em que coincidiram as vontades políticas dos Estados e o cenário geopolítico regional e internacional era favorável, possibilitando maiores margens de manobra para que os países pudessem se organizar regionalmente, buscando conformar um bloco de poder regional (GRASSI, 2019; PINTO, 2019; GRASSI; KERR OLIVEIRA, 2022). No entanto, os arranjos institucionais estabelecidos eram frágeis e não resistiram às mudanças dos contextos nacionais, regionais e internacionais (PINTO, 2019).

Ainda, apesar das diversas iniciativas que buscavam o fortalecimento de medidas de transparência e a construção de confiança ao longo dos anos, os obstáculos na divulgação de algumas informações e dados do setor de defesa foram uma realidade nos anos de funcionamento da instituição (SOUZA, 2015). Assim dizendo, a cultura de sigilo sobre tais informações, considerada sensíveis para a proteção dos Estados, permaneceu na região.

Sobre a questão orçamentária, essa acaba sendo considerada grande entrave para o andamento dos projetos conjuntos, sobretudo, para os projetos na área de segurança e defesa. Diante de todas as deficiências internas, a área de defesa e, particularmente, a destinação de recursos para as instituições regionais, não costumam ser prioridade, nem costumam ser bem-vistos pela sociedade e pela mídia dos países (SOUZA, 2015; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021). Especialmente, diante das crises econômicas que tomaram forma na região, a partir da segunda década do século XXI, pode-se asseverar como esse cenário, que já era uma constante, foi agravado.

Um processo de integração regional deve ser observado como um projeto de longo prazo, no qual os maiores resultados geopolíticos decorrentes das práticas conjuntas entre os países poderão ser verificados ao longo de anos e décadas. Nessa perspectiva, a predominância de políticas de governo, em detrimento de políticas de Estado é outro entrave estrutural. Como consequência, as alternâncias de governos acabam por ocasionar reorientações significativas também na política externa dos países e, portanto, oscilações em relação ao interesse nos processos de cooperação e integração regional (GRASSI, 2019; ARAÚJO; NEVES, 2021; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021).

Assim, nos últimos anos, com a ascensão de governos com agendas neoliberais, buscou-se romper com o legado dos governos considerados progressistas, os quais ampliaram a agenda de cooperação multilateral na região, e priorizar temáticas econômicas e comerciais para acordos de cooperação, preferencialmente com países do Norte Global (MORAIS DA SILVA; GRASSI, 2022). Essa situação afetou todas as iniciativas de cunho pós-liberal e pós-hegemônico, inclusive as novas agendas propostas no âmbito do Mercosul no início do século XXI, o qual se encontra em um momento de paralisia relativa, devido às inúmeras divergências internas, até mesmo nas questões econômico-comerciais (BRICEÑO-RUIZ, 2020; MORAIS DA SILVA; GRASSI, 2022). Especificamente, as poucas discussões no âmbito da segurança da informação e das comunicações não prosperaram, mesmo as que tinham uma perspectiva comercial e em matéria da indústria de software (SFORZIN, 2020).

Diante de todo esse cenário, a partir de 2016 a Unasul foi sendo esvaziada, com alguns países decidindo suspender sua participação na instituição. Logo, anúncios de retirada definitiva começaram a serem feitos. Pouco tempo depois, ainda em 2019, governos neoliberais na região, com agendas pró-estadunidenses, propuseram a constituição do Fórum para o Progresso da América do Sul (Prosul), como um substituto da Unasul. O Prosul, no

entanto, não se configura como uma organização regional, por não possuir uma estrutura institucional concreta, nem tratado constitutivo, nem mesmo sede. Constitui-se, portanto, como uma iniciativa fragmentada, sem maiores compromissos entre os Estados, um espaço para diálogo e coordenação de ações, mas que se mostrou ineficiente e esvaziado em termos de resultados (BARROS; GONÇALVES; SAMURIO, 2020; BRICEÑO-RUIZ, 2020; BIDARRA, GRASSI, KERR OLIVEIRA, 2020; MALAMUD, 2020; ARAÚJO; NEVES, 2021; MORAIS DA SILVA; GRASSI, 2022; PEREIRA DA SILVA et al., 2022).

Como já ressaltado, as interferências externas têm grande impacto no regionalismo latino-americano, sendo impossível desassociar o atual contexto regional da instabilidade sistêmica que permeia o cenário internacional - principalmente levando em conta a importância geopolítica da região. Nesse sentido, a retomada de uma agenda estadunidense mais clara para a região e as interferências de potências euroasiáticas Rússia e China são fatores fundamentais a serem considerados na polarização e na instabilidade regional que, por consequência, abalou diretamente os processos integracionistas sul-americanos.

Como relacionam Morais da Silva e Grassi (2022, p. 41), essa fragmentação da região traz grandes benefícios para as potências externas que atuam na região, uma vez que negociar como um bloco pode aumentar a capacidade de barganha desse países sul-americanos, suas chances de ter seus interesses atendidos e, portanto, seu poder de negociação: “Bilateralmente, os países sul-americanos têm sua capacidade de negociação defasada; em bloco, o peso político e econômico desse conjunto de países é ampliado e, consequentemente, sua capacidade para barganhar também o é”.

Nesse contexto, também se observa que os países têm optado por recorrer a organismos hemisféricos ou extrarregionais, engajando-se em iniciativas que historicamente possuem forte influência dos Estados Unidos, ou que são encabeçados pela potência do Norte. Isso torna a região muito dependente de instituições externas para a resolução de suas questões internas (MORAIS DA SILVA; GRASSI, 2022). No campo cibernético, são as iniciativas formuladas no âmbito da OEA que primeiro foram postas em prática e é nessa esfera que a estrutura de cooperação está mais bem formada, mais documentos foram desenvolvimentos e mais atividades conjuntas estão em andamento (VAN RAEMDONCK, 2020). Fato importante para isso é que organização possui maior aporte financeiro – já que seu maior financiador é justamente os EUA -, tem uma estrutura mais bem estabelecida e mais recursos humanos envolvidos.

Diante do exposto, autores latino-americanistas persistem defendendo o fortalecimento de projetos regionais, para que a região possa se desprender da forte influência norte-americana e, ao mesmo tempo, não se atrelar a dominação de outras potências externas, garantir maior autonomia para gerir suas demandas internas e maiores margens de manobra para as negociações internacionais. Consoante Rodrigues (2015, p. 42) "uma agenda propositiva para a geopolítica latino-americana deve se basear na afirmação dos novos organismos regionais que excluem os Estados Unidos de sua agenda, a fim de que se possa estabelecer uma agenda autônoma e soberana para a América Latina".

Partindo disso, pode-se compreender os rumos tomado nos últimos anos, observando-se que os obstáculos para os processos de integração na região têm origens estruturais e conjunturais, devendo ser observado os diferentes níveis de análise, doméstico, regional e internacional, na busca por compreender toda a sinuosidade dessas dinâmicas. Todas essas variáveis trouxeram um impacto profundo nas relações regionais e a retomada dessas iniciativas de cooperação e integração, seja pela reativação da Unasul e do CDS, seja pela constituição de novas instituições regionais, será um processo complexo e lento, visto que os países da região, na atualidade, parecem não estar dispostos a comprometer-se em arranjos regionais mais densos.

Referindo-se ao processo de cooperação cibernética que estava em curso na Unasul, Herz (2019, p. 17) pondera que o fim do CDS representou "uma oportunidade perdida neste e em outros campos". A ruptura das iniciativas em defesa cibernética em curso no CDS faz com que a temática ainda seja tratada de modo individual, no âmbito doméstico, não havendo homogeneidade nem em termos conceituais nem em termos de políticas e estratégias para o setor (JUSTRIBÓ, 2014; GONZALES; PORTELA, 2018). Como pondera Justribó (2014), os países sul-americanos apresentam marcos legislativos, políticos e doutrinários diferentes, o que resulta em avanços heterogêneos, dificulta posicionamentos e avanços e coloca a região em mais um cenário de dependência dos atores hegemônicos do sistema.

Contudo, Herz (2019, p. 17) frisa que "a harmonização da legislação nacional, a participação em fóruns internacionais, a criação de regras sobre cibersegurança, a coordenação de políticas em relação ao crime cibernético e a criação de mecanismos de gestão de crises são algumas das tarefas que precisam ser realizadas regionalmente." Nessa perspectiva, pensando em todas as dificuldades e fragilidades próprias dos países sul-americanos, a abordagem cooperativa se apresentar como uma alternativa para a construção

de capacidades cibernéticas na região. Santos Júnior et al (2019, p. 11) também corrobora com essa proposição ao destacar que:

> [...] a cooperação intrarregional é peça-chave para o fortalecimento do sistema brasileiro de ciberdefesa, especialmente porque visa a independência tecnológica de países mais poderosos e, simultaneamente, dificultar a prática da espionagem no espaço cibernético brasileiro e dos membros do Mercosul. Dessa forma, um maior engajamento do Brasil na cooperação multilateral na América do Sul pode contribuir para o estabelecimento de um plano estratégico mais efetivo, tendo em vista o interesse dos países vizinhos em aprimorar seus sistemas de defesa cibernética.

Ainda, entre as vantagens de projetos conjuntos na área, afirma-se que coordenar ações é um caminho para a diminuição dos custos envolvidos na construção de capacidades, além de possibilitar, no longo prazo, a redução da dependência em relação às potências do Norte, detentoras e exportadoras das soluções tecnológicas. Como já mencionado, abordagens coletivas também são interessantes para que os Estados tenham maior poder para fazer pressão nos fóruns de governança internacional e terem seus interesses ouvidos nas organizações internacionais. Ademais, frente as diversas ameaças cibernéticas apontadas, mecanismos para compartilhamento de informações, conhecimentos e experiências, iniciativas conjuntas para treinamento e capacitação de recursos humanos e intercâmbio acadêmico são identificados, pelos estudos e índices de capacitação cibernética analisados, como um pilar fundamental na construção de capacidades cibernéticas.

Em perspectiva, diante dos cenários apresentados, outra iniciativa particularmente interessante para os Estados sul-americanos seria o aprofundamento da cooperação em inteligência[81]. A cooperação em inteligência, inclusive, teria especial importância na construção de confiança entre os países. Ademais, entendendo a informação como elemento estratégico nas relações de poder, a cooperação nessa área torna-se crucial para os Estados – e para a região, no geral - incrementarem suas políticas e estratégias de segurança e de defesa e fortalecerem sua posição no cenário internacional. Essa cooperação se torna ainda mais importante tendo em vista a interdependência entre países e a transnacionalidade das novas ameaças (RIBEIRO, 2006; PALACIOS, 2021).

[81] Atividade de Inteligência, conforme a Política Nacional de Inteligência do Brasil, é dividida em dois grandes ramos: Inteligência, compreendida como a "atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado"; e Contrainteligência, definida como a "atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado." (BRASIL, 2016, s. p.).

Cabe destacar que a cooperação em inteligência é uma realidade, por exemplo, na União Europeia, na OTAN, ou entre os Five Eyes, ou Cinco Olhos (Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia), que ficaram conhecidos após as revelações de Snowden (CERQUEIRA FILHO, 2014; PALACIOS, 2021). Na América do Sul, a cooperação em inteligência está em andamento entre alguns países, por exemplo, fazendo parte da agenda da parceria estratégica entre Argentina e Brasil. Diante das perspectivas referidas, essa cooperação poderia transbordar no contexto regional sul-americano, criando "uma estrutura integrada de cooperação de Inteligência Estratégica" (RIBEIRO, 2006, p. 118).

Adicionalmente, cabe assinalar, não há a percepção de disputas de poder no domínio cibernético entre os países da região (JUSTRIBÓ, 2014; OLIVEIRA et al., 2017; GONZALES; PORTELA, 2018). Nesse sentido, não se pode deixar que a construção de capacidades individualmente acabe se tornando fator de desconfianças na região.

Pensar a construção de cibercapacidades desde uma perspectiva cooperativa regional pode melhorar a 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 (MIKSER, 2020).

Finalmente, no âmbito da ciberdiplomacia desses países, alguns consensos parecem persistir. Entre eles estão a sustentação de que as operações de ciberespionagem estadunidense foram uma violação da soberania e do direito internacional, além de ferir direitos humanos, políticos e sociais. Também defendem a necessidade de normas mais específicas e vinculativas no nível internacional, a construção de confiança entre os atores e o estabelecimento da ONU como plataforma para diálogos sobre a paz, a segurança e a estabilidade internacional do ciberespaço. Partindo de consensos já estabelecidos e buscando novas agendas, os Estados podem unir forças para fazer frente em processos de governança internacional ou na construção de dinâmicas cooperativas com outros atores e organizações internacionais, garantindo, com isso, peso maior as suas demandas e interesses nas negociações internacionais.

Assim, apesar de os países estarem avançando individualmente, como mencionado anteriormente e, coincidindo com os autores consultados, diante dos enormes desafios que a

cibersegurança e a ciberdefesa resultam aos Estados, além do investimento, do desenvolvimento de pesquisas nacionais, da coordenação entre os setores internos aos Estados e das demais medidas de construção de capacidades nacionais, é crucial uma coordenação mais complexa no nível regional e no nível internacional, o desenvolvimento da diplomacia cibernética e de medidas de cooperação interestatal.

> [...] 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 (HERZ, 2019, p. 17).

No caso da América do Sul, por um lado, essa agenda de cooperação aparenta ser um grande desafio, principalmente pela descontinuidade dos projetos e as dificuldades enfrentadas pela polarização política enfrentada nos últimos anos e pelas interferências externas que desestabilizam as instituições e a coesão interna. Contudo, por outro lado, o histórico e as inúmeras iniciativas multilaterais demonstraram a capacidade da região em cooperar em uma diversificada agenda e em resolver problemáticas regionais entre si (PAGLIARI, 2015; GONÇALVES; BRAGATTI, 2018; GRASSI, 2019; MORAIS DA SILVA; GRASSI; KERR OLIVEIRA, 2021; PEREIRA DA SILVA et al., 2022).

Particularmente, no âmbito do CDS, os países já haviam dado os primeiros passos na direção de construir uma agenda conjunta sobre defesa cibernética, estabelecendo os caminhos para avançar na construção de uma política regional. No âmbito do Mercosul, há potencial para retomar as discussões e projetos conjuntos no campo das TICs e para o desenvolvimento de ciência e tecnológica própria, a partir da complementariedade que os países possuem no setor, e avançar no Grupo Agenda Digital[82] do bloco.

[82] Recentemente, foi assinado um Acordo Mercosul de Cooperação em Matéria de Cibersegurança. No entanto, não foi possível encontrar o documento repositório institucional do bloco nem no Acervo de atos internacionais do Brasil. Ademais, as atas da Comissão de Cibersegurança não estão disponíveis ou estão incompletas no repositório do bloco, o que dificulta acompanhar o que tem sido discutido nesse âmbito atualmente. Foi possível observar, no entanto, que a cibersegurança é entendida como sinônimo de segurança informática ou segurança da tecnologia da informação e comunicação e compreenderia "as medidas encaminhadas para preservar a privacidade e os dados pessoais de quem utiliza um computador ou qualquer outro dispositivo inteligente." (MERCOSUL, 2022). Diante disso, pode-se compreender que as iniciativas dentro do bloco, contempladas na cibersegurança, são bem específicas e voltadas a medidas de segurança pública, proteção de dados pessoais, garantia da privacidade online e o bom funcionamento das TICs.

Por fim, seguindo a perspectiva de ondas defendida por Souza (2012), o período atual, onde observa-se um refluxo dos processos de integração regional, parece se encaixar em uma fase de transição entre as ondas integracionistas (PEREIRA DA SILVA et al., 2022). Esse período de transição, segundo Souza (2012), caracterizar-se-ia justamente pela intervenção de potências externas na região. Desse modo, uma quinta onda poderia estar sendo conformada, a qual poderá desenvolver novos formatos e criar ou reformar estruturas (PEREIRA DA SILVA et al., 2022). Caberia, então, encontrar formas de sustentar os projetos como políticas de Estado, de modo a se estabelecer avanços concretos para a região.

3.4 CONSIDERAÇÕES PARCIAIS

Medidas direcionadas à construção de confiança e à cooperação internacional no campo cibernético passaram a ser ponderadas como medidas para garantir a estabilidade e a paz no ciberespaço, principalmente levando em conta a interconectividade das redes e a transnacionalidade das ameaças. Diante disso, surge o campo da ciberdiplomacia, como plataforma para que os Estados possam alcançar seus interesses através do diálogo, da coordenação e da cooperação internacional. Com isso, potências cibernéticas têm investido no aperfeiçoamento das suas habilidades diplomáticas para estabelecer parcerias, defender suas posições e garantir a influência nos espaços de discussão internacional, instituindo, inclusive, "embaixadores cibernéticos", com ampla capacitação para atuarem na área. Como pode ser observado, diversas iniciativas de diálogo e cooperação tomaram forma nas últimas duas décadas, por exemplo, no âmbito da ONU, da UIT, da OTAN, da OEA, da UA, da UE, da ASEAN, dos BRICS e, inclusive, na Unasul e no Mercosul.

Para além disso, medidas cooperativas são compreendidas como pilares para a construção de capacidades cibernéticas e essa discussão tem particular relevância para os países do Sul Global e, nesse contexto, para os países sul-americanos. Os países da América do Sul, particularmente, enfrentam desafios geopolíticos, securitários, políticos, sociais, econômicos e tecnológicos que se tornam empecilhos na construção de capacidades e que, por vezes, dificultam processos de cooperação regional, distanciando-os de projetos conjuntos. No entanto, o contexto no qual esses países se encontram também pode ser considerado como fator para os aproximar.

Justamente diante das diversas fragilidades que possuem processos cooperativos podem ser considerados como vias para superar entraves na construção de capacidades. Coordenar ações regionalmente pode garantir a redução dos custos envolvidos, o desenvolvimento de ciência e tecnologias próprias, o intercâmbio de conhecimentos, a troca de experiências e informações, criar possibilidades de treinamento conjunto e de coordenar posições em fóruns e organizações internacionais para aumentar seu poder de negociação. Isso tudo levaria também ao fortalecimento da confiança entre os atores da região, contribuindo para a estabilidade regional. Ademais, esses processos podem garantir a diminuição da dependência externa, principalmente em relação a potências do Norte e a organizações extrarregionais.

Adicionalmente, os fatores mencionados na segunda seção são elencados, por um lado, como algumas das justificativas que tornam a região relevante no cenário de acirramento da competição geopolítica internacional e vulnerável em diversos aspectos, principalmente diante das novas ameaças provenientes do ciberespaço. Por outro lado, configuram-se como um alerta para que os países da região se atentem para os diversos desafios a sua segurança e, ao mesmo tempo, podem ser ressignificados também como a convocação necessária para um processo conjunto de cooperação em vias a superação das ameaças provenientes desse cenário geopolítico.

Na América do Sul, a cooperação multilateral e os processos de integração que foram estruturados demonstraram, ao longo dos anos, as amplas possibilidades de atuação conjunta e os avanços possíveis a partir dessas dinâmicas cooperativas. A institucionalidade construída representou a oportunidade de subtrair as desconfianças e os conflitos regionais, aumentar as margens de autonomia regional, proporcionar maior dinamismo e melhor posicionamento no sistema internacional frente às demandas regionais. Assim, processos de cooperação bem estruturados teriam a capacidade de elevar a região como um polo de poder regional, conforme foi intencionado na primeira década do século XXI.

Nessa perspectiva, observa-se que o primeiro passo, que já estava sendo levado à diante no CDS e precisaria ser retomado, seria criar um arcabouço comum, primeiramente em termos conceituais e, partindo disso, criar uma política regional e mecanismos para coordenar ações, promover o diálogo e desenvolver os projetos necessários. Iniciativas nessa direção precisariam ser retomadas no âmbito regional e poderiam ocorrer em diferentes níveis, de modo a abranger os variados estágios que se encontram os países sul-americanos. Inclusive, a instituição de um centro de capacitação regional seria desejável, já que como destacado pela

OTAN: “a defesa cibernética é tanto sobre pessoas quanto sobre tecnologia”. Já no âmbito do Mercosul iniciativas pontuais estão em vigor, apesar de esbarrarem na polaridade política e nas enormes divergências que vem paralisando os avanços no bloco até mesmo no âmbito econômico-comercial.

Assim, o atual contexto regional reflete o impasse dessa construção, diante do não interesse dos Estados em se inserir em processos mais densos, mais vinculativos e com maior institucionalização. Os países sul-americanos, desse modo, prevalecem desenhando ações individuais no âmbito nacional e recorrendo a organizações extrarregionais para atender às suas demandas na área. Entretando, partindo do exposto até aqui, fica evidente que os Estados devem voltar esforços para ações centradas tanto em nível nacional quanto no nível regional e internacional, que busquem respostas que ultrapassem as estratégias tradicionais e individualizadas implementadas nas áreas de segurança e defesa. O ciberespaço amplifica ainda mais o entendimento de que, isoladamente, os países sul-americanos não serão capazes de garantir papéis efetivos nas dinâmicas de poder internacional, demonstrando, de modo ainda mais evidente para a região, que apenas em conjunto podem construir as capacidades necessárias para se desenvolverem e para fazer frente às novas e mais intensas ameaças que enfrentarão no século XXI.

4 A CONSTRUÇÃO DE CAPACIDADES CIBERNÉTICAS NA AMÉRICA DO SUL E AS POLÍTICAS E ESTRATÉGIAS CIBERNÉTICAS DE ARGENTINA, BRASIL E COLÔMBIA

Após compreender elementos que perpassam a geopolítica cibernética, analisar ameaças, discutir conceitos e examinar os fatores que direcionam o processo de construção de capacidades, explorar as perspectivas diplomáticas e cooperativas e contexto sul-americano frente a essas discussões, chega-se à etapa final desta tese. Este capítulo tem por intuito traçar o contexto em que se encontram os países sul-americanos, de modo geral e, em particular, Argentina, Brasil e Colômbia, no processo de construção de capacidades, além de analisar e comparar alguns componentes específicos desse processo, visando compreender similaridades, divergências e complementaridades entre os países.

Busca-se, desse modo, contribuir para a resolução da pergunta de pesquisa principal delineada para esta investigação: Quais as potencialidades para a construção de capacidades cibernéticas na América do Sul por meio de processos cooperativos regionais se analisado o contexto geopolítico regional e, particularmente, se comparadas as políticas e estratégias cibernéticas da região?

Para isso, a primeira seção apresentará um panorama da construção de capacidades cibernética a partir dos dados obtidos nos três índices internacionais selecionados (o GCI, o NCSI e o dados obtidos a partir do CCMM), comparando as informações dos países, com especial atenção aos três países elegidos para o aprofundamento da pesquisa. Isso com vistas a observar pontos em que cada um se destaca, elementos de similaridade e possível complementaridade entre os países e as lacunas que precisam superar.

Na segunda seção, utilizando principalmente dados obtidos da *Red Iberoamericana de Indicadores de Ciencia y Tecnología* (RICYT), busca-se compreender o contexto da C&T na América do Sul, com destaque aos dados de Argentina, Brasil e Colômbia, estabelecendo comparações também com países mais desenvolvidos e outras regiões do globo. Além disso, abordam-se discussões sobre a necessidade de investimento e desenvolvimento de políticas públicas para educação cibernética e conscientização de todas as camadas da população, formação e capacitação de recursos humanos, incentivo para pesquisa e desenvolvimento tecnológico. Destaca-se a importância desse pilar como sustentáculo das demais dimensões do processo de construção de capacidades cibernéticas e para superar as grandes disparidades e a

dependência que as nações sul-americanas possuem em relação aos países mais desenvolvidos.

Por fim, a seção final focará em Argentina, Brasil e Colômbia - países, como já explicitado anteriormente, de significativa importância geopolítica na América do Sul e considerados expoentes cibernéticos na região, possuindo potencial para liderarem agendas em processos cooperativos regionais no setor. Essa seção final, dividida em três subseções, empenhar-se-á em investigar, principalmente, os documentos de cibersegurança e ciberdefesa e alguns dos seus direcionamentos, as percepções estratégicas desses países em relação ao ciberespaço, como encararam as dinâmicas cooperativas na esfera e como se organizam institucionalmente.

Dessa forma, busca-se investigar, em especial, elementos comuns que podem ser encarados como potencialidades para a formulação de políticas de cooperação regional na América do Sul, visando construir capacidades cibernéticas de forma conjunta. Isso é compreendido como fundamental para incrementar a segurança e a defesa dos Estados, promover desenvolvimento socioeconômico, aumentar as margens de poder e melhorar a posição desses países no cenário internacional, além de aumentar as margens de autonomia e diminuir a dependência externa.

4.1 CAPACIDADES CIBERNÉTICAS NA AMÉRICA DO SUL: O CONTEXTO REGIONAL E AS REALIDADES DE ARGENTINA, BRASIL E COLÔMBIA

A América do Sul possui aproximadamente 437 milhões de habitantes (aproximadamente 5,5% da população mundial) e mais de 368 milhões de usuários de internet, possuindo uma taxa de penetração da internet em torno de 85% - com pouco mais de 15% da população sul-americana sem acesso à internet (INTERNET WORLD STATS, 2022). Contudo, a região nunca foi um bloco homogêneo e sim uma região consideravelmente assimétrica, seja em termos políticos, econômicos, sociais ou securitários. Nesse sentido, por exemplo, a taxa de penetração da internet na região varia de 70% e 97% entre os países (INTERNET WORLD STATS, 2022) e, da mesma forma, observa-se uma disparidade muito significativa nos índices de segurança cibernética entre os países - conforme demonstram os dados e figuras disponibilizadas a seguir.

Tabela 1 – Estatísticas da América do Sul – população, usuários e penetração da internet (2022)[83]

País	População (2022)	% População	Usuários de Internet (30/06/2022)	% População (Penetração)	Facebook (30/06/2022)
Argentina	45,873,172	10.5 %	41,800,000	91.1 %	41,800,000
Bolívia	11,935,560	2.7 %	8,817,749	73.9 %	8,761,800
Brasil	215,016,658	49.2 %	178,100,000	82.8 %	178,100,000
Chile	19,383,887	4.4 %	18,835,100	97.2 %	18,835,100
Colômbia	51,771,495	11.8 %	43,091,700	83.2 %	43,091,700
Equador	18,086,232	4.1 %	15,618,700	86.4 %	15,618,700
Guiana	792,695	0.2 %	574,5	72.5 %	574,5
Guiana Francesa	311,788	0.1 %	162,800	52.2 %	159,600
Paraguai	7,276,583	1.7 %	6,177,748	84.9 %	4,802,400
Peru	33,729,630	7.7 %	29,359,300	87.0 %	29,359,300
Suriname	595,213	0.1 %	428,2	71.9 %	427,8
Uruguai	3,493,160	0.8 %	3,255,800	93.2 %	3,255,800
Venezuela	28,887,118	6.6 %	22,735,000	78.7 %	16,927,100
Total AS	437,156,844	5.5[84] %	368,960,197	84.4 %	361,717,400
Total Mundo	7,932,791,734	100%	5,385,798,406	67.9 %	3,240,870,377

Fonte: elaboração própria, com os dados de Internet World Stats (2022).

O Brasil é o maior país da América do Sul, tanto em termos de população quanto em tamanho do território (8.544.418 km²), possuindo aproximadamente 215 milhões de habitantes, bem como é o maior em número de usuários de internet com pouco mais de 178 milhões de usuários. Já em termos de penetração de internet no território, o Brasil ocupa a oitava posição na região (INTERNET WORLD STATS, 2022). Considerando que é o maior país da região, também é o mais conectado ao Facebook (em número de usuários totais), o que pode ser estendido para a análise das demais redes sociais.

Já a Argentina fica em terceiro lugar na região em termos de população, com mais de 45 milhões de habitantes, e em segundo em quantidade de usuários que acessam a internet, com quase 42 milhões de usuários. Ocupa a terça posição se levarmos em consideração a taxa de penetração da internet, possuindo uma taxa de aproximadamente 91% de penetração – até 2021 ocupava a primeira colocação, sendo, atualmente, ultrapassada por Chile e Uruguai

[83] O quadro do Internet World Stats considera também as Ilhas Malvinas, mas essas foram desconsideradas para a análise.
[84] Enquanto as porcentagens acima dizem respeito ao total da população da América do Sul, esta porcentagem é única estabelecida em relação ao total da população do globo.

(INTERNET WORLD STATS, 2022). Além disso, seguindo o Brasil, é o segundo país da América do Sul em extensão territorial (2.777.409 km²) (INTERNET WORLD STATS, 2022).

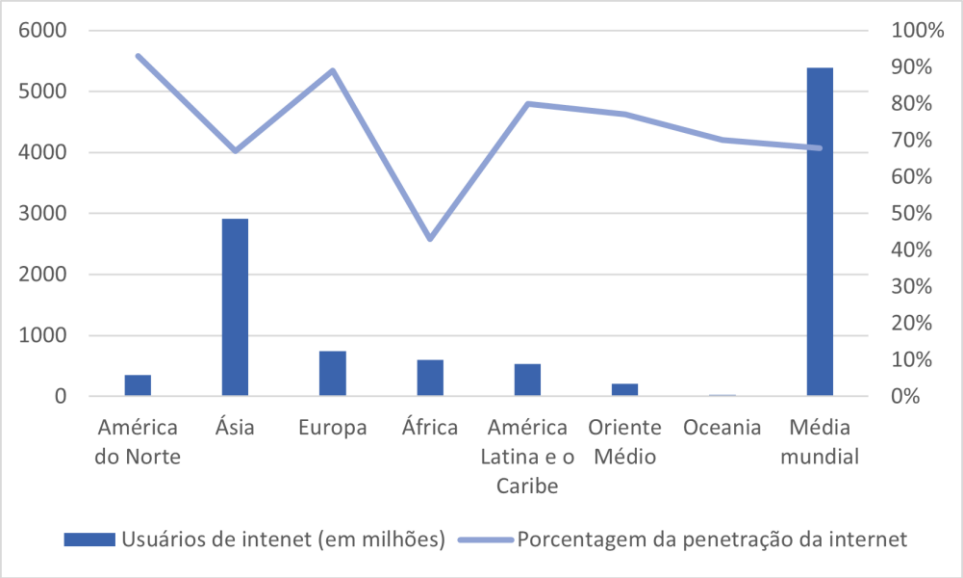
A Colômbia, por sua vez, possui a segunda maior população na América do Sul, com um total de mais de 51 milhões de habitantes, e está na terceira posição regional em termos de usuários de internet, com aproximadamente 43 milhões de usuários. No entanto, no que diz respeito à penetração da internet, a Colômbia ocupa a sétima posição na região (83,2%). Já em termos da extensão territorial, é o quarto maior país da região, com um território de 1.141.748 km² - depois de Brasil, Argentina e Peru (INTERNET WORLD STATS, 2022).

Esses três países são os maiores da região em termos de população da América do Sul e em número de usuários de internet. Juntos, Argentina, Brasil e Colômbia somam mais de 312 milhões de habitantes e quase 263 milhões de usuários de internet, o que corresponde a cerca de 71% da população e dos usuários de internet da América do Sul. Entre os países da região, são, portanto, os mais expostos ao mundo digital. Além disso, em termos de tamanho do território, juntos, correspondem a cerca de 56% do território sul-americano.[85]

Outro dado relevante a ser considerado é que a média global de penetração de internet está em aproximadamente 68%, enquanto a América do Sul está com taxa de aproximadamente 85%, e a maior porcentagem dessa penetração, atualmente, é a da América do Norte, com cerca de 93%, conforme apresenta o gráfico 5.

[85] Território da América do Sul: 17.835.550 km². Argentina, Brasil e Colômbia juntos possuem 9.963.575 km² (INTERNET WORLD STATS, 2022).

Gráfico 5 - Usuários e taxas de penetração da internet no mundo (2022)



Fonte: elaboração própria, com dados de Internet World Stats (2022)

Conforme Oliveira et al. (2017, p. 30), por um lado, "a grande concentração de usuários pode ser benéfica, pois a familiaridade de uma nação com o espaço cibernético pode ser utilizada como recurso de poder cibernético". No entanto, por outra perspectiva, "todos os usuários conectados a esse espaço também representam um canal de acesso para ameaças externas". Consequentemente, quanto mais conectado um país está, seja em relação aos usuários, seja em relação à digitalização dos seus serviços, mais vulnerável ele também estará.

Nesse sentido, inclusive, a grande assimetria entre a quantidade total de usuários de internet no Brasil e o resto dos países sul-americanos pode, por uma perspectiva, corroborar com a ideia do maior poder cibernético do país ou, por outra perspectiva, demonstrar uma grande vulnerabilidade que o Brasil precisa gerir. Isso dependerá, essencialmente, do modo como o Brasil irá gerir seus recursos e criar estratégicas coesas para transformar seus recursos em poder efetivo (OLIVEIRA et al., 2017).

Observando os rankings internacionais, apresentados no primeiro capítulo desta tese, constatam-se níveis de capacitação muito distintos na região. Conforme explicado anteriormente, os índices apresentam dimensões e indicadores diferentes, assim como metodologia e sistemática de coleta de dados distintas, o que acaba por resultar em classificações diferentes quanto ao nível da cibersegurança ou capacitação cibernética dos países. Eles podem, no entanto, serem utilizados de forma complementar para a observação

das lacunas que os Estados e a região, de modo geral, precisam superar na construção das suas capacidades cibernéticas.

O *Global Cybersecurity Index* (GCI), da União Internacional de Telecomunicações da ONU, traz a classificação para a América do Sul[86], conforme apresentado na tabela 2. Pode-se observar que o Brasil se destaca na primeira colocação entre os países sul-americanos, estando bem à frente dos demais países na classificação geral global.

Tabela 2 - Global Cybersecurity Index (América do Sul)

País	Classificação (Global)	Classificação (América)	Classificação (América do Sul)	Pontuação
Brasil	18	3	1	96,6
Uruguai	64	5	2	75,15
Chile	74	7	3	68,83
Colômbia	81	8	4	63,72
Paraguai	84	11	5	57,09
Peru	86	12	6	55,67
Argentina	91	13	7	50,12
Suriname	108	16	8	31,2
Guiana	114	17	9	28,11
Venezuela	116	18	10	27,06
Equador	119	19	11	26,3
Bolívia	140	22	12	16,14
Média regional			**49.67**	

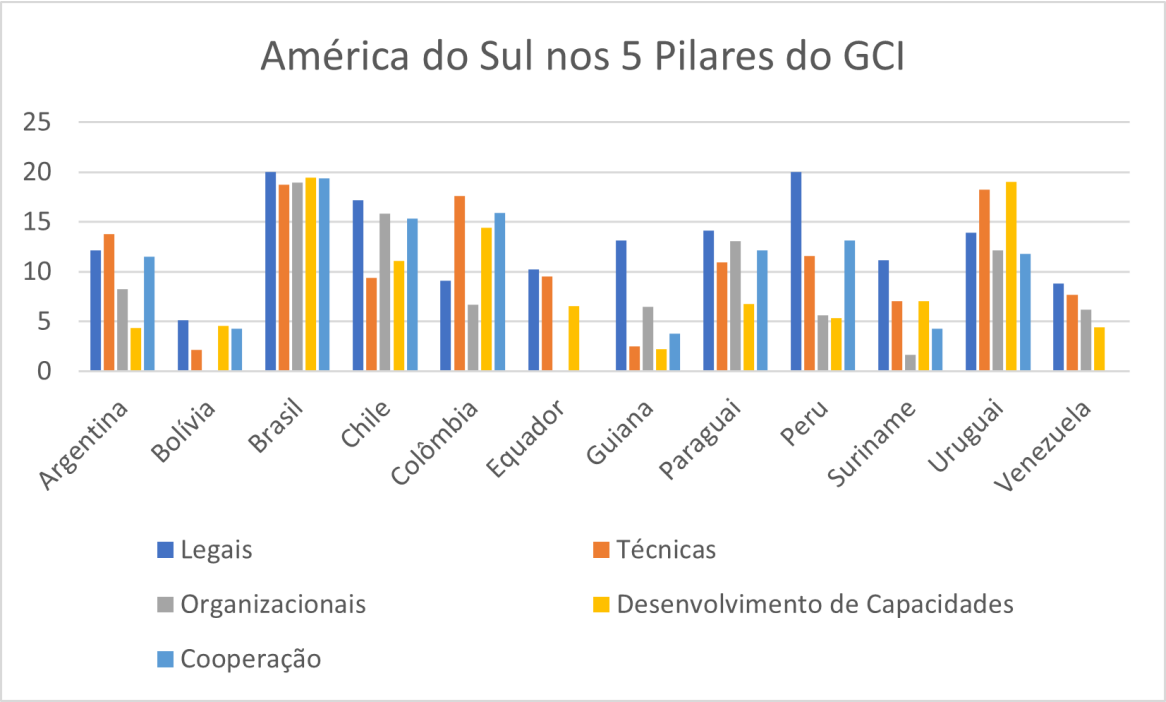
Fonte: elaboração própria, com base nos dados de UIT (2020, p. 28-29)

Ao analisar os pilares separadamente, percebeu-se que alguns países tiraram nota zero em determinados pilares. É o caso da Bolívia nas medidas organizacionais, da Venezuela nas medidas de cooperação e do Equador nas medidas organizacionais e de cooperação. A partir disso, infere-se que, nas 14 perguntas[87] referentes às medidas organizacionais e/ou nas 11 perguntas referentes às medidas de cooperação, esses países responderam 'não' e/ou não forneceram as comprovações. O relatório, no entanto, não expõe precisamente as pontuações

[86] Ressalta-se que todos os países sul-americanos responderam ao questionário da equipe do GCI.
[87] O GCI possui um formulário detalhado com 82 perguntas que são enviadas para que cada país responda. As perguntas de cada pilar podem ser acessadas no anexo B do relatório do GCI (UTI, 2020).

de cada país. O gráfico 6 apresenta a pontuação dos 12 países sul-americanos em cada um dos cinco pilares do GCI[88].

Gráfico 6 - América do Sul nos 5 Pilares do GCI



Fonte: elaboração própria, com base nos dados de UIT (2020)

Observa-se que, em relação à América do Sul, o Brasil se destaca em todos pilares desse índice. Outros destaques merecem atenção:

- Brasil e Peru receberam pontuação máxima nas medidas legais;
- A pior pontuação do Brasil foi nas medidas técnicas;
- Já a Colômbia ficou em 2º lugar nas medidas de cooperação e em 3º nas medidas técnicas e nas medidas de desenvolvimento de capacidades;

[88] Cabe lembra que as Medidas Legais envolvem "medidas baseadas na existência de instituições e quadros jurídicos que tratam da segurança cibernética e do crime cibernético." As Medidas Técnicas são "medidas baseadas na existência de instituições técnicas e quadros que tratam da segurança cibernética." As Medidas Organizacionais dizem respeito às "medidas baseadas na existência de instituições de coordenação de políticas e estratégias para o desenvolvimento da segurança cibernética a nível nacional." Já as Medidas de Desenvolvimento de Capacidades são as "medidas baseadas na existência de programas de investigação e desenvolvimento, educação e formação, profissionais certificados e agências do sector público que promovem a capacitação." E, por fim, as Medidas de Cooperação envolvem "medidas baseadas na existência de parcerias, quadros cooperativos e redes de partilha de informação." (UIT, 2020, p. 131-132).

- Argentina ficou em 4ª posição nas medidas técnicas e em 5ª nas medidas organizacionais entre os países sul-americanos, mas suas melhores pontuações foram nas medidas técnicas e nas medidas legais;
- A pior pontuação da Colômbia foi nas medidas organizacionais e sua segunda pior pontuação foi nas medidas legais – os dois pilares nos quais o Brasil recebeu suas melhores pontuações.
- A pior pontuação da Argentina foi referente às medidas de desenvolvimento de capacidades, apenas ficando acima da Guiana – pilar no qual o Brasil recebeu sua 2ª melhor pontuação;
- Por fim, observou-se que cerca de 33% dos países sul-americanos tiveram suas piores pontuações na dimensão organizacional; outros 33% na dimensão de desenvolvimento de capacidades; outros 25% na dimensão cooperativa; e cerca de 16% obtiveram pontuação mais baixa na dimensão técnica.

O *National Cyber Security Index* (NCSI), por sua vez, ao analisar os países sul-americanos, estabelece uma ordem distinta[89], como pode ser observada na tabela 3. A classificação dos países, conforme detalhado no capítulo 1, refere-se a uma porcentagem em relação a pontuação total atribuída ao país em cada indicadores. Cabe reiterar que, diferente dos demais índices, os resultados disponíveis na plataforma desse *Think Tank* advêm de pesquisas a dados públicos nos países, sejam documentos ou websites oficiais, sendo designado nota zero nos casos em que as evidências não puderam ser obtidas. Além disso, o instituto não fornece relatórios, os resultados e dados são disponibilizados diretamente em seu site oficial.

[89] Sobre isso, chama a atenção o posicionamento do Paraguai, já que, nos demais rankings, o país se coloca na 5ª posição (GCI) e na 6ª colocação (CCMM). Segundo os dados apresentados no site do NCSI, o Paraguai se destaca, com pontuação máxima, no desenvolvimento de sua política cibernética, na Identificação eletrônica e serviços de confiança e na luta contra o cibercrime, além de possuir uma boa pontuação na resposta aos incidentes cibernéticos, no gerenciamento de crises cibernéticas. Todos os dados sobre pontuação e as evidências colhidas estão disponíveis no site do NSCI.

Tabela 3 – National Cyber Security Index (América do Sul)

Ranking regional	Ranking internacional	País	NCSI	Desenvolvimento Digital	Diferença
1	47	Paraguai	63,64	42,58	21,06
2	51	Argentina	63,64	60,43	3,21
3	53	Peru	62,34	48,23	14,11
4	56	Chile	59,74	61,44	-1,70
5	57	Uruguai	59,74	63,86	-4,12
6	67	Equador	53,25	45,57	7,68
7	69	Colômbia	53,25	52,08	1,17
8	71	Brasil	51,95	59,11	-7,16
9	105	Bolívia	31,17	42,09	-10,92
10	111	Venezuela	28,57	43,14	-14,57
11	123	Suriname	22,08	51,50	-29,42
12	155	Guiana	10,39	42,91	-32,51
	Média regional		**46,65**	**51,08**	**-4,43**

Fonte: elaboração própria, com base em National Cyber Security Index (2023)

A tabela 3 mostra também o Nível de Desenvolvimento Digital (DDL). Seu cálculo é feito a partir da média dos percentuais recebidos pelos países no *ICT Development Index* (IDI) e do *Networked Readiness Index* (NRI). Conforme a explicação apresentada no próprio site do NCSI, a diferença entre os dois Índices apresentados demonstra se o desenvolvimento da segurança cibernética do país está de acordo ou à frente do seu desenvolvimento digital (em caso de resultado positivo) ou se sua cibersegurança está aquém do seu desenvolvimento digital (em caso de resultado negativo) (NCSI, 2023). Como pode-se perceber, mais da metade dos países está com nível de desenvolvimento da cibersegurança inferior ao seu desenvolvimento digital, pelos termos propostos pelo NCSI.

Em relação à Argentina, Brasil e Colômbia[90], podemos estabelecer uma comparação a partir da ferramenta disponível no próprio site do NCSI, a qual permite, observar a pontuação dos países em cada um dos 46 indicadores. Importante lembrar que a cada uma das dimensões e dos indicadores é atribuído um valor diferenciado, ponderado em relação à importância dada pelo NCSI àquela dimensão ou indicador - embora não esteja explicado como definem a importância relativa de cada um dos indicadores. O quadro 5 representa as pontuações dos três países nas 12 dimensões e nos 46 indicadores desse índice.

[90] Como o NSCI mantém seu site atualizado conforme as pesquisas vão sendo concluídas, as informações de cada país são de períodos diferentes. Para Argentina, a última versão disponível é de 14 de outubro de 2022. Para Brasil, a atualização é de 19 de agosto de 2022. E, para Colômbia, é de 10 de junho de 2022.

Quadro 5 - Pontuação de Argentina, Brasil e Colômbia nas dimensões e indicadores do NCSI

Capacidades	Argentina	Brasil	Colômbia
1. Desenvolvimento de políticas de segurança cibernética (7 p.)	6 pontos	6 pontos	2 pontos
1.1. Unidade de política de segurança cibernética (3 p.)	✔	✔	
1.2. Formato de coordenação da política de segurança cibernética (2 p.)	✔	✔	
1.3. Estratégia de segurança cibernética (1 p.)	✔	✔	✔
1.4. Plano de implementação da estratégia de segurança cibernética (1 p.)			✔
2. Análise e informações sobre ameaças cibernéticas (5 p.)	2 pontos	4 pontos	2 pontos
2.1. Unidade de análise de ameaças cibernéticas (3 p.)		✔	
2.2. Relatórios públicos sobre ameaças cibernéticas são publicados anualmente (1p.)	✔		✔
2.3. Site de segurança cibernética e proteção (1p.)	✔	✔	✔
3. Educação e desenvolvimento profissional (9 p.)	7 pontos	6 pontos	6 pontos
3.1. Competências de segurança cibernética no ensino primário ou secundário (1 p.)	✔		
3.2. Programa de segurança cibernética de nível de bacharelado (2 p.)	✔	✔	✔
3.3. Programa de segurança cibernética de nível de mestrado (2 p.)	✔	✔	✔
3.4. Programa de segurança cibernética em nível de doutorado (2 p.)			
3.5. Associação Profissional de Segurança Cibernética (2 p.)	✔	✔	✔
4. Contribuição para a segurança cibernética global (6 p.)	2 pontos	2 pontos[91]	2 pontos
4.1. Convenção sobre Crime Cibernético (1 p.)	✔	✔	✔
4.2. Representação em formatos de cooperação internacional (1 p.)	✔	✔	✔
4.3. Organização internacional de segurança cibernética sediada pelo país (3 p.)			
4.4 Capacitação em segurança cibernética para outros países (1 p.)			
5. Proteção de serviços digitais (5 p.)	1 ponto	0 ponto	0 ponto
5.1. Responsabilidade de segurança cibernética para provedores de serviços digitais (1 p.)			
5.2. Padrão de segurança cibernética para o setor público (1 p.)	✔		
5.3. Autoridade de supervisão competente (3 p.)			
6. Proteção de serviços essenciais (6 p.)	1 ponto	1 ponto	1 ponto

[continua...]

[91] O NCSI não pontua o Brasil na dimensão referente à Convenção sobre Crime Cibernético, no entanto, atribuo aqui a pontuação ao país, uma vez que a Convenção foi ratificada pelo país em novembro de 2022 e promulgada por meio do Decreto nº 11.491, de 12 de abril de 2023.

[continuação]

6.1. Operadores de serviços essenciais são identificados (1 p.)	✓	✓	✓
6.2. Requisitos de segurança cibernética para operadores de serviços essenciais (1 p.)			
6.3. Autoridade de supervisão competente (3 p.)			
6.4. Monitoramento regular das medidas de segurança (1 p.)			
7. Identificação eletrônica e serviços de confiança (9 p.)	5 pontos	4 pontos	7 pontos
7.1. Identificador persistente exclusivo (1 p.)	✓		✓
7.2. Requisitos para criptosistemas (1 p.)			
7.3. Identificação eletrônica (1 p.)			✓
7.4. Assinatura Eletrônica (1 p.)	✓	✓	✓
7.5. Carimbo de data/hora (1 p.)			✓
7.6. Serviço de entrega registrada eletrônica (1 p.)			
7.7. Autoridade de supervisão competente (3 p.)	✓	✓	✓
8. Proteção de dados pessoais (4 p.)	4 pontos	4 pontos	4 pontos
8.1. Legislação de proteção de dados pessoais (1 p.)	✓	✓	✓
8.2. Autoridade de proteção de dados pessoais (2 p.)	✓	✓	✓
9. Resposta a incidentes cibernéticos (6 p.)	3 pontos	3 pontos	3 pontos
9.1. Unidade de resposta a incidentes cibernéticos (3 p.)	✓	✓	✓
9.2. Responsabilidade de reporte (1 p.)			
9.3. Ponto de contato único para coordenação internacional (2 p.)			
10. Gerenciamento de crises cibernéticas (5 p.)	3 pontos	1 ponto	1 ponto
10.1. Plano de gestão de crises cibernéticas (1 p.)			
10.2. Exercício de gestão de crises cibernéticas a nível nacional (2 p.)	✓		
10.3. Participação em exercícios internacionais de crise cibernética (1 p.)	✓	✓	✓
10.4. Apoio operacional de voluntários em crises cibernéticas (1 p.)			
11. Luta contra o crime cibernético (9 p.)	9 pontos	4 pontos	9 pontos
11.1. Crimes cibernéticos são criminalizados (1 p.)	✓	✓	✓
11.2. Unidade de crimes cibernéticos (3 p.)	✓	✓	✓
11.3. Unidade forense digital (3 p.)	✓		✓
11.4. Ponto de contato 24/7 (24 horas por dia, 7 dias por semana) para crimes cibernéticos internacionais (2 p.)	✓		✓
12. Operações cibernéticas militares (6 p.)	6 pontos	6 pontos	4 pontos
12.1. Unidade de operações cibernéticas (3 p.)	✓	✓	✓
12.2. Exercício de operações cibernéticas (2 p.)	✓	✓	

[continua...]

[continuação]

12.3. Participação em exercícios cibernéticos internacionais (1 p.)	✔	✔	✔

Fonte: elaboração própria, com base nos dados disponíveis em NCSI (2023)

Observando os dados desse índice sistematizados no quadro 5 é possível perceber claramente pontos nos quais os países estariam em estágios similares, as lacunas que o país precisa preencher no seu processo de construção de capacidades e os tópicos nos quais um ou outro país estaria mais avançado. Esses dados poderiam ser encarados como elementos de complementaridade na formulação de políticas de cooperação ou como áreas em que poderiam propor medidas cooperativas para avançar conjuntamente.

Para exemplificar, em relação aos outros dois países, a Colômbia se destaca nas medidas de confiança dos serviços eletrônicos e no plano de implementação da estratégia de cibersegurança. Esses são pontos nos quais o Brasil precisa avançar, assim como na luta contra o crime cibernético, dimensão na qual tanto Argentina quanto Colômbia tiveram pontuação máxima entre os indicadores analisados pelo NSCI. A Argentina recebeu melhor pontuação no gerenciamento de crises cibernéticas, já o Brasil se destaca na análise e informações sobre ameaças cibernéticas e tem a contribuir regionalmente no âmbito das operações militares. Por outro lado, os três países precisam avançar, por exemplo, na resposta a incidentes cibernéticos, na proteção de serviços essenciais e necessitam participar mais ativamente de processos de cooperação e na governança cibernética global.

Por fim, o terceiro índice analisado se baseia no Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (CCMM), do *Global Cyber Security Capacity Centre* (GCSCC). O relatório sobre cibersegurança do Observatório de Cibersegurança na América Latina e o Caribe da OEA analisa especificamente os países latino-americanos, adaptando o modelo desenvolvido pelo GCSCC para a realidade latino-americana. As investigações e resultados obtidos pelo Observatório representam o panorama da América Latina do ciberespaço, configurando-se como uma ferramenta de grande relevância para compreender as áreas que necessitam maior atenção e investimento por parte dos países, ou nas quais os atores regionais poderiam estabelecer parcerias visando construir capacidades conjuntas e superar suas falhas de segurança e defesa cibernética.

Nas considerações apresentadas no relatório, constata-se que a América Latina está insuficientemente preparada para os desafios originados do espaço cibernético. Dos 32 países investigados pelo Observatório de Cibersegurança na América Latina e Caribe da OEA:

apenas 7 possuíam um plano para proteção das IC; somente 10 haviam estabelecido um organismo central para gestão da segurança cibernética; 20 haviam estabelecido um CSIRT ou uma Equipe de Resposta a Emergências Informáticas (CERT, do inglês, *Computer Emergency Response Team*); e, em 22, considerou-se existir capacidades insuficientes para investigar crimes cibernéticos. Ainda, em um terço dos países não existiam legislações para cibercrimes e, até aquele momento, apenas cinco países haviam ratificado a Convenção de Budapeste sobre Crimes Cibernéticos (BID; OEA, 2020).

Adicionalmente, Moisés J. Schwartz, Gerente de Instituições de Desenvolvimento do BID, relata que há ausência de recursos humanos qualificados para a área, estimando-se que a lacuna de profissionais na América Latina estaria em torno das 600 mil pessoas. Sobre isso, ressalta que apenas 20 países possuíam uma oferta acadêmica em segurança cibernética (BID; OEA, 2020).

A partir dos resultados obtidos pela investigação, o Cone Sul é identificado como a sub-região mais avançada na sua maturidade cibernética, com destaque para a dimensão "Marcos Legais e Regulatórios", dimensão na qual o Brasil obteve a maior pontuação da América do Sul. Na sub-região Andina, a Colômbia destaca-se entre as dimensões do CCMM, principalmente na dimensão "Política e Estratégia de Cibersegurança". Além disso, até 2020, na América do Sul, apenas Colômbia (2016), Chile e Paraguai (2017), Argentina (2019) e Brasil (2020) possuíam uma Estratégia Nacional de Cibersegurança (BID; OEA, 2020).

O relatório do Observatório de Cibersegurança na América Latina e Caribe, no entanto, não estabelece, explicitamente, um ranking dos países com maiores capacidades, trazendo suas pontuações separadamente (de 1 a 5, conforme as definições do CCMM). Assim, analisando os registros apresentados e fazendo uma média da pontuação dos países em cada uma das categorias (considerando todas as categorias com peso igual), obteve-se a classificação da maturidade cibernética dos países sul-americanos (tabela 4).

Tabela 4 - Classificação dos países sul-americanos a partir do CCMM

Posição	País	Pontuação média	Pontuação final[92]
1	Uruguai	3,9	78
2	Colômbia	2,94	58,8
3	Brasil	2,88	57,6
4	Chile	2,73	54,6
5	Argentina	2,33	46,6
6	Paraguai	2,24	44,8
7	Peru	2	40
8	Guiana	1,92	38,4
9	Equador	1,77	35,4
10	Bolívia	1,75	35
11	Venezuela	1,56	31,2
12	Suriname	1,5	30
Média regional		**2,29**	**45,9**

Fonte: elaboração própria, a partir de BID; OEA (2020).

Pode-se observar que a pontuação média da região é inferior a metade da pontuação máxima (5 pontos). Partindo dos estágios de maturidade estabelecidos pelo CCMM da GCSCC (Inicial, Formativa, Consolidada, Estratégica e Dinâmica[93]) e das médias obtidas, a América do Sul estaria na fase Consolidada. No entanto, como já mencionado, a região é consideravelmente heterogênea, sendo assim, por um lado, tem-se o Uruguai como o único país no estágio Estratégico – e Colômbia em vias de alcançar esse estágio -, enquanto mais da metade dos países sul-americanos estão no estágio Formativo.

Lembrando que a fase Inicial indica que não existe uma maturidade em matéria de cibersegurança ou que esta está em fase muito embrionária, podendo haver algumas discussões a respeito, mas sem medidas concretas sendo tomadas. O estágio Formativo indica que iniciativas começaram a ser tomadas, mas estas ainda são pontuais, desorganizadas, mal definidas ou ainda muito recentes para serem avaliadas concretamente. A fase Consolidada demonstra que os indicadores avaliados já estão em funcionamento e com evidências de que estão funcionando; contudo, a alocação de recursos ainda é insuficiente, sendo necessário maior comprometimento com o setor. Enquanto a Estratégica indica que o país dá a devida importância ao setor e demonstra que foram feitas escolhas sobre quais aspectos são mais relevantes para serem priorizados, levando em conta as circunstâncias particulares da nação

[92] A pontuação média considera os 5 pontos dados a cada um dos indicadores apresentados no relatório, enquanto a pontuação final foi obtida considerando nota 100 como total, buscando uma comparação com os outros dois índices.

[93] Compreendo as pontuações de 0 a 5, atribuímos: de 0 a 1 como Inicial; de 1,1 a 2 como Formativa; de 2,1 a 3 como Consolidada; de 3,1 a 4 como Estratégica; e de 4,1 a 5 como Dinâmica.

em questão. Por fim, na fase Dinâmica revela que existem claros mecanismos implementados, sofisticação tecnológica, rápida tomada de decisão, alocação de recursos de forma eficiente, atenção constante ao ambiente e às suas mudanças, bem como percebe-se uma liderança global no setor (GCSCC, 2021).

Como em cada aspecto[94] são atribuídas pontuações de 1 a 5, pode-se identificar em que fase os países se encontram em cada um deles. Assim, observando as pontuações dos países, definiu-se os cinco países sul-americanos mais avançados em cada uma das 5 dimensões do CCMM, obtendo o resultado demonstrado na tabela 5.

[94] O relatório do GCSCC (2021) e apresenta as definições para cada umas das dimensões, dos fatores, dos aspectos e dos indicadores e o que é necessário para que os países obtenham as pontuações de 1 a 5.

Tabela 5 – Liderança nas 5 dimensões do CCMM (América do Sul)

Política e Estratégia de Cibersegurança

Posição	País	Pontuação média
1	Colômbia	3,66
2	Uruguai	3,53
3	Brasil	2,86
4	Chile	2,6
5	Argentina	2,6

Marcos Legais e Regulatórios

Posição	País	Pontuação média
1	Brasil	3,3
2	Chile	3
3	Uruguai	2,9
4	Argentina	2,86
5	Colômbia	2,69

Cultura Cibernética e Sociedade

Posição	País	Pontuação média
1	Uruguai	3,88
2	Chile	3
3	Colômbia	2,88
4	Brasil	2,44
5	Peru	2,2

Padrões, Organizações e Tecnologias

Posição	País	Pontuação média
1	Uruguai	3,9
2	Brasil	2,8
3	Chile	2,4
4	Colômbia	2,3
5	Paraguai	2,2

Educação, Capacitação e Habilidades

Posição	País	Pontuação média
1	Uruguai	3,33
2	Brasil	2,83
2	Colômbia	2,83
3	Chile	2,66
4	Argentina	2,23
5	Paraguai	2,16

Fonte: elaboração própria, a partir de BID; OEA (2020)

Observando as dimensões separadamente, tem-se:

- Na dimensão “Política e Estratégia de Cibersegurança” estão Colômbia e Uruguai no estágio Estratégico e Brasil, Chile e Argentina no Consolidado;
- Na dimensão “Marcos Legais e Regulatórios” estão Brasil e Chile no estágio Estratégico e Uruguai, Argentina e Colômbia no Consolidado;
- Na dimensão “Cultura Cibernética e Sociedade”, Uruguai e Chile estão no estágio Estratégico e Brasil, Colômbia e Peru no Consolidado;
- Na dimensão “Padrões, Organizações e Tecnologias”, Uruguai se destaca no estágio Estratégico e Brasil, Colômbia, Chile e Paraguai estão no Consolidado; e
- Na dimensão “Educação, Capacitação e Habilidades” está apenas Uruguai no estágio Estratégico e Brasil, Colômbia, Chile, Argentina e Paraguai estão no Consolidado.

Adicionalmente, a tabela 6 apresenta as pontuações obtidas por Argentina, Brasil e Colômbia em cada um dos aspectos definidos pelo CCMM e a média obtida nos fatores e nas dimensões, demonstrando que os países conseguiram atingir a fase Estratégica em alguns dos fatores e dos aspectos – Colômbia chegou a alcançar a fase Dinâmica no aspecto de desenvolvimento da estratégia de cibersegurança -, enquanto ainda estão na fase Formativa e, até mesmo, Inicial em outros.

Tabela 6 - Pontuação de Argentina, Brasil e Colômbia nas dimensões, fatores e aspectos do CCMM

Dimensões, fatores e aspectos	Argentina	Brasil	Colômbia
1. Política e Estratégia de Cibersegurança	**2,7**	**2,9**	**3,7**
1.1. Estratégia Nacional de Segurança Cibernética	2,3	2	4,3
1.1.1. Desenvolvimento da Estratégia	2	2	5
1.1.2. Organização	3	2	4
1.1.3. Conteúdo	2	2	4
1.2. Resposta a Incidentes	3	3,8	3,8
1.2.1. Identificação de Indicentes	4	4	3
1.2.2. Organização	3	4	4
1.2.3. Coordenação	3	4	4
1.2.4. Modo de Operação	2	3	4
1.3. Proteção das Infraestruturas Críticas	2	3	3,7
1.3.1. Identificação	2	3	3
1.3.2. Organização	2	3	4
1.3.3. Gestão de Riscos e Resposta	2	3	4
1.4. Gerenciamento de Crise	2	3	4
1.5. Defesa Cibernética	1,7	2,7	3,3

[continua...]

[continuação]

1.5.1. Estratégia	2	3	4
1.5.2. Organização	2	3	3
1.5.3. Coordenação	1	2	3
1.6. Redundância de Comunicações	2	2	2
2. Cultura Cibernética e Sociedade	**2,1**	**2,4**	**2,9**
2.1. Mentalidade de Segurança Cibernética	2,3	2,3	3
2.1.1. Governo	2	2	4
2.1.2. Setor Privado	3	3	2
2.1.3. Usuários	2	2	3
2.2. Confiança e Segurança na Internet	2	3	3
2.2.1. Confiança e Segurança na Internet dos Usuários	2	3	3
2.2.2. Confiança dos Usuários nos Serviços de Governo Eletrônico	2	3	3
2.2.3. Confiança dos Usuários nos Serviços de Comércio Eletrônico	2	3	3
2.3. Compreensão do Usuário sobre Proteção de Informações Pessoais On-line	2	2	2
2.4. Mecanismos de denúncia	2	2	3
2.5 Mídia e Redes Sociais	2	2	3
3. Educação, Treinamento e Habilidades em Cibersegurança	**2,3**	**2,8**	**2,8**
3.1. Conscientização	2,5	3	3
3.1.1. Programas de Conscientização	2	3	3
3.1.2. Conscientização Executiva	3	3	3
3.2. Estrutura para a Educação	2	2,5	2,5
3.2.1. Provimento	3	3	3
3.2.2. Administração	1	2	2
3.3 Quadro para a Formação Profissional	2,5	3	3
3.3.1. Provimento	2	3	3
3.3.2. Administração	3	3	3
4. Marcos Legais e Regulatórios	**2,8**	**3,3**	**2,7**
4.1. Marcos Legais	3,1	3,8	2,9
4.1.1. Quadros legislativos para a segurança das TIC	3	4	3
4.1.2. Privacidade, liberdade de expressão e outros direitos humanos online	4	4	3
4.1.3. Legislação sobre proteção de datas	3	4	3
4.1.4. Proteção infantil on-line	3	3	3
4.1.5. Legislação de Defesa do Consumidor	3	4	2
4.1.6. Legislação de Propriedade Intelectual	3	3	3
4.1.7. Legislação Substantiva Contra o Cibercrime	3	4	3
4.1.8. Legislação Processual Contra o Cibercrime	3	4	3
4.2. Sistema de Justiça Criminal	2,7	3	2,3
4.2.1. Aplicação da lei	3	4	3

[continua...]

[continuação]

4.2.2. Acusação	3	3	2
4.2.3. Tribunais	2	2	2
4.3. Quadros de Cooperação Formal e Informal para Combater o Crime Cibernético	2	2	2,5
4.3.1. Cooperação Formal	2	2	3
4.3.2. Cooperação Informal	2	2	2
5. Padrões, Organizações e Tecnologias	**2**	**2,8**	**2,3**
5.1. Aderência aos Padrões	2	2,7	2,3
5.1.1. Padrões de Segurança de TIC	2	4	2
5.1.2. Padrões de Aquisição	2	2	2
5.1.3. Padrões em Desenvolvimento de Software	2	2	3
5.2. Resiliência da Infraestrutura de Internet	2	3	3
5.3. Qualidade do Software	2	2	2
5.4. Controles Técnicos de Segurança	2	3	3
5.5. Controles Criptográficos	2	3	2
5.6. Mercado de Cibersegurança	2	3	2
5.7. Divulgação Responsável	2	3	2

Fonte: elaboração própria, com dados de BID e OEA (2020).

Enquanto Colômbia chega a atingir a fase Dinâmica no que diz respeito ao desenvolvimento da Estratégia Nacional de Cibersegurança, Argentina e Brasil permanecem na fase Formativa. Outro fator interessante demonstrado pela tabela 6 é que Brasil e Colômbia estão mais avançados nos aspectos "Gerenciamento de Crise", "Defesa Cibernética" e "Proteção das Infraestruturas Críticas" em relação à Argentina. Já em termos de "Marcos Legais", Brasil e Argentina parecem ligeiramente mais avançados que Colômbia.

Observando os aspectos, fica mais claro compreender quais são as áreas e elementos específicos que precisam ser desenvolvidos pelos países, bem como em quais tópicos os países poderiam colaborar, compartilhar conhecimentos e experiências em prol da construção das suas capacidades cibernéticas. No entanto, o que parece evidente ao analisar o nível de capacitação cibernética dos países e no quanto ainda precisam evoluir para alcançar graus mais aceitáveis de segurança e defesa, é que as possibilidades de medidas cooperativas são amplas.

Cabe mencionar, no entanto, que esses índices retratam um panorama desses países quando as investigações foram feitas. Considerando que os Estados estão em processo constante de implementação de medidas de segurança e defesa cibernética, alguns desses dados podem já estar desatualizados. Isso, no entanto, não compromete os resultados dessa pesquisa, uma vez que a intenção é aprofundar a compreensão da situação dos países sul-

americanos em termos de construção de capacidades cibernéticas, para analisar, de modo geral, as possibilidades e a viabilidade de medidas cooperativas nos diversos setores, processos e mecanismos envolvidos.

Por fim, como foi discutido no primeiro capítulo desta tese, os investimentos e o desenvolvimento da ciência e da tecnologia são considerados essenciais para a construção de capacidades cibernéticas. Conforme ponderado por Calderaro e Craig (2020, p. 14, tradução própria), "quanto mais pesquisas científicas um país produzir, maior será sua capacidade cibernética, controlando outros fatores", já que o "conhecimento de C&T é um recurso crucial para o desenvolvimento da prontidão para a segurança cibernética".[95] Diante disso, uma das dimensões do processo de construção de cibercapacidades – apresentados pelos índices, mas também pelas pesquisas destacadas no primeiro capítulo - envolve justamente os fatores educacionais, de ciência e tecnologia, pesquisa e inovação nacional.

Nessa perspectiva, a próxima seção irá destacar esse pilar da construção de capacidades cibernética dos países, com ênfase nos 3 países investigados. Depois disso, analisar-se-á a atual estrutura institucional, as legislações em vigor e as políticas e estratégias que Argentina, Brasil e Colômbia têm desenvolvido neste setor.

4.2 CENÁRIO REGIONAL DA CIÊNCIA & TECNOLOGIA E PARTICULARIDADES DE BRASIL, ARGENTINA E COLÔMBIA

No que se refere especificamente ao investimento em Ciência e Tecnologia (C&T) na América Latina[96] e, particularmente, nos países sul-americanos, a *Red Iberoamericana de Indicadores de Ciencia y Tecnología* (RICYT) fornece dados imprescindíveis, tornando possível estabelecer as comparações disponíveis nessa seção. Todavia, cabe destacar que, em alguns casos, não há dados de todas as nações sul-americanas, sendo assim, em alguns gráficos, poderão faltar informações de alguns países da região. Em outros casos podem não haver dados disponíveis para os anos mais recentes.

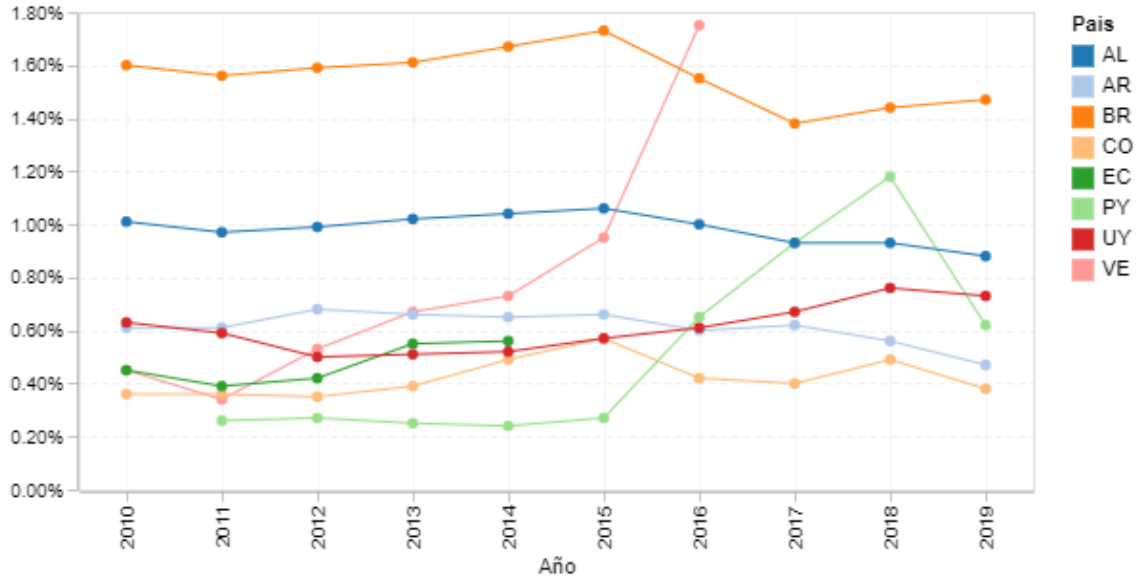
---

[95] "*The more scientific research a country produces, the higher its cyber capacity is likely to be while controlling for other factors, […] S&T knowledge is a crucial resource for developing cybersecurity readiness*." (CALDERARO; CRAIG, 2020, p. 14).

[96] Reitera-se que o foco analítico da pesquisa é a América do Sul, no entanto, alguns dados e gráficos apresentados nesta trazem o contexto latino-americano já que não foi possível obter os dados sul-americanos separadamente.

No que se refere ao investimento em C&T, o gráfico 7 apresenta um panorama do subcontinente. Os valores observados se referem à porcentagem do investimento em relação ao Produto Interno Bruto (PIB). É possível também comparar os dados dos países com a média de investimento da América Latina e o Caribe.

Gráfico 7 - Investimento em C&T entre 2010 e 2019 (porcentagem em relação ao PIB)



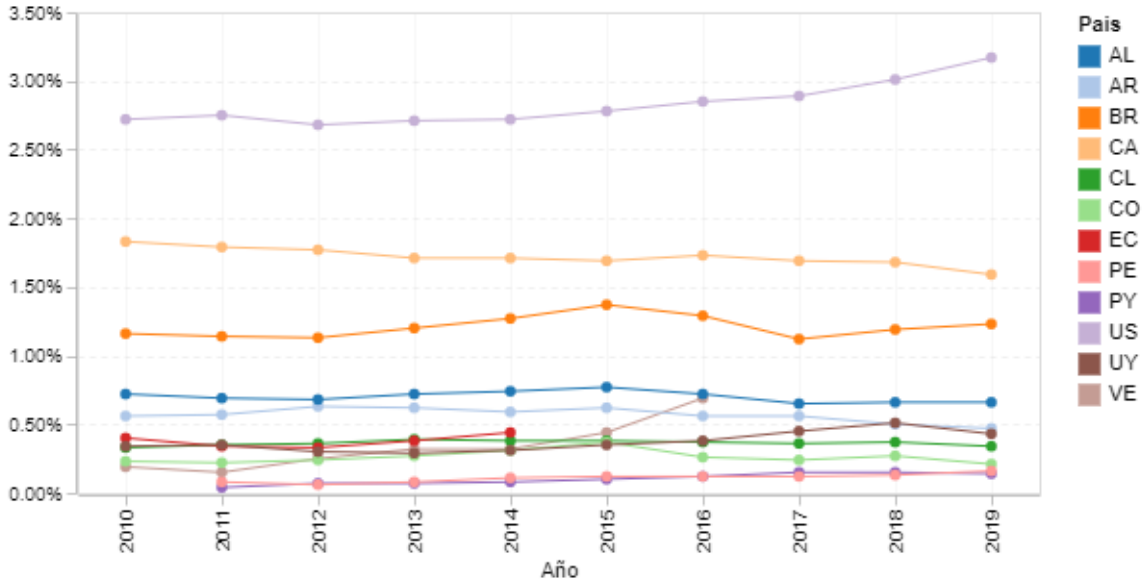
Fonte: RICYT (2023)
Legenda: AL – América Latina (média); AR – Argentina; BR – Brasil; CO – Colômbia; EC – EquadorPY – Paraguai; UY – Uruguai; VE - Venezuela

O gráfico 7 permite observar que entre 2015 e 2016 a Venezuela aumentou exponencialmente seus investimentos, estabelecendo-se, em 2016, como o país com maiores investimentos em C&T, correspondendo a 1,75% do seu PIB. Entretanto, não há dados mais recentes sobre os investimentos no país, não sendo possível analisar os parâmetros atuais. Diante disso, em 2019, Brasil foi o país da região com maior investimento no setor, uma vez que investiu 1,47% do seu PIB em C&T, tendo a maior porcentagem de investimento no ano de 2015, no qual investiu 1,73% do PIB em C&T. Por sua vez, Argentina investiu apenas 0,52% e Colômbia apenas 0,38% do seu PIB em C&T no ano de 2019. Esses dois países ficaram abaixo de países como Uruguai que investiu 0,76% e Paraguai, que investiu, nesse mesmo ano, 0,62% e da média geral da América Latina e o Caribe, a qual foi de 0,81%, em 2019.

Dentro do campo da C&T, a RICYT apresenta os dados referentes à Pesquisa e Desenvolvimento (P&D). O gráfico 8 reflete a realidade dos países sul-americanos nesse

contexto e possibilita comparar com os investimentos de Canadá e Estados Unidos nesse setor. Os dados são claros ao demonstrar a grande disparidade entre os países sul-americanos e esses países do norte do continente. Em 2019, enquanto EUA investiu em P&D 3,17% do seu PIB, o Brasil, país sul-americano com o maior investimento nesse setor, destinou apenas 1,23%. Depois do Brasil está a Argentina que destinou apenas 0,48% do seu PIB e Uruguai que investiu 0,43% em P&D.

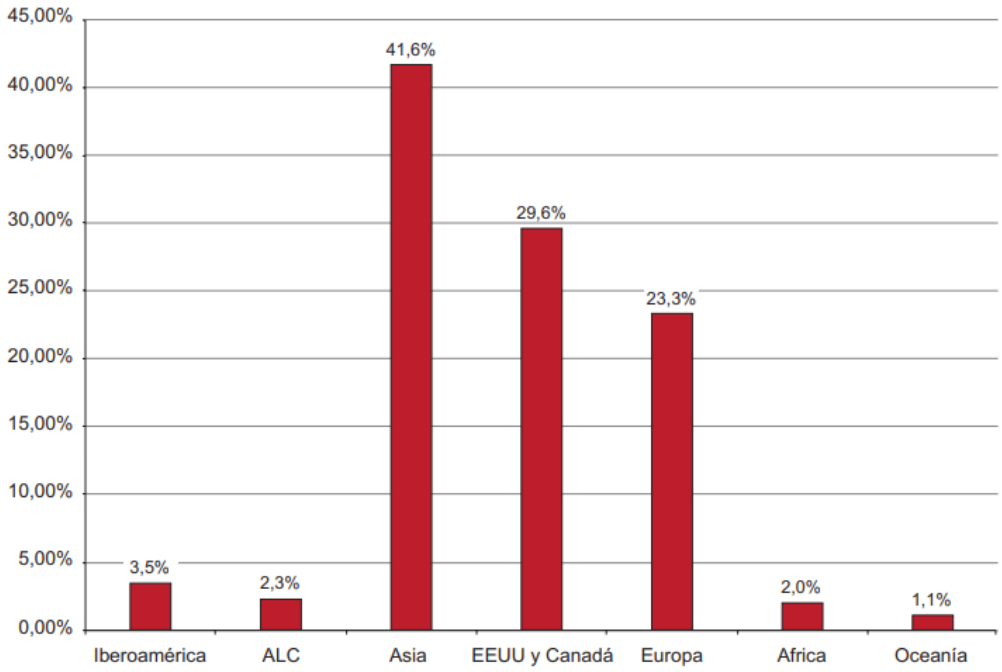
Gráfico 8 - Investimento em P&D entre 2010 e 2019 (porcentagem em relação ao PIB)



Fonte: RICYT (2023)
Legenda: AL – América Latina (média); AR – Argentina; BR – Brasil; CA – Canadá; CL – Chile; CO – Colômbia; EC – Equador; PE – Peru; PY – Paraguai; US – Estados Unidos; UY – Uruguai; VE - Venezuela

Observando os dados mundiais em relação aos investimentos e P&D, pode-se trazer uma análise comparativa entre algumas regiões do globo. O gráfico 9 resume o cenário internacional nesses termos.

Gráfico 9 - Distribuição do investimento mundial (em dólares) em P&D por blocos geográficos (2020)

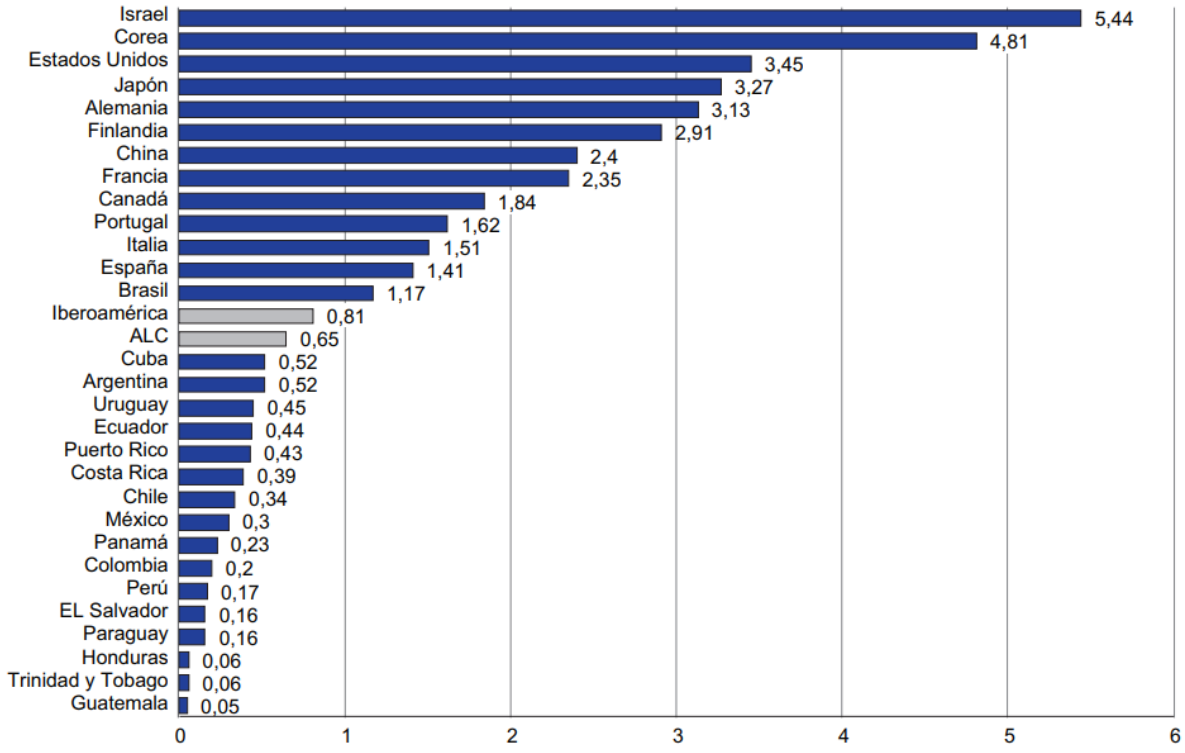


Fonte: RICYT (2022, p. 17)

Pode-se identificar que o investimento em P&D médio da América do Sul representa 2,3% do valor total investido no mundo, sendo que, Brasil, México e Argentina concentram 84% desse montante. Já os países asiáticos correspondem a quase 42% do investimento mundial; o investimento de Estados Unidos e Canadá corresponde a quase 30% do valor investido no mundo; e a Europa corresponde a pouco mais de 23% do investimento mundial (RICYT, 2022). A partir desses dados, pode-se ter a dimensão do atraso dos países da região nesse setor.

Entre os países que mais investem em P&D no mundo estão: Israel, investindo quase 5,5% em relação ao seu PIB; Coreia do Sul, com um investimento de 4,8%; Estados Unidos, com quase 3,5% do PIB investido em P&D; e Japão, com cerca de 3,3% de investimento. A China se configura na 7ª posição, com 2,4% em termos de investimento. Já o Brasil ficou na 13ª colocação, com um investimento de 1,17% do PIB em 2020 – tendo diminuído o investimento em relação a 2019. A Argentina ficou em 15º lugar, com 0,52% investido e Colômbia em 23º lugar, com apenas 0,2% investido em P&D (gráfico 10).

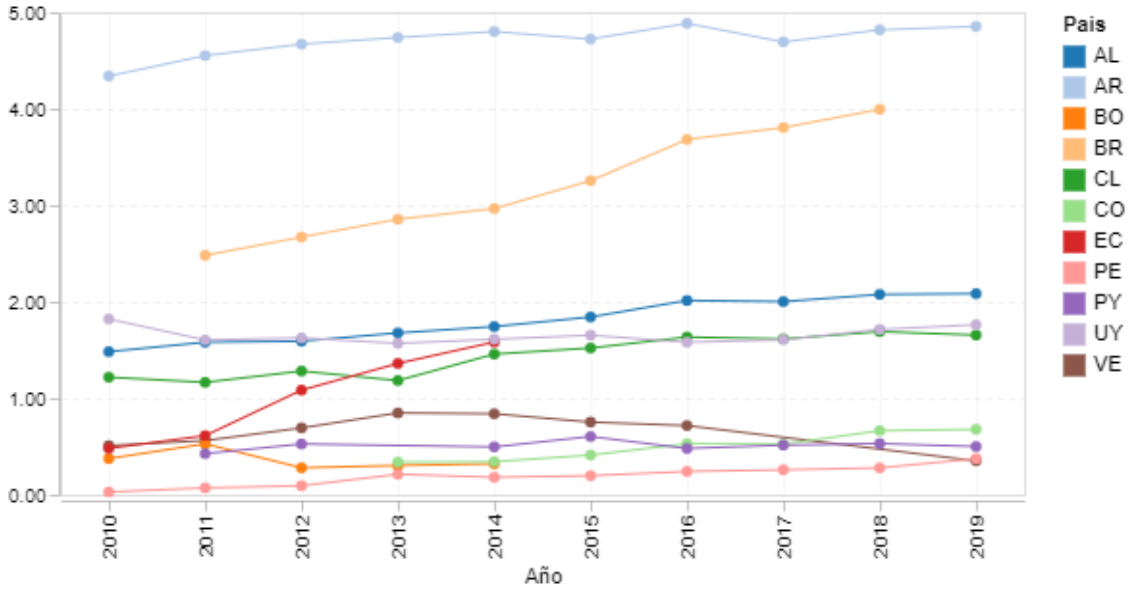
Gráfico 10 - Investimento em P&D em relação ao PIB em países e regiões selecionados (2020)



Fonte: RICYT (2022, p. 19)

Por outro lado, é interessante observar também, em termos de recursos humanos, a quantidade de pesquisadores na região. O gráfico 11 traz a quantidade de pesquisadores em relação à População Economicamente Ativa (PEA). Esse dado é estabelecido pelo número de pesquisadores, expresso em pessoas físicas, para cada 1.000 membros da força de trabalho dos países selecionados.

Gráfico 11 - Número de pesquisadores em relação à PEA (2010-2019)

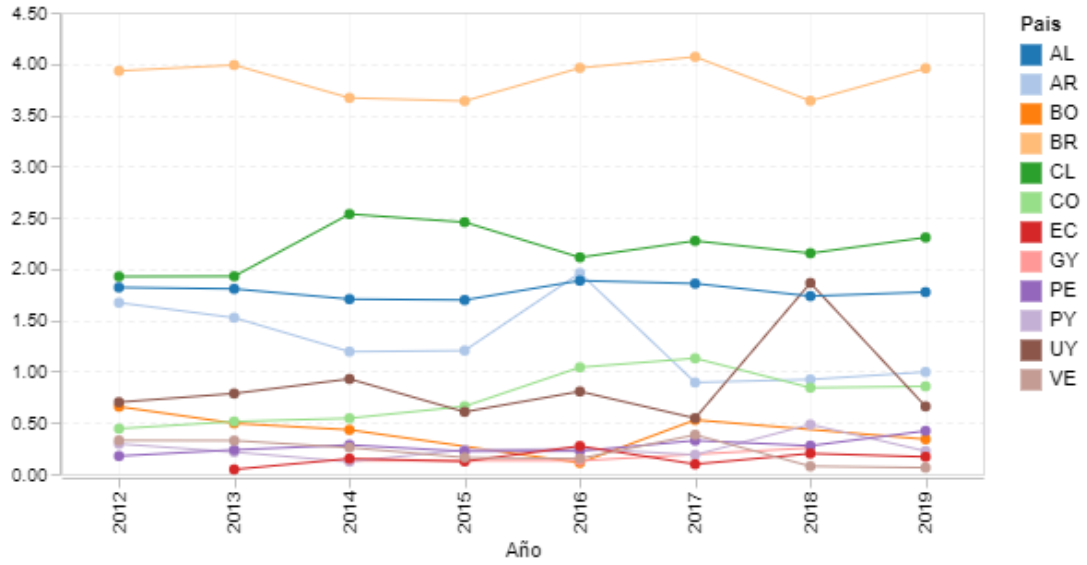


Fonte: RICYT (2023)
Legenda: AL – América Latina (média); AR – Argentina; BO – Bolívia; BR – Brasil; CL – Chile; CO – Colômbia; EC – Equador; PE – Peru; PY – Paraguai; UY – Uruguai; VE – Venezuela.

Os dados demonstram que a Argentina lidera na América do Sul, possuindo, em 2018, 4,82 pesquisadores a cada mil pessoas economicamente ativas, seguida por Brasil que possuía, nesse ano, 3,99 pesquisadores em relação a sua PEA. A título de comparação, em 2018, Portugal tinha 18,91 e Espanha contabilizava 10,30 pesquisadores a cada mil pessoas economicamente ativas (RICYT, 2023).

Por outro ponto vista, é possível analisar o coeficiente de invenção dos países, coeficiente estabelecido entre as patentes solicitadas pelos residentes e o total da população do país. O gráfico 12 demonstra que o Brasil possui o melhor coeficiente da América do Sul, seguido por Chile, Argentina e Colômbia. A título de comparação, em 2019, enquanto o coeficiente do Brasil fica em 3,96, o de Portugal é 6,78, o do Canadá é de 13,36, dos Estados Unidos é 86,84, demonstrando, novamente, a grande disparidade entre os países do Norte desenvolvido e os países sul-americanos (RICYT, 2023).

Gráfico 12 - Coeficiente de invenção (2012-2021)



Fonte: RICYT (2023)
Legenda: AL – América Latina (média); AR – Argentina; BO – Bolívia; BR – Brasil; CL – Chile; CO – Colômbia; EC – Equador; GY – Guiana; PE – Peru; PY – Paraguai; UY – Uruguai; VE - Venezuela

Percebe-se uma distribuição muito desigual entre os países sul-americanos em relação às suas capacidades e, particularmente, conforme apresentado nessa seção, em termos de ciência e tecnologia. Para mais, no que se refere aos investimentos em P&D, as disparidades entre esses países e os do Norte Global, no geral, são expressivas e, particularmente, as discrepâncias em relação aos países asiáticos é gigantesca. Considerando o contexto sul-americano apresentado e as discussões acerca da relevância do desenvolvimento de ciência e tecnologias nacionais para o processo de construção de capacidades, constata-se o grau de atraso da região nesse setor.

Retomando a discussão proposta no capítulo anterior, sobre os desafios enfrentados pela América Latina - particularmente, pela América do Sul -, Ceballos, Maisonnave e Londoño (2020, p. 152, tradução própria) destacam o papel da educação, do conhecimento, da formação de profissional e do desenvolvimento científico e tecnológico dos países para fazer frente às diversas ameaças digitais, mencionado, especialmente, o potencial antidemocrático das ferramentais digitais e as interferências externas na região através dessas ferramentas:

> As *fake news* e o *lawfare*, fenômenos plenamente presentes nas disputas latino-americanas, são apenas exemplos do potencial antidemocrático que as ferramentas digitais oferecem se não houver uma visão estratégica em torno delas. A colonialidade do poder e do saber faz com que em nossa época, enquanto as grandes potências priorizam sua autonomia digital na América Latina, os avanços neoliberais

> desfazem as políticas estatais de desenvolvimento nacional. Dessa forma, a formação de profissionais em tecnologia é negligenciada, eles são flexíveis à estrangeirização dos nossos sistemas tecnológicos e de gestão da informação e, na perspectiva de uma integração tecnológica regional essencial, carecem de projetos sustentáveis. (CEBALLOS; MAISONNAVE; LONDOÑO, 2020, p. 152, tradução própria).

Nesse sentido, os autores apontam ser essencial questionar:

> Por que destinar fundos à compra de produtos ou soluções de outros países que não partilham problemas, modelos ou políticas com a região? [...] Em que medida o suposto critério racional de poupança econômica que leva a não investir adequadamente em determinadas produções nacionais e/ou regionais prejudica a soberania tecnológica digital? (CEBALLOS; MAISONNAVE; LONDOÑO, 2020, p. 157, tradução própria).

Garantir a soberania digital, no entanto, dependeria da construção de capacidades cibernéticas pelos Estados e a diminuição da sua dependência externa, incluindo, portanto, o desenvolvimento dos fatores já mencionados. Entre os fatores necessários para a soberania digital, Ceballos, Maisonnave e Londoño (2020) citam educação e formação, democratização do conhecimento, desenvolvimento de P&D, financiamento público/privado nacional, regulação e ordenamento jurídico favorável à criação de um ecossistema tecnológico, produção de software e hardware, infraestrutura adequada, controle dos recursos naturais envolvidos. Ademais, defendem ser fundamental que, "como política de Estado, as patentes estratégicas para os desenvolvimentos latino-americanos não fiquem nas mãos exclusivas de interesses privados" (CEBALLOS; MAISONNAVE; LONDOÑO, 2020, p. 153, tradução própria).

Levando em consideração os pilares apontados pelos índices analisados e a lacuna de profissionais e de conhecimento na região, reitera-se ser prioritário promover educação cibernética e ampliar a formação e capacitação dos talentos. Esse processo é elementar para garantir o desenvolvimento das demais dimensões, sendo considerado pilar-chave para uma coerente estratégia nacional de segurança cibernética.

Diante disso, o Programa de Cibersegurança do Comitê Interamericano contra o Terrorismo da OEA desenvolveu relatório em que aponta para a necessidade de desenvolver um Plano de Ação de Educação em Segurança Cibernética (CEAP, do inglês *Cybersecurity Education Action Plan*), um plano para formular políticas públicas eficazes para fortalecer as estratégias nacionais e desenvolver os recursos humanos qualificados e necessários para a segurança e defesa cibernética nacional. O estabelecimento dos objetivos e metas deve levar

em consideração o contexto nacional para que o plano possa ser bem-sucedido, identificando metas específicas, mensuráveis e alcançáveis (OEA, 2020).

Esse plano deveria ser formulado no modelo de tríplice hélice (setor público, setor privado e academia), mapeando as partes interessadas em cada um dos setores. As metas devem perpassar o ensino fundamental e médio, ensino superior, cursos técnicos, educação continuada, conscientização em segurança cibernética, treinamentos, P&D e o desenvolvimento de ferramentas e técnicas necessárias para a efetiva implementação do plano (OEA, 2020).

> Por meio de universidades, grupos de reflexão e outras instituições acadêmicas, o meio acadêmico reúne múltiplos especialistas que, com suas pesquisas, continuam os avanços no campo da segurança cibernética. A integração de acadêmicos em parcerias público-privado-acadêmicas pode proporcionar análises objetivas, científicas e revisadas por pares para o desenvolvimento de políticas. O meio acadêmico pode muitas vezes ser a fonte de inovação e avanço de tecnologias. [...] A integração do setor acadêmico deve incentivar os formuladores de políticas a usarem os conselhos e dados disponíveis para construir políticas eficazes que possam assegurar a integração dos princípios de segurança cibernética na educação. E o que é ainda mais importante: estas são as entidades primárias que devem ser apoiadas financeiramente para continuarem inovando e avançando no trabalho de segurança cibernética e educação (OEA, 2020, p. 18).

No ensino superior, as mais diversas áreas devem ser atualizadas para atender as demandas provenientes da Revolução Tecnológica, inclusive com maior incentivo à interdisciplinaridade. Cursos de graduação e pós-graduação na área se tornam cada vez mais essenciais - como o Curso Superior em Segurança e Defesa Cibernética da Escola Superior de Guerra (ESG) do Brasil e a pós-graduação em cibersegurança e ciberdefesa ofertada pela Escola Superior de Guerra da Colômbia e. Da mesma forma, cursos técnicos precisam ser ampliados, como os programas oferecidos pelo Serviço Nacional de Aprendizagem Industrial (SENAI), no Brasil, e do Serviço Nacional de Aprendizagem (SENA), na Colômbia, e deve haver o fortalecimento da formação continuada visando a atualização constante dos profissionais (OEA, 2020).

Apesar do destaque dado ao papel das universidades, centros de pesquisa e institutos de formação e especialização, o documento reafirma a necessidade de promover ações de base no ensino fundamental e médio, com incentivo aos docentes para a incorporação da temática nas salas de aula, estímulo para que os estudantes reflitam sobre cibersegurança, educando as novas gerações e trazendo incentivos para a carreira no setor. Ademais, faz-se necessário a

criação de uma cultura de segurança cibernética, conscientização dos profissionais de todas as carreiras e da população em geral, com campanhas de capacitação para atuarem de forma segura no ambiente digital (OEA, 2020).

Esse é um caminho necessário para a superação da dependência tecnológica e, de modo geral, de soluções externas para as demandas próprias dos países da região. Ainda, cabe frisar que:

> A STD [Soberania Tecnológica Digital] não é um estado permanente e irreversível; pode ser conquistado, preservado ou perdido. Isto implica considerar prioritária a educação tecnológica e a formação de especialistas; fornecer incentivos ao pessoal treinado para evitar que a sua migração para potências estrangeiras ou que os seus conhecimentos sejam aplicados apenas na esfera privada; apoiar com políticas públicas empresas de desenvolvimento tecnológico comprometidas com linhas estratégicas para nossas nações; coordenar com os países da região um sistema de patentes e propriedade intelectual que proteja a pesquisa e o desenvolvimento; e colocar o Estado num papel fundamental para a criação de contextos que favoreçam a soberania tecnológica digital, com intervenções diretas e indiretas enquadradas em paradigmas de direitos humanos para a autonomia e independência. (CEBALLOS; MAISONNAVE; LONDOÑO, 2020, p. 164, tradução própria).

Em suma, somando-se aos dados analisados na seção anterior que destacam o pilar educacional, de habilidades e conhecimentos, os países precisam criar estratégias que partam da base educacional, da conscientização de todas as camadas da sociedade e promover a formação e capacitação dos recursos humanos, garantindo o desenvolvimento de ciência e tecnologia nacional, para, a partir disso, aprimorar as outras dimensões necessárias à construção de capacidades cibernéticas. Com isso, diminuir sua dependência das soluções advindas das potências cibernéticas, melhorar sua segurança, aumentar suas margens de poder e proteger seu sistema democrático e sua população cada vez mais conectada e, portanto, vulnerável. Construir capacidades e desenvolver estratégicas coerentes para fazer frente às aceleradas mudanças do século XXI e às diversas ameaças que o ambiente cibernético continuará apresentando aos Estados.

Partindo das análises acerca do posicionamento dos países sul-americanos nesse campo da construção das capacidades cibernéticas, a seção final deste capítulo buscará compreender a estrutura institucional e o modo em que Argentina, Brasil e Colômbia estão se organizando e desenvolvendo suas políticas e estratégias cibernéticas, analisando alguns de seus pontos norteadores. Parte-se, essencialmente, dos documentos e dos dados disponíveis em sites oficiais, trazendo também algumas contribuições e pesquisas já realizadas sobre a temática.

4.3 PRINCIPAIS DIRECIONAMENTOS DAS POLÍTICAS E ESTRATÉGIAS CIBERNÉTICAS DE ARGENTINA, BRASIL E COLOMBIA: ESTRUTURA INSTITUCIONAL, DOCUMENTOS ESTRATÉGICOS E LEGISLAÇÕES EM MATÉRIA CIBERNÉTICA

A primeira seção deste capítulo dimensionou a construção de capacidades de Argentina, Brasil e Colômbia, examinando os aspectos em que se destacam e os que possuem maiores debilidades. A segunda seção analisou, especificamente, o panorama da pesquisa, da ciência e do desenvolvimento tecnológico nesses países, levando em consideração que este é fator considerado crucial na construção de capacidades cibernéticas. Partindo disso, esta seção apresentará a estrutura central da segurança e da defesa cibernética de Brasil, Argentina e Colômbia, identificará os principais documentos e legislações em matéria de cibersegurança e ciberdefesa e buscará compreender os alguns dos direcionamentos dados pelos países e suas percepções estratégicas em relação ao ciberespaço.

Ao analisar os documentos elencados, buscar-se-á identificar alguns elementos em especial, visando nortear a compreensão sobre as dinâmicas de cibersegurança e ciberdefesa dos países. São estes:

I) Com definem os principais conceitos da área e quais os objetivos e temáticas principais abordadas em suas documentações oficiais, de modo a entender as áreas e assuntos que estão sendo priorizados pelos países.

II) A estrutura institucional, observando os órgãos responsáveis e a criação de organismos específicos para o setor, bem como a coordenação e integração entre os diversos setores nacionais que contribuem nas áreas de segurança e defesa.

III) A relevância dada ao fator humano, em relação à educação cibernética, formação e capacitação dos recursos humanos do país e à produção científica e tecnológica.

IV) Como entendem o ciberespaço, os recursos e as ameaças cibernéticas em suas estratégias de segurança e defesa – por exemplo, se enfatizam a dimensão dos conflitos, se compreendem a interdependência entre os países, se identificam tais recursos como novas oportunidades para o desenvolvimento, aumento de poder e de ascensão internacional e, principalmente, se ou como sinalizam para possibilidades de cooperação no setor,

particularmente com o entorno geográfico, e que significância essas estratégias cooperativas têm para os países.

Assim, antes de passar para uma análise individual dos países, para iniciar a discussão proposta nesta seção, faz-se necessário comparar como os países definem em seus documentos oficiais alguns conceitos para a área ciber. Essa foi a primeira etapa da análise dos documentos dos países ao realizar esta pesquisa. Essa etapa é essencial, visto que os conceitos que contornam o ciberespaço não possuem definições universalmente aceitas e a forma como os Estados os definem, ou se não os definem, pode orientar sobre seu entendimento e perspectivas de atuação nesse ambiente.

Brasil e Argentina possuem glossário específico que auxilia na compreensão dos termos utilizados em seus documentos estratégicos. O Brasil possui um amplo glossário sobre termos de segurança e defesa, o Glossário das Forças Armadas, publicado em 2015, e o Glossário de Segurança da Informação do Gabinete de Segurança Institucional (GSI), publicado em 2019. Da mesma forma, a Argentina possui o Glossário de Termos de Cibersegurança, publicado em 2019, no entanto, este é bem limitado, não constando diversos termos, principalmente os que perpassam a área de defesa. Ambos os países trazem algumas definições também em outros documentos oficiais e legislações. A Colômbia, por sua vez, não possui um glossário, estando alguns termos definidos ao longo dos documentos consultados ou ao final desses.

O quadro 6 apresenta as definições propostas pelos países nos documentos consultados, a partir dos termos selecionados para esta pesquisa.

Quadro 6 - Conceitos apresentados nos documentos de Argentina, Brasil e Colômbia

Termo	País	Definição
Espaço cibernético / Ciberespaço / *Ciberespacio*	**Argentina**	"O ambiente complexo que resulta da interação de pessoas, softwares e serviços na Internet por meio de dispositivos e redes conectados. Não tem existência física, mas é um domínio virtual que engloba todos os sistemas de TICs." (Argentina, 2019e, p. 4, grifo nosso)
	Brasil	"Espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente." (Brasil, 2019, p. 10). "Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas. [...] o espaço cibernético pode ser descrito em três camadas inter-relacionadas: a) Camada de Física; b) Camada de Lógica; e c) Camada de Ciberpersona." (Brasil, 2023, p. 14, grifo nosso)
	Colômbia	"É o ambiente físico e virtual composto por computadores, sistemas computacionais, programas de computador (softwares), redes de telecomunicações, dados e informações que são utilizados para interação entre os usuários." (Colômbia, 2011, p. 38, grifo nosso).
Segurança cibernética / Cibersegurança / *Ciberseguridad*	**Argentina**	"A preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço." (Argentina, 2019e, p. 4, grifo nosso)
	Brasil	"Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis." (Brasil, 2019, p. 20, grifo nosso)
	Colômbia	"É entendida como a capacidade do Estado de minimizar o nível de risco a que estão expostos os seus cidadãos, face a ameaças ou incidentes de natureza cibernética, procurando a disponibilidade, integridade, autenticação, confidencialidade e não repúdio das interações digitais. A Cibersegurança visa proteger os utilizadores e ativos do Estado no Ciberespaço e inclui o conjunto de recursos, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de risco, ações, investigação e desenvolvimento, formação, melhores práticas, seguros e tecnologias que podem ser utilizadas para este propósito." (Colômbia, 2020, p. 43, grifo nosso).
Defesa cibernética / Ciberdefesa / *Ciberdefensa*	**Argentina**	"As ações e capacidades desenvolvidas pelo Ministério de Defesa, pelo Estado Maior Conjunto e pelas Forças Armadas para antecipar e prevenir ataques cibernéticos e exploração cibernética de redes nacionais que possam afetar o Ministério de Defesa e o Instrumento Militar de Defesa Nacional, bem como Infraestruturas Críticas operacionais de apoio a Serviços Essenciais de interesse para a Defesa ou Infraestruturas operacionais de apoio a processos industriais de fabricação de bens sensíveis para a Defesa ou que

[continua...]

[continuação]

		possibilitem o acesso aos ativos digitais estratégicos atribuídos a sua custódia.” (Argentina, 2019b, p. 5, grifo nosso)
	Brasil	“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. 84, grifo nosso) “Ações 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 ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente.” (Brasil, 2023, p. 13, grifo nosso).
	Colômbia	“Capacidade do Estado para prevenir e combater 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 capacidades militares contra ameaças cibernéticas, ataques cibernéticos ou atos hostis de natureza cibernética.” (Colômbia, 2020, p. 42, grifo nosso).
Poder cibernético / Ciberpoder	**Argentina**	Não foi encontrada uma definição.
	Brasil	“Capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder.” (Brasil, 2015, p. 211)
	Colômbia	Não foi encontrada uma definição.
Capacidade cibernética / Cibercapacidades	**Argentina**	Não foi encontrada uma definição.
	Brasil	Definição exposta na Doutrina Militar de Defesa Cibernética: “é a aptidão para emprego de ações cibernéticas implementadas para criar efeito no espaço cibernético ou por meio dele.” (Brasil, 2023, p. 13, grifo nosso).
	Colômbia	Capacidade em segurança digital: “o conjunto de qualidades e aptidões de um país que lhe permitem gerar um ambiente adequado para abordar, gerar conhecimento e aumentar o grau de desenvolvimento em termos de segurança digital [...]” (Colombia, 2020, p. 16, grifo nosso)
Ameaça cibernética / Ciberameaça/ *Ciberamenaza / Amenaza Informática*	**Argentina**	“Ameaça: circunstância desfavorável que pode ocorrer e que quando ocorre tem consequências negativas sobre os ativos provocando a sua indisponibilidade, funcionamento incorreto ou perda de valor. Uma ameaça pode ter causas naturais, ser acidental ou intencional.” (Argentina, 2019e, p. 1) “Ameaça cibernética: ameaça a sistemas e serviços presentes no ciberespaço ou acessíveis através dele.” (Argentina, 2019e, p. 3)
	Brasil	“Causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse.” (Brasil, 2019, p. 8)
	Colômbia	“Aparição de uma situação potencial ou atual, onde um agente tem a capacidade de gerar uma agressão cibernética contra a população, o território e a organização política do Estado” (Colômbia, 2016, p. 87).

[continua...]

[continuação]

Crime Cibernético / Cibercrime / *Delito cibernético* / *Ciberdelito*	**Argentina**	Não foi encontrada uma definição.
	Brasil	"Ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro." (Brasil, 2015, p. 27)
	Colômbia	"Uma atividade ilegal ou abusiva conectada com as redes de computadores ou comunicações, por meio do qual um computador é usado como uma ferramenta para cometer a ofensa ou o alvo da ofensa é um sistema de computador (ou seus dados)." (Colômbia, 2011, p. 38).
Ataque cibernético / Ciberataque	**Argentina**	"Ação produzida no ciberespaço que comprometa a disponibilidade, integridade e confidencialidade da informação através de acesso não autorizado, modificação, degradação ou destruição dos sistemas de informação e telecomunicações ou das infraestruturas que os suportam." (Argentina, 2019e, p. 3).
	Brasil	"Ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais em dispositivos e redes computacionais e de comunicações do oponente." (Brasil, 2015, p. 39). "[...] é uma ação não cinética, executada como parte de uma operação militar que abrange as dimensões física e informacional." (Brasil, 2023, p. 15, grifo nosso).
	Colômbia	"Ação organizada e/ou premeditada por uma ou mais pessoas para causar danos ou problemas a um sistema informático através do ciberespaço." (Colômbia, 2011, p. 38).
Espionagem cibernética / Ciberespionagem *Espionaje cibernético* / *Ciberespionaje*	**Argentina**	Não foi encontrada uma definição.
	Brasil	"Atividade que consiste em ataques cibernéticos dirigidos contra a confidencialidade de sistemas TIC com o objetivo de obter dados e informações sensíveis a respeito de planos e atividades de um governo, instituição, empresa ou pessoa física, sendo geralmente lançados e gerenciados por serviços de inteligência estrangeiros ou por empresas concorrentes." (Brasil, 2019, p. 11, grifo nosso)
	Colômbia	"É o ato ou prática de obter segredos sem a permissão do dono da informação (pessoal, sensível, privada ou de natureza classificada) para vantagem pessoal, econômica, política ou militar no espaço cibernético, através do uso de técnicas mal-intencionadas." (Colômbia, 2016, p. 88, grifo nosso).
Terrorismo cibernético / Ciberterrorismo	**Argentina**	Não foi encontrada uma definição.
	Brasil	"Crime cibernético perpetrado por razões políticas, religiosas ou ideológicas contra qualquer elemento da infraestrutura cibernética com os objetivos de: provocar perturbação severa ou de longa duração na vida pública; causar danos severos à atividade econômica com a intenção de intimidar a população; forçar as autoridades públicas ou uma organização a executar, a tolerar, a revogar ou a omitir um ato; ou abalar ou destruir as bases políticas, constitucionais, econômicas ou sociais de um Estado, organização ou empresa. É principalmente realizado por atos de sabotagem cibernética organizados e gerenciados por indivíduos, grupos político-fundamentalistas, ou serviços de inteligência estrangeiros." (Brasil, 2019, p. 21, grifo nosso).

[continua...]

[continuação]

	Colômbia	"A convergência do terrorismo e do ciberespaço para atacar ilegalmente computadores, redes e informações neles armazenadas inclui violência contra pessoas ou bens ou, pelo menos, gera medo. Abrange assassinatos, explosões, poluição das águas ou grandes perdas econômicas, entre outras ações." (Colômbia, 2011, p. 39, grifo nosso).
Guerra cibernética / Ciberguerra	**Argentina**	Não foi encontrada uma definição.
	Brasil	"Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC." (Brasil, 2015, p. 134). "Atos de guerra utilizando predominantemente elementos de TIC em escala suficiente por um período específico de tempo e em alta velocidade em apoio a operações militares através de ações tomadas exclusivamente no espaço cibernético de forma a abalar ou incapacitar as atividades de uma nação inimiga, especialmente pelo ataque aos sistemas de comunicação, visando obter vantagem operacional militar significativa. Tais ações são consideradas uma ameaça à Segurança Nacional do Estado." (Brasil, 2019, p. 12, grifo nosso).
	Colômbia	Não foi encontrada uma definição.
Arma cibernética	**Argentina**	Não foi encontrada uma definição.
	Brasil	"Software, hardware e firmware projetado ou aplicado especificamente para causar dano através do domínio cibernético. Estão incluídas nessa categoria: ferramentas para acesso não autorizado, vírus, worms, trojans, DoS, DDoS, botnets e rootkits. Além disso, atividades como a engenharia social também são consideradas armas cibernéticas. Armas cibernéticas podem ser utilizadas individualmente ou em conjunto para aumentar os efeitos desejados." (Brasil, 2019, p. 3)
	Colômbia	Não foi encontrada uma definição.
Infraestruturas críticas	**Argentina**	"São aquelas indispensáveis ao funcionamento adequado dos serviços essenciais da sociedade, a saúde, a segurança, a defesa, o bem-estar social, a economia e o efetivo funcionamento do Estado, cuja destruição ou perturbação, total ou parcial, os afete e/ou tenha um impacto significativo." (Argentina, 2019e, p. 10).
	Brasil	"Instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança." (Brasil, 2019, p. 13).
	Colômbia	"É o conjunto de computadores, sistemas de computação, redes de telecomunicações, dados e informações, cuja destruição ou interferência pode enfraquecer ou impactar a segurança da

[continua...]

[continuação]

		economia, da saúde pública, ou da combinação delas, de uma nação.” (Colômbia, 2011, p. 39).
***Resiliência cibernética** / Resiliencia*	**Argentina**	“Capacidade de um sistema ou rede de se recuperar automaticamente de uma interrupção”. (Argentina, 2019e, p. 17)
	Brasil	“Capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa.” (Brasil, 2015, p. 241)
	Colômbia	Não foi encontrada uma definição.
Governança da Internet / Governança cibernética / *Gobernanza de Internet*	**Argentina**	"É o desenvolvimento e aplicação pelos governos, setor privado e sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomada de decisão e programas comuns que moldam a evolução e o uso da Internet." (Argentina, 2019e, p. 8)
	Brasil	A E-ciber apresenta ao longo do seu texto: “a governança cibernética abrange o desenvolvimento e a aplicação de princípios comuns, de normas, de procedimentos e de programas que moldam a evolução e o uso das ferramentas digitais. [...] A governança na área cibernética está relacionada às ações, aos mecanismos e às medidas a serem adotados com o fim de simplificar e modernizar a gestão dos recursos humanos, financeiros e materiais, e acompanhar o desempenho e avaliar os resultados dos esforços empreendidos nesse campo. Essa governança visa incorporar elevados padrões de conduta em segurança cibernética, e orientar as ações de agentes públicos e de agentes privados, ao considerar o papel que exercem em suas organizações, conforme a finalidade e a natureza de seu negócio. Inclui, ainda, o planejamento voltado à execução de programas, de projetos e de processos, e o estabelecimento de diretrizes que irão nortear a gestão de riscos. Nesse contexto, orienta pessoas e organizações quanto à observância das normas, dos requisitos e dos procedimentos existentes em segurança cibernética.” (Brasil, 2020, p. 12-13).
	Colômbia	Não foi encontrada uma definição.
Diplomacia cibernética / Ciberdiplomacia	**Argentina**	“É a diplomacia posta ao serviço da cooperação e da criação de regras para o ciberespaço.” (Argentina, 2019e, p. 4).
	Brasil	Não foi encontrada uma definição.
	Colômbia	Não foi encontrada uma definição.

Fonte: elaboração própria com base nos documentos mencionados.

É possível observar que alguns termos não são definidos pelos três países. Sobre isso cabe pontuar algumas questões. Dos 16 termos destacados, a Argentina não possui definição para 7, apesar de alguns desses conceitos serem mencionados ao longo dos documentos analisados. Particularmente, é interessante observar que menciona o termo ‘guerra eletrônica’ e ‘ciberguerra’ em seu Livro Branco e ‘guerra eletrônica’, ‘guerra cibernética’ e guerra híbrida’ em sua Política de Defesa Nacional, mas não há definições para esses termos. Também não foram encontradas definições para ciberdelito ou cibercrime, ciberterrorismo,

ciberespionagem, arma cibernética, poder cibernético e capacidade cibernética. A Colômbia também não traz definições para os termos ciberpoder, ciberguerra, ciberarma, diplomacia cibernética e governança cibernética ou termos que poderiam ser similares.

A não definição de termos relevantes, como os mencionados, ou a carência de definições precisas para a atuação dos Estados nesse setor, pode resultar em formulação de políticas e estratégicas inadequadas. Por outro lado, a não divulgação do entendimento dos Estados sobre conceitos importantes pode abrir espaço para manipulação desses conceitos a partir de interesses estatais específicos, ou seu uso como ferramenta retórica em discursos, além de gerar incertezas quanto à atuação do país no campo cibernético, podendo causar desconfianças por parte de outros atores.

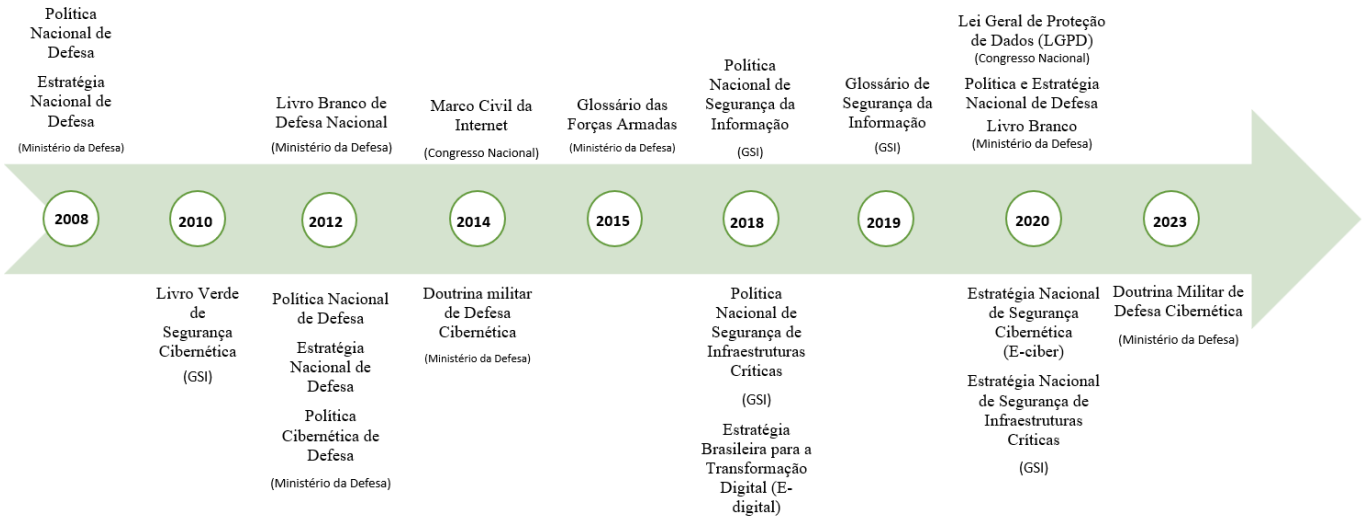
A partir dessa análise inicial, as próximas subseções buscarão compreender os outros elementos mencionados, partindo principalmente das legislações, documentos e sites oficiais. Cabe destacar que a documentação apresentada não corresponde a totalidade das legislações e documentos oficiais dos países sobre as temáticas, já que existe uma grande quantidade de documentação sobre temas afins ou desenvolvidas por outros órgãos dos Estados e relacionadas de alguma forma à temática. Os documentos apresentados são os que foram analisados nesta pesquisa e sobre os quais a seção se debruçará, buscando compreender alguns direcionados das políticas e estratégias nacionais dos Estados em relação à temática ciber.

4.3.1 Brasil

O Brasil é considerado pioneiro na América do Sul ao elencar o setor cibernético como estratégico para a Defesa Nacional - juntamente com o setor nuclear e o setor espacial – em seus documentos de defesa de 2008. Partindo disso, no campo da defesa, foram publicados o Livro Branco de Defesa Nacional (LBDN), a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) que mencionam o setor cibernético como decisivo para garantir a defesa do país - os quais foram atualizados em 2012, 2016 e 2020. Especificamente sobre ciberdefesa, o Brasil possui, como principais documentos, a Política Cibernética de Defesa (PCD) e a Doutrina Militar de Defesa Cibernética (DMDC). A defesa cibernética, de responsabilidade militar, fica a cargo do Ministério da Defesa, particularmente do Comando de Defesa Cibernética (ComDCiber), como poderá ser visto adiante na estrutura institucional.

A segurança cibernética, por seu turno, fica sob responsabilidade do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). No que se refere à segurança cibernética – e, de modo mais amplo, a segurança da informação[97] -, o principal documento, atualmente, é a Estratégia Nacional de Segurança Cibernética (E-Ciber), que se soma ao Livro Verde de Segurança Cibernética, escrito ainda em 2010. Além disso, tem-se a Política Nacional de Segurança da Informação (PNSI), a Política Nacional de Segurança das Infraestruturas Críticas (PNSIC) e a Estratégia Nacional de Segurança das Infraestruturas Críticas (ENSIC) e, no âmbito legislativo, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD).

Figura 6 – Linha do tempo: Principais documentos sobre segurança e defesa cibernética do Brasil



Fonte: elaboração própria.

Ainda em 2010, a publicação do Livro Verde: Segurança Cibernética do Brasil, visava iniciar o debate sobre o tema da cibersegurança no Brasil. O documento tinha por objetivo expressar diretrizes estratégicas para direcionar o estabelecimento de uma política de segurança cibernética brasileira, oferecendo uma contextualização sobre a temática, evidenciando as tendências e apresentando desafios e oportunidades na área. No documento já

[97] Em sentido mais amplo, "a Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade." (BRASIL, 2020, p. 2).

se mencionava, entre os requisitos essenciais para a segurança cibernética do país, adotar políticas e normas específicas com objetivos claros, promover e educação cibernética, garantir medidas para aceleração de pesquisas e inovações no setor, coordenar as atividades entre os setores público e privado e estabelecer acordos de cooperação bilaterais e multilaterais, em nível regional e internacional, para favorecer a troca de experiências e fortalecer a segurança nacional. Também mencionava a formulação da Política Nacional de Segurança das Infraestruturas Críticas e o mapeamento das vulnerabilidades dos sistemas de informação e das IC do país, de modo a definir os requisitos de segurança e desenvolver um sistema de monitoramento de ameaças cibernéticas (MANDARINO JÚNIOR; CANONGIA, 2010).

Partindo disso, em 2018, é instituída a Política Nacional de Segurança da Informação (PNSI), por meio do Decreto 9.637/2018. Segundo o artigo 2º da PNSI, a segurança da informação abrange: "I - a segurança cibernética; II - a defesa cibernética; III - a segurança física e a proteção de dados organizacionais; e IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação." Assim, devido à abrangência da Segurança da Informação, a PNSI indicou que a ENSI seria construída em cinco módulos: I - segurança cibernética; II - defesa cibernética; III - segurança das infraestruturas críticas; IV - segurança da informação sigilosa; e V - proteção contra vazamento de dados (BRASIL, 2018, art. 6º).

Considerando a segurança cibernética "como a área mais crítica e atual a ser abordada", o GSI definiu a Estratégia Nacional de Segurança Cibernética (E-Ciber) como primeiro módulo da ENSI, contando com a colaboração de mais de 40 órgãos e entidades do Governo, instituições privadas e do setor acadêmico (BRASIL, 2020c, p. 1). Assim, a E-Ciber foi publicada em 2020, configurando-se como o principal documento de cibersegurança do país.

A E-Ciber visa preencher uma lacuna normativa sobre a temática da segurança cibernética no país e "estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto." (BRASIL, 2020c, p. 2). Atenta para a fragmentação das iniciativas existentes no setor e identifica a falta de um arcabouço normativo, estratégico e operacional alinhado no país, o que dificulta ações coordenadas para enfrentar os desafios e prejudica a absorção de conhecimento e experiência ao longo do tempo.

A E-Ciber evidencia sobre a necessidade de construção de capacidades cibernéticas quando afirma que para proteger o ciberespaço é fundamental adaptação contínua nos âmbitos

políticos, tecnológicos, educacionais, legais e internacionais. Partindo disso, a E-Ciber elenca o que denomina de Eixos de Proteção de Segurança e Eixos Transformadores. Para essa definição, o documento leva em consideração o CCMM do GCSCC e suas cinco dimensões, considerando-as como suficientemente abrangentes para analisar o processo de construção de capacidades, compreender a maturidade e as necessidades do país nesse âmbito. Assim, foram definidos 7 eixos de atuação para a Estratégia do país. São estes:

Eixos de Proteção de Segurança:

- Governança da segurança cibernética nacional;
- Universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas;
- Proteção estratégica;

Eixos Transformadores[98]:

- Dimensão normativa;
- Dimensão internacional e parcerias estratégicas;
- Pesquisa, desenvolvimento e inovação; e
- Educação.

A partir disso, além de trazer o contexto da segurança cibernética do Brasil, são definidos objetivos estratégicos e as ações estratégicas para alcançar tais objetivos, visando garantir um ambiente cibernético mais próspero, seguro e resiliente, fortalecer a atuação brasileira nesse campo no cenário internacional e, com isso, melhorar as condições para o crescimento econômico e o desenvolvimento social do país (BRASIL, 2020c). São 10 as ações estratégicas:

I) Fortalecer as ações de governança cibernética;

II) Estabelecer um modelo centralizado de governança no âmbito nacional;

III) Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade;

IV) Elevar o nível de proteção do Governo;

V) Elevar o nível de proteção das Infraestruturas Críticas Nacionais;

VI) Aprimorar o arcabouço legal sobre segurança cibernética;

VII) Incentivar a concepção de soluções inovadoras em segurança cibernética;

[98] A E-ciber define que são denominados como Eixos Transformadores "pelo potencial que possuem em modificar, de forma decisiva e estruturante, os temas por eles influenciados" (BRASIL, 2020c, p. 12).

VIII) Ampliar a cooperação internacional do Brasil em segurança cibernética;

IX) Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade;

X) Elevar o nível de maturidade da sociedade em segurança cibernética (BRASIL, 2020c).

Contornando os eixos e as ações estratégicas previstas pela E-Ciber cabem algumas considerações. Sobre a governança cibernética nacional, o documento dedica-se a explicá-la e propõe que esta deve orientar os direitos, as obrigações e as responsabilidades dos diversos segmentos da sociedade, estabelecer princípios, normas, procedimentos, criar estruturas, mecanismos e medidas, possibilitando a atuação coordenada entre os atores estatais e não estatais de interesse, propiciar o compartilhamento de informações e soluções, otimizar os recursos disponíveis e alinhar o planejamento estratégico, doutrinário e operacional (BRASIL, 2020c).

Sobre a atuação conjunta entre setores público, privado, academia e sociedade em geral, esta é considerada essencial para a segurança cibernética, "uma vez que, como o tema é transversal, os melhores resultados somente serão alcançados se todos agirem de forma coordenada, sempre cientes de que nenhum ator poderá, de forma isolada, enfrentar com todos os desafios impostos pelas novas tecnologias." (BRASIL, 2020c, p. 29). Além disso, a gestão de riscos é definida como um dos principais elementos que sustentam a governança cibernética, "uma vez que indica a adoção de melhores políticas e metodologias, o que permite gerir, de forma otimizada, os limites aceitáveis de risco", além de desenvolver ferramentas para que as vulnerabilidades possam ser conhecidas e, assim, os pontos críticos possam ser protegidos (BRASIL, 2020c, p. 13).

A E-Ciber define também que um modelo centralizado de governança deve ser adotado, conforme posto em prática por países como Estados Unidos, Reino Unido, Portugal, França, Índia, Singapura, Coréia do Sul e Japão. Nesse sentido, o GSI seria o organismo governamental que precisaria ser redimensionado para ser capaz de assumir esse papel centralizador das ações de governança nacional (BRASIL, 2020c).

Partindo disso, o documento menciona o papel fundamental da Pesquisa, Desenvolvimento e Inovação (PD&I), na área de segurança cibernética, entendendo como prioritário investir e incentivar a formação de investigadores capacitados, o desenvolvimento projetos e produção científica e tecnológica de alto nível, como nos moldes desenvolvidos por países líderes na área. Defende, ainda, a necessidade de investir em cursos de graduação e

pós-graduação e criar mecanismos para a colaboração entre universidades, institutos e centros de pesquisa, refletindo que a aproximação com a academia não deve ficar restrita aos cursos de computação aplicada, mas deve agregar outras áreas do conhecimento, o que "pode ser uma via eficaz para formação, aprimoramento e qualificação de pessoal interessado no tema, além de geração de conhecimento." (BRASIL, 2020c, p. 26).

Assim, E-Ciber recomenda também o estabelecimento de parcerias com o Ministério da Educação para implementar projetos em todos os níveis educacionais, inclusive na educação básica, de modo a promover a educação digital, desenvolver uma cultura de segurança cibernética e identificar e capacitar talentos que possam vir a ser recrutados (BRASIL, 2020c). Frisa, ademais, ser crucial, além de formar recursos humanos qualificados, ser capaz de reter os talentos e profissionais capacitados para contribuir com os setores nacionais (BRASIL, 2020c).

Sobre a educação cibernética, esta é compreendia a partir de 3 níveis:

- Capacitação - profissionais da área ou com funções que requerem competências específicas, sejam professores, gestores ou outros profissionais;
- Formação – para os indivíduos em formação ao promover cursos em todos os níveis e a inserção da temática nos currículos escolares; e
- Conscientização – em todos os setores da sociedade, todas as faixas etárias e classes sociais, através da instituição de políticas públicas, promoção de campanhas e divulgação de boas práticas.

No que se trata de cooperação internacional, esta também é destacada ao longo da E-ciber. O documento ressalta que:

> [...] a segurança cibernética é assunto global em que se faz primordial a interação entre diversos atores da comunidade internacional para a construção de um ambiente digital seguro e confiável. Nesse sentido, recomenda-se que o País adote diretrizes que, por meio de medidas de construção de confiança, visem à cooperação interestatal, ao intercâmbio intenso de informações, à transparência, à previsibilidade de ações, à reafirmação da paz internacional e à estabilidade, de modo a corroborar para reduzir o risco da escalada de incidentes cibernéticos em âmbito global (BRASIL, 2020c, p. 28).

Diante disso, é fundamental a participação nos organismos e fóruns internacionais de modo a colaborar nas iniciativas de estabelecimento de normativas, elaboração de procedimentos para colaboração, compartilhamento de informações, combate ao crime e

ações agressivas no ciberespaço e contribuir na resolução de possíveis crises. Ademais, aponta-se para as oportunidades comerciais advindas da cooperação internacional no âmbito da segurança cibernética. Por fim, a E-Ciber menciona a necessidade de maior integração entre o Brasil e os países latino-americanos, sem mencionar especificamente a América do Sul em nenhum momento (BRASIL, 2020c).

Em 2020 também foi aprovada a Estratégia Nacional de Infraestruturas Críticas (ENSIC) e, em 2022, o Plano Nacional de Segurança de Infraestruturas Críticas, partindo da Política Nacional de Infraestruturas Críticas (PNIC), instituída em 2018. Os documentos visam garantir a segurança e a resiliência das IC do país, assim como a continuidade da prestação de seus serviços, através, principalmente, do esforço contínuo para o aperfeiçoamento dessas infraestruturas, identificação das ameaças e das vulnerabilidades e o estabelecimento de medidas de controle e redução de riscos (BRASIL, 2020d).

Nesse sentido, são definidos como eixos estruturantes da ENSIC: articulação institucional; conscientização e capacitação; fomento às ações; gestão de dados e informações. Para cada eixo estruturante são elencados objetivos e iniciativas estratégicas. Cabe destacar que ela prevê que os prestadores de serviços - já que grande parte das IC estão no domínio privado -, os usuários e o Estado – nas suas diversas esferas e níveis - unam esforços para garantir a manutenção, o aperfeiçoamento e a segurança dessas IC, já que todos compartilham interesses para que tais IC funcionem de forma regular e segura. Para isso, propõe a instituição do Sistema de Governança de Segurança de Infraestruturas Críticas, compostos pelos órgãos e entidades do setor público e privado, proporcionando a atuação integrada e o compartilhamento de informações, além de outras ações relacionadas à conscientização, estabelecimento de diretrizes, elaboração de projetos, desenvolvimento de capacidades e outras iniciativas (BRASIL, 2020d).

Ainda, no marco legislativo brasileiro, cabe mencionar a implementação, por meio da Lei 12.965 de 23 de abril de 2014, do Marco Civil da Internet, conhecido como a Constituição da Internet no Brasil. O Marco Civil regula o uso da internet no país, ao estabelecer os "princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina(r) as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria" (BRASIL, 2014b, art. 1º). Estão entre seus objetivos e fundamentos o direito de acesso à internet, do acesso à informação, a proteção dos dados dos indivíduos, o respeito à privacidade, a liberdade de expressão, o exercício da cidadania no ambiente digital, responsabilização pelas ações realizadas no ambiente online, entre outros.

E, por fim, em 2020, entrou em vigor a LGPD, baseada no Regulamento Geral sobre a Proteção de Dados da União Europeia. A LGPD complementa o Marco Civil da Internet, com maiores especificações sobre a coleta, armazenamento, tratamento e comercialização dos dados pessoais, visando garantir a proteção dos direitos fundamentais, como liberdade, dignidade e privacidade, além de instituir a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2020e).

Já no que se trata da defesa cibernética, o LBDN, a PND e a END estabeleceram as bases para sua estruturação a partir de 2008. A partir dessas bases, foram elaborados documentos específicos sobre a temática e foram criados o Sistema Militar de Defesa Cibernética (SMDC) e outros organismos como o Centro de Defesa Cibernética (CDCiber), o Comando de Defesa Cibernético (ComDCiber), a Escola Nacional de Defesa Cibernética (EnaDCiber) e outros organismos e mecanismos para sustentar a defesa cibernética do país - os quais serão especificados adiante.

A END já apontava, em 2012, para a necessidade de desenvolver o aparato tecnológico do país assim como a formação de recursos humanos, estabelecer uma política de formação de cientistas para atuar na área cibernética com a aproximação entre a produção científica e as atividades relativas ao desenvolvimento tecnológico da Base Industrial de Defesa. Expõe como uma das prioridades fomentar a pesquisa científica e estruturar a produção de conhecimento na área. A formação qualificada e a aproximação entre a academia e o setor de defesa, em geral, se dariam a partir de instituições como a Escola Superior de Guerra (ESG), a EnaDCiber, Instituto Pandiá Calógeras e projetos como Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Defesa Nacional (Pró-Defesa) e do Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Assuntos Estratégicos de Interesse Nacional (Pró-Estratégia), por exemplo (BRASIL, 2012c).

A Política Cibernética de Defesa (PCD), aprovada no final de 2012 (e não mais atualizada), foi o primeiro documento estratégico formulado especificamente para o âmbito da defesa cibernética. A PCD foi formulada visando "orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos." (BRASIL, 2012b, p. 11). Entre os objetivos delimitados estão: capacitar os recursos humanos para atuarem no setor cibernética do MD; produzir conhecimentos de Inteligência; implementar atividades de pesquisa e desenvolvimento e adequar as estruturas de ciência,

tecnologia e inovação nacional; definir os princípios básicos que norteiam a criação de normas para o setor cibernético; conhecer as infraestruturas críticas nacionais; e contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no âmbito da segurança cibernética (BRASIL, 2012b).

Entre as propostas estão a criação de cargos para suprir as necessidades do setor cibernético nacional, selecionar pessoal com competências e habilidades, sejam internos ou externos às Forças Armadas, para atuarem no Sistema Militar de Defesa Cibernética (SMDC) que seria instituído, mantendo a capacitação desses recursos humanos. Seriam viabilizados cursos, seminários, exercícios de simulação ou outras atividades no Brasil e no exterior e fomentar-se-ia o desenvolvimento de teses, dissertações e outros trabalhos sobre a temática nas instituições civis e militares. A partir disso, também seriam estabelecidas parcerias e intercâmbios entre as Forças Armadas e outras instituições, bem como outras medidas de cooperação com as instituições de pesquisa civis e militares (BRASIL, 2012b).

No que se trata da cooperação internacional, a PCD menciona apenas, entre suas diretrizes, que irá "promover intercâmbio doutrinário, normativo e técnico, com instituições civis e militares, nacionais e de nações amigas." (BRASIL, 2012b, p. 16). Já os demais documentos de defesa de 2012 mencionavam em vários momentos a cooperação internacional e regional em matéria de defesa, destacando que o Brasil precisava buscar oportunidades de intercâmbio com seus principais parceiros, no entanto, sem especificar a cooperação na área ciber. Especificamente sobre a América do Sul, os documentos deixavam claro que a América do Sul era o entorno estratégico imediato do Brasil, sendo necessário, portanto, aprofundar os laços de cooperação com os países vizinhos, visando aumentar a confiança e favorecer o desenvolvimento de soluções negociadas para possíveis contenciosos que possam se formar na região (BRASIL, 2012c).

Defendia-se também a construção de uma identidade de defesa sul-americana e frisava-se que a estabilidade regional era prioridade para o país. Partia-se do entendimento da América do Sul como uma "comunidade de segurança", "motivada pelo fato de os países vizinhos compartilharem experiências históricas comuns, desafios de desenvolvimento semelhantes e regimes democráticos, que facilitam a compreensão recíproca e propiciam uma acomodação pacífica dos diversos interesses nacionais" (BRASIL, 2012a, p. 29)

Nesse sentido, estabelece ser necessário, entre outros posicionamentos, fortalecer a integração regional a partir do Mercosul e da Unasul, aprofundar a integração física na América do Sul, fomentar a cooperação militar e a integração das bases de defesa através do

CDS e estreitar o relacionamento com os países amazônicos por meio da Organização do Tratado de Cooperação Amazônica (OTCA) (BRASIL, 2012c). A PND, especificamente, afirmava que:

> A segurança de um país é afetada pelo grau de estabilidade da região onde ele está inserido. Assim, é desejável que ocorram o consenso, a harmonia política e a convergência de ações entre os países vizinhos para reduzir os delitos transnacionais e alcançar melhores condições de desenvolvimento econômico e social, tornando a região mais coesa e mais forte. [...] Como consequência de sua situação geopolítica, é importante para o Brasil que se aprofunde o processo de desenvolvimento integrado e harmônico da América do Sul, que se estende, naturalmente, à área de defesa e segurança regionais. (BRASI, 2012c, p. 22).

No que se trata das atualizações do LBDN, da PND e da END de 2020, os documentos se mostraram bem reduzidos e consideravelmente superficiais se comparados com as versões de 2012. O setor cibernético continua no tripé estratégico da Defesa Nacional nas versões mais recentes desses documentos e o LBDN pondera que a proteção do ciberespaço abrange diversas áreas, envolvendo "capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal" (BRASIL, 2020a, p. 47).

Fato interessante de se observar é que o LBDN menciona as possibilidades de guerras cibernéticas ocorrerem, enquanto na versão anterior do LBDN e mesmo nas versões da PND e na END de 2012, o termo era sequer mencionado.

> Entre os novos temas que apresentam implicações para a proteção da Soberania Nacional está a defesa cibernética. A possibilidade do surgimento de "guerras cibernéticas" no século XXI representa desafio importante para a Defesa Nacional e para a segurança internacional. A possibilidade de o País sofrer um ataque cibernético de origens das mais diversas e de difícil identificação, que poderão causar danos consideráveis a estruturas estratégicas ou mesmo a outros setores de importâncias vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter importância fundamental para a Defesa Nacional (BRASIL, 2020a, p. 23).

O documento também é mais sucinto ao falar da cooperação com o entorno geográfico sul-americano, mas mantém o discurso acerca da prioridade dada à América do Sul e à cooperação regional. A integração com os vizinhos é destacada como objetivo estratégico para manter a estabilidade e promover o desenvolvimento econômico e a paz na região, além de salientar que a cooperação em termos de defesa pode resultar em oportunidades importantes ao país. Aponta também para o intercâmbio acadêmico entre as

instituições de ensino do país e as dos parceiros sul-americanos. Não cita, entretanto, iniciativas de integração regional neste documento (BRASIL, 2020a).

A PND de 2020 destaca que "a convergência de interesses contribui para o incremento da cooperação entre os países sul-americanos, o que poderá promover a consolidação da confiança mútua e a execução de projetos de defesa". Essa cooperação visaria, principalmente, o desenvolvimento tecnológico e industrial, além da construção de estratégias para a solução de problemas comuns (BRASIL, 2020b, p. 17).

A END de 2020 enfatiza a necessidade colaboração entre o Setor de Defesa e a Base Industrial de Defesa, setores público e privado e o setor acadêmico, nacional e internacional, para ampliar as capacidades cibernéticas, devendo haver o fomento à "pesquisa, o desenvolvimento e a inovação, com foco nas tecnologias que permitam o planejamento e a execução das atividades Cibernéticas no âmbito do Setor de Defesa e que contribuam com a Segurança Cibernética no âmbito nacional". Além disso, ressalta a importância de intensificar as parcerias estratégicas e o intercâmbio com as Forças Armadas de outros países (BRASIL, 2020b, p. 60).

Sobre a diplomacia em defesa, a END entende que:

> A atividade diplomática estimula o conhecimento recíproco entre nações e permite a conciliação de eventuais diferenças de percepções. Portanto, o diálogo e a cooperação com outros países são fundamentais para o êxito da Estratégia Nacional de Defesa, por serem poderosos instrumentos de prevenção e de resolução de conflitos. Em um ambiente internacional cada vez mais complexo e de uma crescente interdependência entre as nações em diversos domínios, a diplomacia ganha cada vez maior importância no encaminhamento das grandes questões globais. (BRASIL, 2020b, p. 44).

Além disso, nos Objetivos Nacionais de Defesa (OND), a consolidação do setor cibernético é mencionada como ação estratégica para o fortalecimento do poder nacional, para o fortalecimento da capacidade de dissuasão e para o fortalecimento da área de ciência e tecnologia de defesa. Além disso, entre as ações estratégias de defesa estão a capacitação dos recursos humanos, a criação da carreira civil de defesa, o desenvolvimento de tecnologia cibernética, o incremento das relações diplomáticas com outros países, o incremento da temática de defesa no sistema de educação nacional, ampliação das iniciativas de apoio à pesquisa científica e tecnológica, o estímulo ao desenvolvimento de uma identidade sul-americana de defesa, a intensificação de parcerias estratégicas e iniciativas de cooperação e

intercâmbio militar com as Forças Armadas dos países vizinhos, bem como o incremento à participação do país em organismos e fóruns regionais e internacionais (BRASIL, 2020b).

Ainda, no âmbito da defesa cibernética, foi elaborada a Doutrina Militar de Defesa Cibernética, em 2014, sendo atualizada neste ano de 2023, conforma-se como o documento mais recente sobre a ciberdefesa do país. A Doutrina tem por objetivo proporcionar unidade de pensamento sobre cibernética no âmbito da Defesa Nacional e contribuir para a atuação conjunta das Forças Armadas na defesa dos interesses brasileiros no ciberespaço. Além disso, deixa claro que o Brasil reconhece o ciberespaço "como um domínio operacional, no qual ações cibernéticas ofensivas e defensivas tendem a potencializar ou complementar as ações realizadas nos demais domínios (terra, mar, ar e espaço)." (BRASIL, 2023, p. 12).

Interessante também observar que a DMDC define o ciberespaço a partir das três camadas, conforme apresentado no capítulo 1 desta tese. A camada física compreende os dispositivos e infraestruturas de tecnologias de informação, aquilo que possibilita o armazenamento, transporte e processamento das informações no ciberespaço. Essa camada, portanto, está ligada a uma localização geográfica, o que permite maior precisão sobre o enquadramento legal e, consequentemente, maior controle sobre as delimitações da soberania estatal (BRASIL, 2023). A camada lógica é compreendida como a "abstração da camada física podendo ser representada por aplicações, programas, serviços, protocolos que possibilitam o funcionamento e o tráfego de dados no espaço cibernético" (BRASIL, 2023, p. 15). Já a denominada camada ciberpersona é:

> [...] formada pelas representações das identidades virtuais dos usuários da rede (ciberpersonas). Essas identidades virtuais podem ser uma conta em um serviço online. O uso de ciberpersonas pode tornar a atribuição de responsabilidades pelas ações cibernéticas difícil, fator preponderante que caracteriza a complexidade dessa camada, com elementos em muitas localizações virtuais que não compartilham uma única localização ou forma física. Desse modo, sua identificação requer uma considerável coleta e análise de Inteligência para permitir uma seleção de alvos efetiva ou para criar o efeito desejado dentro do contexto de uma operação militar. (BRASIL, 2023, p. 15).

A DMDC também apresenta as características da defesa cibernética, as quais são:

- Insegurança latente – já que nenhum sistema computacional é totalmente seguro e as ameaças são constantes;
- Alcance global – entendendo que os limites físicos e geográficos não se aplicam ao ciberespaço;

- Vulnerabilidade das fronteiras geográficas – decorrente da característica anterior;
- Mutabilidade – as ações cibernéticas estão em constante adaptação e desenvolvimento a partir da criatividade humana;
- Incerteza – ações cibernéticas podem gerar efeitos não pretendidos inicialmente, devido às diversas variáveis envolvidas;
- Dualidade – as mesmas ferramentas cibernéticas podem ser utilizadas para operações ofensivas ou defensivas;
- Paradoxo tecnológico – o maior desenvolvimento tecnológico gera maior dependência das TICs e, consequentemente, maior será a vulnerabilidade do país frente às ações cibernéticas. Paradoxalmente, o maior grau de desenvolvimento tecnológico garante melhores condições de defesa;
- Dilema de segurança – a dúvida existente sobre "a busca ou não da correção de uma vulnerabilidade identificada em um determinado sistema, uma vez que a correção tornará mais eficiente a sua defesa, enquanto a não correção aumenta a capacidade de ataque a sistemas congêneres de posse de um eventual oponente" (BRASIL, 2023, p. 15); e
- Assimetria - desbalanceamento de forças entre Estados ou organizações com maiores condições econômicas para introduzir melhores elementos tecnológicos, metodológicos ou procedimentais.

Sobre cooperação, a DMDC apenas menciona, entre as possibilidades de ação, a cooperação com a Segurança Cibernética, seja com órgãos internos e externos ao MD, "mediante solicitação ou no contexto de uma operação" e que irá cooperar para "a produção do conhecimento de Inteligência por meio da Fonte Cibernética", sem especificar como se daria essa cooperação ou os níveis dessas iniciativas de cooperação (BRASIL, 2023, p. 15). Adicionalmente, o documento ressalta que, diante das particularidades do ciberespaço, o cumprimento da missão das Forças Armadas depende do comprometimento de toda a sociedade.

> A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o Ministério da Defesa, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o Ministério da Defesa e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a Estratégia Nacional de Defesa (END) (BRASIL, 2023, p. 16).

A Doutrina também deixa claro a estrutura e o funcionamento do SMDC[99], reiterando a divisão das áreas de segurança cibernética, a cargo do GSI/PR, e a defesa cibernética, a cargo do Ministério da Defesa. Dessa última, destaca a Guerra Cibernética, a cargo dos Comandos Operacionais ativados e de suas Forças Componentes. Estabelece, assim, uma divisão em níveis, conforme apresenta a figura 7.

Figura 7 - Níveis de decisão e atores no espaço cibernético, conforme a DMDC

Fonte: Brasil (2023, p. 13)

Desse modo, no nível político está a Segurança Cibernética, coordenada pelo GSI, abrange a APF e as IC. No nível estratégico, a Defesa Cibernética, fica a cargo do MD, do Estado-Maior Conjunto das Forças Armadas (EMCFA) e dos Comandos das Forças Armadas, interagindo com o GSI/PR, APF, agências e IC de interesse para a Defesa Nacional. Já o nível operacional e tático, a Guerra Cibernética, fica a cargo dos Comandos Operacionais ativados e das Forças Componentes. Adicionalmente, DMDC esclarece que a Defesa Cibernética é a

[99] O Sistema Militar de Defesa Cibernética pode ser definido como "um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses. Cabe também ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC²), possibilitando a capacidade de atuar em rede com segurança, bem como de maneira integrada e colaborativa na gestão de riscos que envolvam a proteção de infraestruturas críticas, conforme previsto no Plano Nacional de Segurança de Infraestruturas Crítica" (Brasil, 2023, p. 16).

denominação utilizada quando do “planejamento e da execução de ações cibernéticas afetas ao nível estratégico de decisão”. Já a denominação Guerra Cibernética se refere “quando o nível de decisão considerado for operacional ou tático” (BRASIL, 2023, p. 13).

Portanto, a defesa cibernética, no âmbito do Ministério da Defesa, fica como responsabilidade principal do Comando de Defesa Cibernética (ComDCiber), órgão central do SMDC. O ComDCiber foi criado em 2015, vinculado à estrutura regimental do Exército Brasileiro e sua missão central é:

> [...] planejar; orientar; coordenar; integrar; e executar atividades relacionadas ao desenvolvimento e à aplicação das capacidades cibernéticas, como órgão central e no âmbito do SMDC, a fim de contribuir para o uso efetivo do espaço cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional (BRASIL, 2023, p. 18).

Assim, atua no assessoramento do MD para a implantação e gestão do SMDC, coordena as unidades cibernéticas distribuídas nas três Forças, promove ações conjuntas com os demais organismos da Defesa e mantém um canal técnico com órgãos de inteligência das Forças Armadas, visando garantir “a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários.” (BRASIL, 2023, p. 16). Ainda, mantém um canal para coordenação com órgãos externos que podem vir a contribuir com as atividades de defesa cibernética e colabora com o GSI e os órgãos da APF nos assuntos relacionados à proteção das IC de interesse da Defesa. A atuação do ComDCiber, segundo a DMDC, também se orienta no sentido de fomentar a pesquisa e o aperfeiçoamento das capacidades cibernéticas de interesse da Defesa, além de propor e executar ações colaborativas com países parceiros (BRASIL, 2023).

O ComDCiber conta com um braço operacional, o Centro de Defesa Cibernética (CDCiber), e um braço acadêmico, a Escola Nacional de Defesa Cibernética (EnaDCiber) (LOBATO; KENKEL, 2015; AMIN, 2019; COSTA, 2019; GRASSI; AYRES PINTO, 2022b). O CDCiber foi criado ainda em 2010 e, mais tarde, integrado ao ComDCiber, atuando nas operações de proteção, exploração e ataque cibernético, na pesquisa e compreensão de ameaças, na análise de riscos e incidentes e na resolução de diversos problemas no espaço cibernético. Atua também de forma cooperativa com outros organismos nacionais assim como com países parceiros (COSTA, 2019).

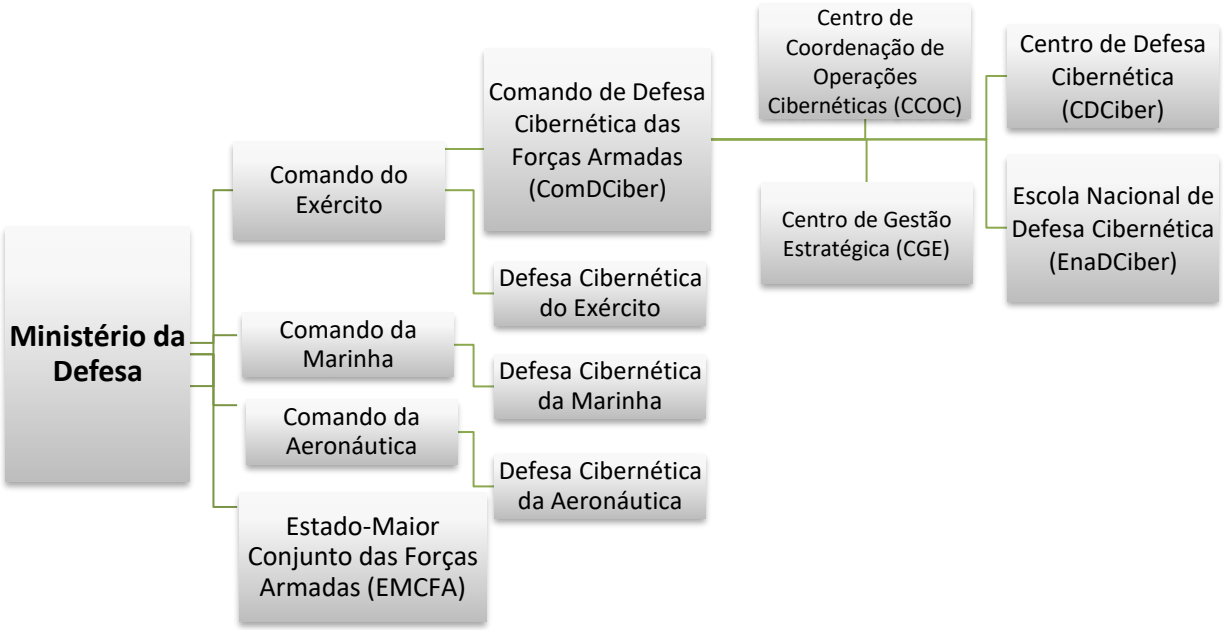
Já ENaDCiber foi ativada oficialmente em fevereiro de 2019 – embora desde 2015 funcionasse como um núcleo na Estrutura Regimental do Comando do Exército - e tornou-se

o braço acadêmico do ComDCiber. A criação da EnaDCiber já havia sido mencionada na END de 2012, como um meio para promover o intercâmbio multidisciplinar acadêmico-científico entre instituições civis e instituições militares, visando incrementar a base de C&T nacional (BRASIL, 2012b).

A Escola tem estrutura de ensino dual - civil e militar - e tem como missão "fomentar e disseminar as capacitações necessárias à Defesa Cibernética [...] bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão do assunto e para a melhoria da qualificação da mão de obra nacional para o setor" (BRASIL, 2019, s. p.). Apesar de ainda limitada, se sua atuação avançar com o proposto na sua criação, pode vir a cumprir um papel importante de formação e capacitação de recursos humanos, intercâmbio de conhecimentos e experiências com especialistas de países parceiros, bem como de maior interação entre especialistas civis e militares no setor cibernético (GRASSI; AYRES PINTO, 2022b).

Somando a esses órgãos, foi criado, no âmbito do ComDCiber, o Centro de Coordenação de Operações Cibernéticas (CCOC) que, segundo a DMDC, "tem como tarefas aplicar as capacidades cibernéticas, no âmbito do SMDC, realizando o planejamento das operações conjuntas, combinadas e interagências"; e o Centro de Gestão Estratégica (CGE) que atua na coordenação dos processos de planejamento, gestão estratégica, relações institucionais, gestão do conhecimento e de talentos. A Doutrina ainda prevê o Centro de Ações Cibernéticas (CAC), que executaria as operações de Defesa e Guerra Cibernética, função que atualmente é exercida pelo Centro de Defesa Cibernética (CDCiber) (BRASIL, 2023, p. 19).

Figura 8 – Organograma central da defesa cibernética do Brasil

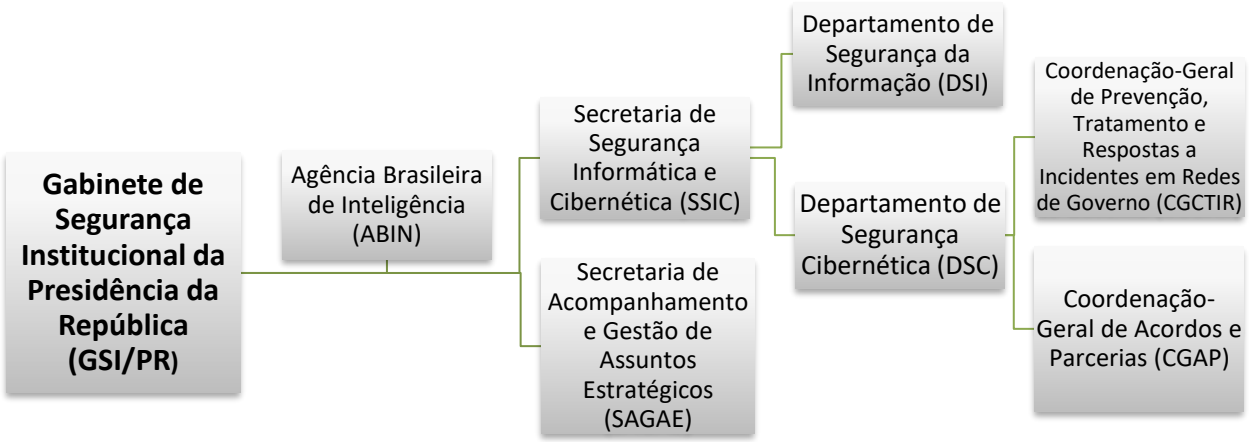


Fonte: elaboração própria com base em TCU (2020) e Brasil (2023).

Por fim, como já mencionado, a segurança cibernética fica a cargo do Gabinete de Segurança Institucional da Presidência da República (GSI), sendo que a estrutura institucional do órgão passou por uma reorganização, a partir do Decreto nº 11.676 de 30 de agosto de 2023. Diante disso, atualmente, a Secretaria de Segurança Informática e Cibernética (SSIC) conta com dois departamentos, o Departamento de Segurança da Informação (DSI) e o Departamento de Segurança Cibernética (DSC), e a Secretaria de Acompanhamento e Gestão de Assuntos Estratégicos (SAGAE) passou a abrigar a Coordenação-Geral de Segurança das Infraestruturas Críticas (CGSIC) (GSI, 2023).

Além desses, existem outros órgãos e entidades que atuam de forma coordenada, como a Agência Brasileira de Inteligência (ABIN) – a qual, atualmente, faz parte da estrutura institucional da Casa Civil, no âmbito da Presidência da República; o Departamento de Política Federal, com sua atuação na investigação de crimes cibernéticos; outros organismos que auxiliam no campo da segurança cibernética, como a o Comitê Gestor da Internet no Brasil (CGI.br), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e outros (TCU, 2020).

Figura 9 – Organograma central da segurança cibernética do Brasil



Fonte: elaboração própria com base em TCU (2020).

Por fim, apesar da clara separação entre os organismos responsáveis pela segurança e pela defesa cibernética no Brasil, há um papel protagonista dos militares em relação ao setor cibernético em geral, os quais acabam por assumir funções que extrapolam o campo da defesa e adentram o âmbito da segurança cibernética (Solar, 2020; Hurel, 2021), o que demonstra a debilidade das instituições civis em coordenar os processos na área e uma sobrecarga de funções às Forças Armadas.

Ademais, ainda não foi estabelecida uma carreira civil no âmbito da defesa nacional, a qual havia sido mencionada ainda na END de 2008 e o profissional civil segue tendo menor espaço do que o necessário. Desse modo, apesar do entendimento de que novas abordagens e profissionais com novas características e capacidades são necessários para enfrentar os obstáculos no setor cibernético e que os documentos ressaltam a preocupação em relação a formação de recursos humanos, os incentivos à produção científica diversificada e à parceria com especialistas civis, isso carece de maior desenvolvimento na prática (GRASSI; AYRES PINTO, 2022b).

Todavia, essa situação não é exclusividade do Brasil, sendo uma problemática comumente enfrentada nos países latino-americanos. Ainda assim, vem se observando o amadurecimento do campo de pesquisa nas universidades e a academia tem se engajado com temáticas que eram predominantemente do âmbito militar. Cursos acadêmicos sobre a área vêm estimulando a participação e o diálogo entre civis e militares, visando a construção de

conhecimentos e a capacitação conjunta, as escolas militares têm contado com maior participação de civis e projetos e exercícios conjuntos vem sendo impulsionados por instituições civis e militares (GRASSI; AYRES PINTO, 2022b).

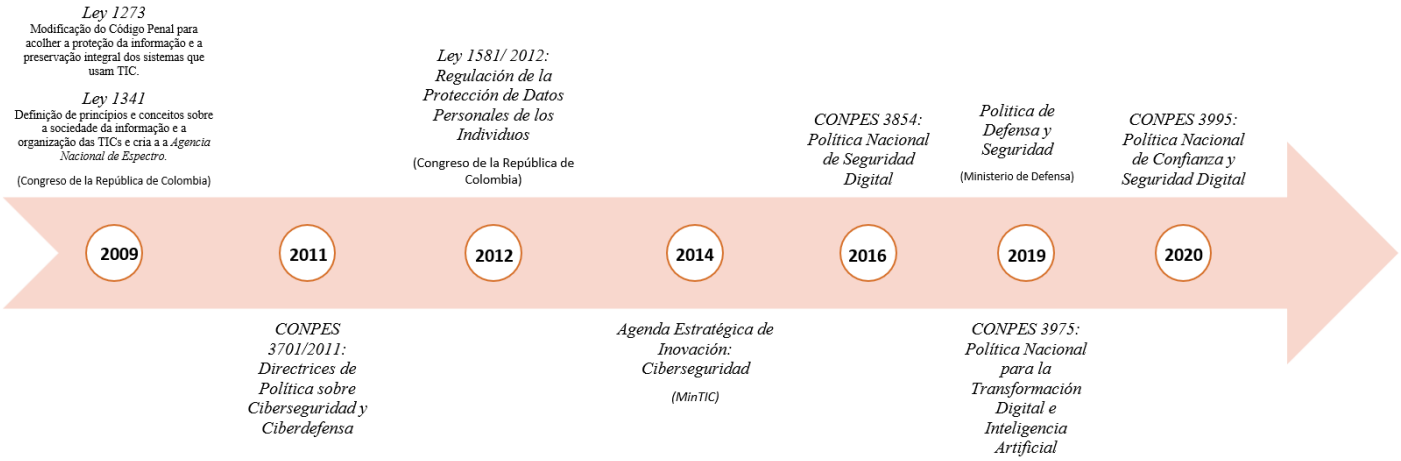
4.3.2 Colômbia

A Colômbia é considerada o primeiro país da região a desenvolver política e estratégia para a cibersegurança e a ciberdefesa, com a aprovação da Política de Cibersegurança e Ciberdefesa (Conpes 3701), em julho de 2011. Cinco anos mais tarde, a Política Nacional de Segurança Digital (Conpes 3854) é publicada para atualizar e complementar a anterior, trazendo novos enfoques e perspectivas para a segurança e defesa cibernética do país. Mais recentemente, em 2020, a Colômbia publicou nova atualização, a Política Nacional de Confiança e Segurança Digital (Conpes 3953). Importante notar que Colômbia não desenvolveu um Livro Branco de Defesa Nacional, como os de Brasil e Argentina, possuindo somente sua Política de Defesa e Segurança.

Cabe ressaltar também, entre a diversas legislações que abrangem a temática, que, ainda em 2009, o país modificou seu Código Penal, através da Lei 1.273, visando proteger as informações e dados pessoais, criando tipos penais relacionados aos crimes cibernéticos (PÉREZ, 2017). Ademais, a lei 1.585 de 2012 estabeleceu a regulação do país em relação à proteção dos dados pessoais, estabelecendo princípios, normas e padrões para o tratamento dos dados e criando uma Autoridade de Proteção de Dados, instituindo-se, assim, como marco importante para a proteção e garantia de direitos fundamentais.

Sobre isso, a figura 10 traz a linha do tempo com os principais documentos produzidos pela Colômbia a partir de 2008 em relação à cibersegurança e a ciberdefesa nacional.

Figura 10 - Linha do tempo: principais documentos sobre cibersegurança e ciberdefesa da Colômbia



Fonte: elaboração própria.

Com a Conpes 3701 o país adotou uma estratégia abrangente que envolve as nuances da segurança e da defesa cibernética do país, expõe os perigos do crime cibernético, mas também os desafios para a defesa nacional e os riscos para as infraestruturas críticas. O documento cria as normativas e os organismos, esquematizando a atuação coordenada desses organismos nacionais e definindo suas funções específicas (BORRERO, 2015; GARCÍA, 2017; PÉREZ, 2017; CASTAÑO; SEGOVIA; VELASCO, 2020; CASTILLO; BEJARANO, 2020; VILLAMIL et al., 2020).

O documento identificou 3 eixos problemáticos no âmbito da ciberdefesa e da cibersegurança no país, os quais precisam ser enfrentados: i) a falta de uma coordenação interinstitucional apropriada para lidar com os novos desafios do ambiente digital; ii) a fragilidade da formação especializada em cibersegurança e ciberdefesa, identificando o limitado conhecimento na área; iii) a fraqueza na regulamentação e na legislação para a proteção de informações e dados (COLOMBIA, 2011).

Assim, o objetivo central do Conpes 3701 é "fortalecer as capacidades do Estado para enfrentar ameaças que comprometem a sua segurança e defesa no domínio cibernético (cibersegurança e ciberdefesa), criando o ambiente e as condições necessárias para fornecer proteção no ciberespaço" (COLOMBIA, 2011, p. 20, tradução própria). Para isso, compreende a necessidade de criar um ambiente participativo, atuando de forma coordenada, fortalecer os níveis de cooperação internacional, apoiar pesquisas, desenvolver conhecimento na área e elevar a capacitação na área, bem como conscientizar toda a população. O

documento também define alguns termos, estabelece planos de ação e expectativa de financiamento para o período entre 2011 e 2014 e aporta recomendações para superar os eixos problemáticos e implementar os objetivos propostos (COLOMBIA, 2011).

Diante disso, o país passou a estruturar as bases para a defesa cibernética nacional, criando uma Comissão Intersetorial, com representantes do Ministério da Defesa junto ao Grupo de Resposta a Emergências Cibernéticas da Colômbia (ColCERT), o Comando Cibernético Conjunto (CCOC) e o Centro Cibernético da Polícia (CCP). Portanto, esses órgãos são os encarregados principais de liderar a cibersegurança e a ciberdefesa nacional (GARCÍA, 2017; CASTAÑO; SEGOVIA; VELASCO, 2020; VILLAMIL et al., 2020), conforme a figura 11.

Figura 11 - Modelo de Coordenação da cibersegurança e da ciberdefesa da Colômbia

Fonte: Conpes 3701 (COLOMBIA, 2011, p. 21)

Essa Comissão Intersetorial é chefiada pelo Presidente da República e integrada pelo Alto Assessor para Segurança Nacional, pelo Ministro da Defesa, pelo Ministro das Tecnologias de Informação e Comunicações, pelo Diretor do Departamento Administrativo de Segurança (DAS), pelo Diretor da Planejamento Nacional e pelo Coordenador do ColCERT, havendo a possibilidade de serem convidados outros atores nacionais, sejam estes do setor

público, privado ou da academia, ou especialistas internacionais, a depender das discussões propostas (COLOMBIA, 2011).

Assim nasce o Grupo de Resposta a Emergências Cibernéticas da Colômbia (ColCERT), responsável por coordenar os aspectos da segurança cibernética e da defesa cibernética a nível nacional (BORRERO, 2015; GARCÍA, 2017; OLIVEIRA et al., 2017; PÉREZ, 2017; CASTAÑO; SEGOVIA; VELASCO, 2020; VILLAMIL et al., 2020). O ColCERT é um grupo do Ministério da Defesa, integrado por militares e funcionários civis e atuando coordenadamente com outras entidades (COLOMBIA, 2011).

Conforme Borreiro (2015, p. 13, tradução própria):

> A sua responsabilidade central é a coordenação da cibersegurança e ciberdefesa nacional, que se enquadrará no processo missionário de gestão da segurança e defesa do Ministério da Defesa Nacional. Esta coordenação corresponde às ações necessárias para proteger a infraestrutura crítica do Estado colombiano contra emergências de segurança cibernética que ameaçam ou comprometem a segurança e defesa nacional.

Assim, entre seus objetivos estão: coordenar e assessorar as equipes de respostas à incidentes cibernéticos e outras entidades nas esferas pública e privada para responder aos incidentes cibernéticos; oferecer serviços para prevenção e resposta a esses incidentes, bem como serviços de informação, conscientização e formação em matéria cibernética; atuar como ponto de contato internacional, estabelecendo diálogo com outros organismos estatais e internacionais; promover o desenvolvimento de capacidades e promover procedimentos, protocolos e estruturação de guias de boas práticas para a atuação no setor; e apoiar os órgãos de investigação, de segurança e de prevenção de ameaças no âmbito das TICs (BORRERO, 2015; CASTILLO; BEJARANO, 2020).

Figura 12 - Modelo Relacional ColCERT

Fonte: Conpes 3701 (COLOMBIA, 2011, p. 21)

Atuando conjuntamente está o Comando Cibernético Conjunto das Forças Militares (CCOC), integrante da estrutura do Comando Geral das Forças Militares. O CCOC visa proteger os interesses nacionais no âmbito cibernético, encarregando-se de coordenar as respostas frente a incidentes cibernéticos que ponham em risco a segurança nacional. Sua atuação perpassa as operações de ciberdefesa, operações de inteligência, auditorias e avaliações de segurança e desenvolvimento das estratégias de capacitação cibernética (BORRERO, 2015; GARCÍA, 2017; CASTAÑO; SEGOVIA; VELASCO, 2020; CASTILLO; BEJARANO, 2020; VILLAMIL et al., 2020). Além disso, sob a liderança do CCOC, criou-se unidades de ciberdefesa especializadas em cada uma das Forças Militares: a Unidade Cibernética Exército Nacional, a Unidade Cibernética Armada Nacional e a Unidade Cibernética Força Aérea (CASTAÑO; SEGOVIA; VELASCO, 2020).

Já o Centro Cibernético Policial (CCP), no âmbito da Polícia Nacional[100], se encarrega da prevenção, investigação e repressão dos crimes informáticos. É responsável, entre outras funções, por desenvolver programas, projetos e estratégias para a investigação dos crimes que afetem a segurança da informação e dos dados e atua coordenadamente com a

[100] A Policia Nacional também faz parte da estrutura institucional do Ministério da Defesa da Colômbia

Organização Internacional de Polícia Criminal (Interpol) (BORRERO, 2015; GARCÍA, 2017; CASTAÑO; SEGOVIA; VELASCO, 2020; CASTILLO; BEJARANO, 2020; VILLAMIL et al., 2020).

Nesse sentido, de modo geral, o CCP fica com a responsabilidade da segurança cibernética e o CCOC está responsável pela defesa cibernética. No entanto, ambos os organismos fazem parte da estrutura institucional do Ministério da Defesa da Colômbia. Este Ministério tem o papel de contribuir para o desenvolvimento e a execução de "políticas de defesa e segurança nacional para garantir a soberania nacional, a integridade territorial e a aplicação das condições necessárias ao direito às liberdades públicas e garantir que os habitantes da Colômbia vivam em paz". Ademais, tem por objetivo proteger "a democracia, através do uso da segurança e da defesa, além da aplicação adequada e focada da força e do desenvolvimento de capacidades que salvaguardem a integridade da nação." (CASTILLO; BEJARANO, 2020, p. 32, tradução própria). Dessa forma, a ele é delegado o papel central no desenvolvimento e execução de todos os aspectos da cibersegurança e da ciberdefesa do país (BORRERO, 2015; OLIVEIRA et al., 2017; CASTILLO; BEJARANO, 2020; VILLAMIL et al., 2020).

Com base nos documentos e na literatura consultada e observando o organograma do Ministério da Defesa da Colômbia, tem-se a estrutura institucional da cibersegurança e da ciberdefesa nacional apresentada na figura 13.

Figura 13 - Organograma central da Cibersegurança e da Ciberdefesa do Ministério de Defesa da Colômbia

Fonte: elaboração própria, com base em Conpes 3701 (2011); Castaño, Segovia e Velasco (2020); Colombia (2021); Colombia (2023)

Além do Ministério da Defesa e dos organismos a ele ligados, o Ministério das Tecnologias de Informação e Telecomunicações (MinTIC) também atua no sentido de colaborar para a concretização das políticas cibernéticas do país (BORRERO, 2015). Este tem como objetivo "propor, adotar e promover políticas e projetos no setor das tecnologias de informação e comunicação", bem como atua de modo incrementar e facilitar o uso das TIC pela população, garantindo que essa possa se beneficiar dessas tecnologias de forma apropriada (CASTILLO; BEJARANO, 2020, p. 32, tradução própria).

Observa-se também que, no caso da Colômbia, o Conselho Nacional de Política Econômica e Social (CONPES), autoridade máxima de coordenação da política econômica do país e responsável, entre outras coisas, por aprovar documentos sobre o desenvolvimento de políticas públicas, é designado também para emitir os documentos estratégicos em matéria de cibersegurança e ciberdefesa. O Conpes é presidido pelo Presidente do país e a secretaria

técnica é responsabilidade do chefe do Departamento Nacional de Planejamento (DNP). O DNP, ao qual o Conpes está ligado, é uma entidade técnica dependente da Presidência da República, que revisa, organiza e avalia as políticas públicas colombianas e designa o investimento público, coordenando o Plano Nacional de Desenvolvimento com os ministérios e outras autoridades, entre outras funções (GARCÍA, 2017; PÉREZ, 2017; CEPAL, 2023).

Ainda em relação aos documentos oficiais da Colômbia, cinco anos mais tarde da publicação do Conpes 3701, a Colômbia lançou a Política Nacional de Segurança Digital (Conpes 3854), em abril de 2016, visando complementar e atualizar as discussões de cibersegurança e ciberdefesa abordadas no documento anterior. Esse documento entende a necessidade de "passar de uma abordagem que procura preservar a segurança dos sistemas e redes de informação, para uma abordagem focada na gestão do risco inerente às atividades sociais e econômicas no ambiente digital." (VILLAMIL et al., 2020, p. 371, tradução própria). Isso ocorre pela identificação de que o país focava seus esforços em neutralizar ameaças no âmbito da segurança e da defesa nacional, mas não havia uma preocupação mais ampla e preventiva que envolvesse todas as partes interessadas. Nesse sentido, essa nova visão estratégica não diferenciaria o objetivo da prosperidade econômica e social dos objetivos relacionados à segurança e a defesa no ambiente digital (COLOMBIA, 2016). A partir disso, passa-se a discutir a segurança digital como um sentido amplo, abrangendo todas as questões de cibersegurança e de ciberdefesa.

A gestão de risco da segurança digital é definida como:

> [...] o conjunto de ações adotadas para enfrentar os riscos e maximizar as oportunidades no ambiente digital. É um esquema para enfrentar, prevenir e contrariar a materialização de ameaças ou incidentes que possam afetar a soberania nacional e as atividades econômicas e sociais dos cidadãos. A utilização de um esquema de gestão de risco garante que as medidas tomadas são apropriadas e proporcionais. (COLOMBIA, 2016, p. 78, tradução própria).

O Conpes 3854 se organiza como um documento bem estruturado que aponta os avanços realizados pelo país desde 2011, delimita os princípios fundamentais, os objetivos, os resultados desejados e as dimensões estratégicas que devem nortear a atuação no país no setor. Também traz conceitos, planos de ação, recomendações e esquemas de financiamento para a área.

Vale mencionar alguns desses pontos. O Conpes 3854 elenca quatro princípios fundamentais: i) a necessidade de proteger os direitos humanos e direitos fundamentais dos

indivíduos, entre eles a liberdade de expressão, o livre fluxo de informações, a proteção dos dados pessoais, a privacidade e outros consagrados pela Constituição do país; ii) a abordagem inclusiva e colaborativa que deve ser adotada entre todos os atores nacionais; iii) a responsabilidade partilhada, promovendo a colaboração e a coordenação entre os atores; e iv) a abordagem baseada na gestão de riscos, visando, entre outras coisas, garantir um ambiente seguro e confiável, promovendo a prosperidade econômica, a inovação, a produtividade e a competitividade (COLOMBIA, 2016).

Assim, o documento destaca a necessidade de maiores investimentos e capacitação de recursos humanos, identificados como ainda insuficientes diante da grandiosidade dos desafios enfrentados nesse ambiente. Também entende a importância de desenvolver um enfoque integrado, identificando atores de interesse que podem contribuir para o avanço das capacidades do país - sejam atores do setor público, privado, da academia, ou outras entidades da sociedade civil - e a partilha de responsabilidades, visando estabelecer estratégias de coordenação e cooperação, reforçar a capacitação dos intervenientes ligados ao setor e maximizar as oportunidades provenientes desse novo espaço de atuação (COLOMBIA, 2011; GARCÍA, 2017; PÉREZ, 2017; VILLAMIL et al., 2020).

Além disso, importa mencionar os cinco objetivos estratégicos elencados:

OE1. Fortalecer a capacidade institucional, regulatória, administrativa e de gestão em termos de segurança digital para a Colômbia, desde o mais alto nível;

OE2. Promover a prosperidade econômica e social do país, com a promoção de um ambiente que permita a realização de atividades digitais de forma aberta, segura e confiável;

OE3. Garantir a integridade e a segurança dos indivíduos e do Estado, a nível nacional e transnacional, num ambiente digital crescente e dinâmico;

OE4. Fortalecer a defesa e a soberania nacionais num ambiente digital;

OE5. Promover a cooperação, colaboração e assistência em matéria de segurança digital, a nível nacional e internacional (COLOMBIA, 2016, p. 65, tradução própria).

Em 2019, a Colômbia publicou também a Política Nacional de Transformação Digital e Inteligência Artificial (Conpes 3975), com objetivo de desenvolver planos para a transformação digital dos setores público e privado no país, através do uso estratégico das novas tecnologias para impulsionar maior produtividade e impactar positivamente no desenvolvimento socioeconômico e no bem-estar da sociedade colombiana. Isso se daria, principalmente, por meio do fortalecimento do capital humano e do desenvolvimento de habilidades e da diminuição das barreiras para a incorporação dessas tecnologias nos setores

público e privado, através de um plano de ação estruturado para cada objetivo específico definido e apresentado no documento (COLOMBIA, 2019a).

Nesse documento, além do marco conceitual, do diagnóstico do país e da contextualização dos desafios enfrentados, são delineados 14 princípios que norteiam o desenvolvimento da inteligência artificial (IA) do país, entre esses destaca-se o papel estratégico das universidades e da pesquisa científica na criação de um mercado de IA, salientanto ser imprescindível o estímulo no meio acadêmico para o desenvolvimento de projetos e a interação com o setor privado. Além desse, aponta a necessidade de estabelecer medidas de intercâmbio internacional e atração de pessoal especializado para atuar na área, buscando que a Colômbia se torne "uma referência mundial em questões de inteligência artificial, gerando alianças internacionais que permitam esse reconhecimento." (COLOMBIA, 2019a, p. 23, tradução própria).

Por fim, em 2020, a Colômbia lançou a Política Nacional de Confiança e Segurança Digital (Conpes 3995). Esse documento é a última atualização no marco da cibersegurança e da ciberdefesa do país, com estruturação similar aos anteriores. Este documento aponta os avanços na implementação dos planos e na capacitação e aponta para o que ainda precisa ser fortalecido e desenvolvido, identificando, entre outros elementos, a necessidade de aumentar a confiança no ambiente digital e fortalecer as capacidades de cibersegurança e ciberdefesa para garantir os interesses do país nesse espaço.

O documento define o que entende por confiança, sendo compreendida, em termos gerais, como "a probabilidade suficientemente elevada de que um ator externo realize uma ação que nos seja benéfica (ou pelo menos não prejudicial), para que seja considerada a cooperação com esse ator" (COLOMBIA, 2020, p. 15, tradução própria). Assim, a confiança digital seria estabelecida "através da privacidade, segurança, responsabilidade, transparência e práticas participativas eficazes e aplicáveis." (COLOMBIA, 2020, p. 16, tradução própria). Sendo essa, portanto, a base de todas as interações humanas e fundamental no ambiente digital com vistas ao progresso socioeconômico da nação.

Nesse documento também fica clara a definição de segurança digital proposta pelo país, como:

> […] a situação de normalidade e tranquilidade no ambiente digital (ciberespaço), derivada da concretização dos propósitos essenciais do Estado através (i) da gestão do risco de segurança digital; (ii) a implementação eficaz de medidas de cibersegurança; e (iii) a utilização eficaz das capacidades de defesa cibernética; que

> exige a vontade social e política dos múltiplos interessados e dos cidadãos do país. (COLOMBIA, 2020, p. 44, tradução própria).

Desse modo, o objetivo delimitado nesse documento é o de:

> Estabelecer medidas para desenvolver a confiança digital através da melhoria da segurança digital para que a Colômbia seja uma sociedade inclusiva e competitiva no futuro digital, fortalecendo as capacidades e atualizando o quadro de governança da segurança digital, bem como com a adoção de modelos com ênfase nas novas tecnologias. (COLOMBIA, 2020, p. 27, tradução própria).

A partir disso, estabelece 3 objetivos específicos e planos de ação para concretizá-los. São estes:

OE 1. Reforçar as capacidades de segurança digital dos cidadãos, do setor público e do setor privado para aumentar a confiança digital no país.

OE 2. Atualizar o quadro de governança da segurança digital para aumentar o seu nível de desenvolvimento e melhorar o progresso do país na segurança digital.

OE 3. Analisar a adoção de modelos, padrões e estruturas em matéria de segurança digital para preparar o país para os desafios da Quarta Revolução Industrial (COLOMBIA, 2020, p. 27).

O país ressalta seu foco na construção de capacidades, definindo capacidade cibernética como "o conjunto de qualidades e aptidões de um país que lhe permitem gerar um ambiente adequado para abordar, gerar conhecimento e aumentar o grau de desenvolvimento em termos de segurança digital [...]" (COLOMBIA, 2020, p. 16, tradução própria). Afirma partir do aporte metodológico fornecido pelo GCI da UIT e das dimensões propostas por esse instrumento. Ademais, no Conpes 3995, cita-se os aportes trazidos pelo NCSI para contextualizar o cenário nacional. Nesse sentido, percebe-se a preocupação do país em torno da construção de capacidades cibernéticas e a utilização dessas ferramentas para identificar as lacunas e os avanços do país no setor.

Entre as iniciativas para capacitação, os documentos oficiais demonstram uma particular preocupação na formação, treinamento e qualificação dos recursos humanos nacionais, implementando cursos de graduação, pós-graduação e formação técnica e tecnóloga, além de projetos e programas específicos de formação e conscientização, como o projeto Criação de um Caminho Profissional em Segurança Digital, destinado a jovens estudantes universitários de engenharia, e a iniciativa Hacker Girls, também com apoio da OEA, visando capacitar as mulheres no setor das TICs (COLOMBIA, 2020).

Observando mais especificamente sobre a cooperação internacional, os documentos ressaltam as oportunidades de cooperação no âmbito digital, tanto no nível nacional quanto internacional, para compartilhamento de informações e de conhecimentos, intercâmbio de experiências, pesquisas e desenvolvimento tecnológico entre os países (COLOMBIA, 2011; COLOMBIA, 2016). Ademais, propõe-se a implementação de uma agenda estratégica para promover a colaboração e cooperação internacional em temas de segurança digital. Também se menciona a necessidade de implementar uma "diplomacia digital" - sem nenhuma definição a respeito – propondo a implementação de um curso de formação específico em Diplomacia Digital (COLOMBIA, 2016).

A Política de Defesa e Segurança, particularmente, coloca como um dos seus eixos estratégicos a "segurança coletiva" e ressalta a questão da cooperação internacional em segurança e defesa em vários momentos ao longo do seu texto. Sobre a cooperação internacional, em relação ao tema ciber, afirma que, "na esfera digital, a gestão de riscos é uma responsabilidade coletiva, portanto, cooperaremos com outros países para atuar sob o princípio da responsabilidade partilhada e atuar de forma articulada e transnacional para enfrentar o crime cibernético." (COLOMBIA, 2019b, p. 37, tradução própria).

Dessa forma, aponta que a cooperação será intensificada "nas áreas operacionais e de inteligência, formação, fortalecimento institucional, troca de informações, segurança cibernética, proteção de infraestruturas críticas e troca de experiências." (COLOMBIA, 2019b, p. 53, tradução própria). Isso é posto como uma via para a construção de capacidades cibernéticas pelo país, a qual perpassará o fortalecimento do quadro legal, a promoção de projetos de pesquisa, formação de recursos humanos e a adoção de uma doutrina conjunta que integre "as capacidades do ciberespaço disponíveis em terra, mar e ar, bem como em programas de formação no âmbito da cooperação com países aliados." (COLOMBIA, 2019b, p. 52, tradução própria).

Ainda, a Colômbia tornou-se, em 2018, o primeiro país latino-americano a ser considerado parceiro externo da OTAN (MORAIS DA SILVA; GRASSI, 2022). Assim, a Política de Defesa e Segurança afirma que será prioridade para o país o trabalho conjunto com a Organização, visando o "intercâmbio de conhecimentos em áreas como inteligência, operações regulares de guerra, contra-insurgência, tráfico de drogas, assistência humanitária e gestão de riscos de catástrofes", além de buscarem "aumentar o conhecimento e as

experiências em áreas como a interoperabilidade, os apoios logísticos integrados e os padrões logísticos – operacionais e de ciberdefesa" (COLOMBIA, 2019, p. 50-51).

Especificamente sobre o entorno regional, o Conpes 3701 indica o desejo do país em torna-se um líder regional na área. Essa liderança se daria "através do intercâmbio de boas práticas, conhecimentos e experiências, prestando especial atenção à promoção da experiência nacional no processo de desenvolvimento da política de segurança cibernética e defesa cibernética." (COLOMBIA, 2011, p. 28, tradução própria). Para isso, destaca a necessidade de participar também em conferências, workshops e reuniões especializadas em nível internacional (COLOMBIA, 2011).

Não há, entretanto, menções específicas sobre a América do Sul ou América Latina, ou discussões específicas sobre cooperação com o entorno regional sul-americano nessa temática, em nenhum dos documentos oficiais analisados. Já Política de Defesa e Segurança assinala a cooperação regional em outros temas, tais como questões fronteiriças, narcotráfico, terrorismo, crime transnacional, a proteção da Amazônia, a preservação dos direitos humanos e da democracia.

Por outra perspectiva, os documentos específicos mencionam as ameaças cibernéticas e a preocupação em garantir a defesa nacional, aumentar as capacidades militares, mencionado a preocupação com a proteção da soberania e das infraestruturas críticas e outros âmbitos de defesa, mas em nenhum momento há a menção a guerra cibernética nos documentos, nem mesmo na Política de Defesa e Segurança. Também não há menção a poder cibernético explicitamente (COLOMBIA, 2011; COLOMBIA, 2016; COLOMBIA, 2020).

Para finalizar, Castillo e Bejarano (2020, p. 26, tradução própria), ao discutir a cibersegurança e a ciberdefesa do país, apontam para a necessidade da clara diferenciação entre os termos, definindo:

> A defesa cibernética visa a proteção e segurança de uma nação, utilizada pelas suas forças militares para salvaguardar a sua integridade e neutralizar todas as ameaças a que se encontra. está exposto. Por outro lado, a cibersegurança mostra-nos todas aquelas ações que podem ser realizadas não só no estado, mas também no setor privado, a fim de manter uma segurança que permita minimizar os ataques cibernéticos que uma pessoa ou qualquer tipo de entidade possa sofrer.

Contudo, apesar da diferenciação entre os termos cibersegurança e ciberdefesa feita pela Colômbia em seus documentos e a identificação da necessidade de ampliação da atuação

a partir da coordenação entre atores nacionais diversos, percebe-se ainda uma estruturação centrada na dimensão militar. Além disso, ao analisar os documentos oficiais, percebe-se que o país compreende a segurança cibernética como uma área mais ampla dentro da qual está a defesa cibernética. Por fim, o país passou a utilizar o termo segurança digital como um conceito mais geral em seus documentos oficiais, abrangendo todas as ações e dinâmicas realizadas do setor cibernético.

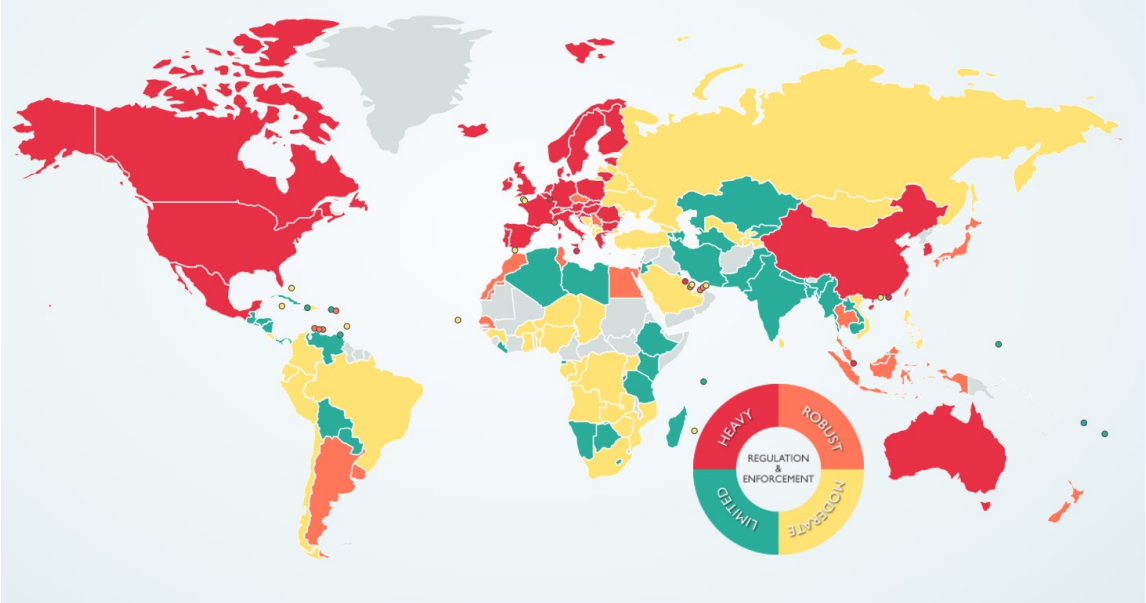
4.3.3 Argentina

A Argentina foi o primeiro país da América do Sul a ter um marco regulatório para a proteção de dados, através da Lei 25.326 de outubro de 2000, a qual vem buscando fortalecer ao longo dos anos (BID; OEA, 2020). Conforme Oliveira et al. (2017), o país possui nível de proteção de dados pessoais reconhecido como adequado pela Comissão Europeia (OLIVEIRA et al., 2017). É também classificada como uma nação com regulamentação de proteção de dados robusta pela DLA Piper - uma importante multinacional de advocacia anglo-americana, que possui escritórios em todos os continentes do globo (inclusive em Argentina, Brasil e Colômbia), e que investiga e fornece dados sobre as leis de proteção de dados ao redor do globo (DLA Piper, 2023).

Conforme pode ser visualizado na figura 14, enquanto a Argentina possui uma robusta regulação, Brasil e Colômbia possuem uma moderada regulamentação de proteção de dados[101].

[101] O relatório com as informações dos países pode ser obtido no site da DLA Piper.

Figura 14 - Leis de Proteção de Dados no Mundo



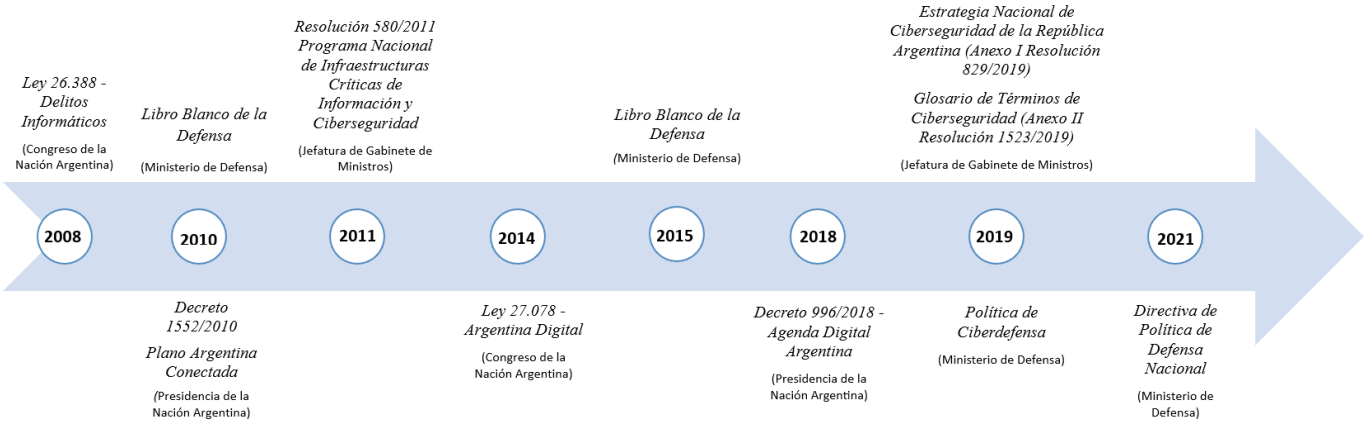
Fonte: DLA (2023)

Além disso, no campo da segurança cibernética o país publicou, em 2019, a Estratégia Nacional de Cibersegurança da República da Argentina, que se soma ao Programa Nacional de Infraestrutura Críticas de Informação e Cibersegurança, instituído por meio da Resolução nº 580 de 2011. No que diz respeito à defesa cibernética, o principal documento é Política de Ciberdefesa, de 2019, que se junta ao Livro Branco de Defesa, atualizado em 2015, e à Política de Defesa Nacional, publicada em 2018 e atualizada em 2021.

Além desses, ao longo dos anos outras legislações foram implementadas a fim de organizar e modernizar a estrutura organizacional do país, entre essas estão: a Lei 26.388/2008 que modifica o Código Penal argentino, incorporando a este os delitos cometidos por meios informáticos; o Plano Argentina Conectada (Decreto 1552/2010), que cria o Plano Nacional Argentina Conectada, visando melhorar o acesso e apropriação de sua população às TICs; a Lei 27.078/2014 - Argentina Digital, que estabelece o acesso às TICs como um direito humano, sendo que o acesso de qualidade deve ser garantido em condições sociais e geográficas equitativas, bem como estabelece a neutralidade das redes; e o Decreto 996/2018 - Agenda Digital Argentina, a qual pretende, entre outros objetivos, desenvolver capacidades de segurança cibernética para gerar confiança em ambientes digitais.

A figura 15 apresenta os principais documentos e legislações em matéria de segurança e defesa cibernética da Argentina.

Figura 15 - Linha do tempo: Principais documentos de cibersegurança e ciberdefesa da República Argentina



Fonte: elaboração própria

Em relação ao setor cibernético, o Livro Branco de Defesa ressalta os desafios decorrentes do avanço tecnológico e as ameaças para a defesa nacional provenientes do ciberespaço, mencionando, inclusive as possibilidades de conflitos armados e guerras ocorrerem nesse ambiente:

> Embora as ações de uma guerra cibernética tenham a sua origem e desenvolvimento no campo virtual das redes de comunicação e dos sistemas informáticos, podem desencadear efeitos cinéticos específicos no mundo real, afetando potencialmente o controle de infraestruturas críticas, o abastecimento de energia e água potável, o ar e o tráfego terrestre e, entre outros aspectos, a segurança da informação estratégica. Portanto, o novo desafio que o ciberespaço representa exige uma rápida adaptação dos sistemas de defesa e o desenvolvimento de capacidades específicas neste campo operacional único. (ARGENTINA, 2015a, p. 25, tradução própria).

Por outra perspectiva, o Livro Branco menciona também os esforços cooperativos do país e, particularmente, com os países sul-americanos em vários momentos. Aponta que o país suprimiu "as hipóteses históricas de conflito militar com os países do seu imediato ambiente geográfico" (ARGENTINA 2015a, 130, tradução própria). Assim, atualmente, identifica o espaço sul-americano como área de atuação prioritária, destacando a necessidade de construção de medidas de confiança mútua e aumentar a cooperação em matéria de defesa na região. Nessa perspectiva, afirmar promover "ações de cooperação com os Ministérios da Defesa e as Forças Armadas dos países amigos, priorizando os vínculos sub-regionais, especialmente no âmbito do Conselho de Defesa Sul-Americano" (ARGENTINA, 2015a, p. 216, tradução própria).

Ademais, entre os princípios da política de defesa do país está a promoção e a consolidação da América do Sul como uma zona de paz, a construção progressiva de uma identidade sul-americana em matéria de defesa e de um sistema de defesa sub-regional. Entre as diretrizes estão: a promoção do diálogo entre os Ministérios da Defesa e as Forças Armadas dos países da região, intercâmbio técnico-profissional e consolidação de medidas de cooperação com a América Latina e, particularmente, com a América do Sul, principalmente a partir do CDS, visando implementar projetos conjuntos na área, como projetos de complementação científica e tecnológica (ARGENTINA, 2015a).

Em relação ao tema ciber, menciona as medidas de cooperação em curso naquele período no âmbito do CDS da Unasul e aponta para a importância de aumentar a autonomia e avançar no estabelecimento de ações coordenadas para garantir a segurança dos sistemas e redes, mas também proteger o ciberespaço dos países diante das interferências externas que possam ser contrárias aos interesses vitais e estratégicos dos países e suas populações. Diante disso frisa: "Neste caminho sul-americano rumo à unidade, convergem princípios e valores de cada um dos Estados membros e canalizam-se questões estratégicas de consideração urgente, como a proteção dos recursos naturais e a defesa do ciberespaço sul-americano." (ARGENTINA, 2015a, p. 32, tradução própria).

A Política de Defesa Nacional reafirma algumas discussões já mencionadas no Livro Branco e traz alguns pontos adicionais e complementares. Ressalta a transversalidade do ciberespaço e afirma que o ciberespaço "gerou reconsiderações sobre as categorias tradicionais com que se abordava a 'guerra real', exigindo rápida adaptação por parte dos sistemas de defesa." (ARGENTINA, 2021, p. 7, tradução própria). Nesse contexto, aponta para a necessidade de explorar a possibilidade de novas ações militares, combinando o conhecimento tradicional e formas inovadoras baseadas na tecnologia. A inovação é compreendida a partir de uma visão mais abrangente que deve ser incentivada e sistematizada para alcançar vantagens operacionais e estratégicas (ARGENTINA, 2021).

Isso posto, defende ser necessário desenvolver "capacidades de vigilância, comando, controle, comunicações, computação, inteligência e guerra eletrônica [...]" (ARGENTINA, 2021, p. 25, tradução própria). O documento também destaca o caráter defensivo do instrumento militar argentino e a disposição à cooperação na área. Diante disso, pondera que a Argentina irá "reforçar os laços internacionais, fundamentalmente na região, para o desenvolvimento da capacidade soberana em termos de infraestruturas de comunicações e de

defesa cibernética" e buscará participar dos fóruns de discussão internacionais sobre o ciberespaço (ARGENTINA, 2021, p. 32, tradução própria).

Salienta que, de modo geral, a região sul-americana é uma região pacífica em que se há buscado desenvolver acordos de cooperação militar tanto bilateralmente quanto multilateralmente. Assim, mesmo em um momento de fragmentação política na região e um cenário menos favorável à construção de consensos, a relação com os vizinhos permanece como prioridade para a Argentina, destacando a necessidade de reestabelecer instâncias de diálogo, coordenação e intercâmbio regional, visando construir vínculos mais profundos (ARGENTINA, 2021). Ademais, menciona os recursos estratégicos sul-americanos e ressalta a necessidade de unir os países da região frente aos interesses estrangeiros na região, acrescentando que:

> [...] a política de defesa nacional deve evitar o problema histórico da reprodução acrítica e descontextualizada de conceitos e doutrinas de emprego que refletem, por um lado, os interesses e perspectivas das potências estrangeiras e, por outro, realidades geopolíticas diferentes daquelas que prevalecem na América do Sul (ARGENTINA, 2021, p. 18, tradução própria).

Ainda, sugere que desenvolver projetos conjuntos no âmbito das indústrias de defesa regionais poderia resultar em diversas vantagens para os países, diminuindo "os custos do desenvolvimento tecnológico e o ônus financeiro da produção, além de se beneficiarem do conhecimento acumulado e da expansão dos mercados, os Estados da região poderiam retomar uma linha estratégica de trabalho com vistas ao futuro" (ARGENTINA, 2021, p. 9, tradução própria).

O documento mais específico sobre defesa cibernética é a Política de Ciberdefesa, publicada em 2019. A Política de Ciberdefesa da Argentina estabelece os objetivos do Ministérios da Defesa no ciberespaço:

- Antecipar e prevenir ataques no ciberespaço;
- Reduzir as vulnerabilidades e aumentar a resiliência dos sistemas e redes TI das Forças Armadas, EMCO e MD;
- Detectar ameaças e gerir riscos de ataques cibernéticos e recuperação de sistemas e infraestruturas críticas de interesse para a Defesa Nacional;
- Adotar ações contra potenciais adversários ou agentes hostis que afetem a integridade e disponibilidade das redes e sistemas de Defesa;

- Contribuir para o fortalecimento da base tecnológica e industrial nacional de segurança cibernética em trabalho conjunto com o Ministério das Relações Exteriores e o Ministério da Produção;
- Promover programas de formação para superar a lacuna entre os recursos humanos disponíveis e os que são procurados.

Para o cumprimento de tais objetivos, define quatro linhas de ação:

I) Criação do Centro Nacional de Defesa Cibernética;

II) Proteger a disponibilidade do ciberespaço como espaço soberano;

III) Reengenharia das redes das Forças Armadas, do Estado-Maior Conjunto e do Ministério de Defesa;

IV) Convergência das capacidades das Forças Armadas (ARGENTINA, 2019a, p. 2).

Diante disso, estabelece o desenvolvimento de três políticas para auxiliar no desenvolvimento das linhas de ação mencionadas. São essas: i) Política regulatória; ii) Política de desenvolvimento de capacidades para interação no espaço cibernética – focada na adoção e aperfeiçoamento das soluções tecnológicas; e iii) Política de conscientização e capacitação (ARGENTINA, 2019a).

Sobre a última, ela reforça que a capacitação dos recursos humanos é crucial, sendo basilar a oferta de cursos de formação continuada, cursos técnicos em segurança informática, cursos operacionais e de nível político-estratégico destinados especialmente aos formuladores de políticas de defesa cibernética, visando também a aquisição de conhecimentos sobre o direito internacionais aplicado às operações cibernéticas. Menciona também a oferta de Mestrado e Especialização em Ciberdefesa "dirigida a profissionais com experiência e conhecimento em diferentes aspectos específicos ligados à ciberdefesa e à cibersegurança (TICs, sistemas, direito informático, políticas públicas, etc.), seguindo modelos curriculares dos centros de renome internacional" (ARGENTINA, 2019a, p. 13, tradução própria).

Desse modo, propõe a criação do Centro Nacional de Ciberdefesa que concentraria as atividades para o desenvolvimento das capacidades de interação no ciberespaço, visando garantir a liberdade de ação neste domínio e evitar situações que possam afetar a confidencialidade, integridade e disponibilidade da informação que é transportada e/ou processada nas redes e sistemas das Forças Armadas, do EMCO e do Ministério de Defesa, bem como proteger as IC da Defesa Nacional (ARGENTINA, 2019a). Nesse Centro funcionariam o CSIRT Defesa, o Centro de Operações de Segurança Inteligente (iSOC) e o Laboratório de Análise Cibernética (CyberLab) (ARGENTINA, 2019b). Ainda, propõe a

criação de um Conselho Consultivo de Ciberdefesa, no âmbito do Centro Nacional de Ciberdefesa com a participação de empresas, institutos de formação, universidades e outros. Isso visaria promover programas para construção de capacidades, potencializar a base tecnológica e industrial nacional com o financiamento de projetos de pesquisa, desenvolvimento e inovação e articular acordos internacionais (ARGENTINA, 2019a).

Assim, entre as prioridades operacionais do Ministério de Defesa no ciberespaço, citadas no documento, especialmente no que se refere à implementação da primeira linha de ação, estão: o desenvolvimento de cursos de formação contínua e atualização constante, a reformulação dos planos de formação de recursos humanos, tendo em vista o desenvolvimento de capacidades específicas em defesa cibernética e o desenvolvimento de capacidades de dissuasão e de habilidades de resposta ofensiva frente às ameaças e possíveis ataques (ARGENTINA, 2019a).

O documento também descreve o Plano Nacional de Proteção de Infraestruturas Cibernéticas Críticas de Defesa Nacional, criado com o objetivo de "reforçar a capacidade de segurança e recuperação das infraestruturas críticas de Defesa, mediante a gestão dos riscos físicos e cibernéticos através dos esforços colaborativos e integrados de todos os atores envolvidos", listando entre esses atores o Comitê de Cibersegurança, criado através do Decreto 577/2017 e modificado pelo Decreto 480/2019, a Secretaria de Governo de Modernização (atual Secretaria de Inovação Pública), os entes reguladores, os operadores críticos (provedores de serviços essenciais e produtores de bens de interesse para a Defesa Nacional) e Ministério da Defesa.

A Política de Ciberdefesa se mostra um documento vago e sem grandes ambições, não analisa o contexto em que o país se encontra na temática, nem aprofunda discussões sobre elementos importantes para a construção das capacidades da nação, detendo-se em apresentar alguns órgãos envolvidos e mencionar brevemente algumas ações a serem desenvolvidas pelo país. Além disso, não consta nenhuma menção à América do Sul ou medidas de cooperação internacional na área.

Por fim, a Estratégia de Cibersegurança, também publicada em 2019, tem como objetivo central proporcionar um ciberespaço seguro para a utilização dos indivíduos e organizações públicas e privadas, "desenvolvendo, de forma coerente e estruturada, ações de prevenção, deteção, resposta e recuperação contra ameaças cibernéticas, juntamente com o desenvolvimento de um quadro regulamentar." (ARGENTINA, 2019d).

O documento destaca que as novas tecnologias trazem diversas possibilidades para o desenvolvimento humano e o progresso econômico e científico da nação, ao mesmo tempo em que produzem ameaças capazes de gerar danos efetivos às sociedades e organizações e "riscos potencialmente devastadores para a paz e a segurança internacionais." (ARGENTINA, 2019d, p. 2, tradução própria). Desse modo, destaca as características do ciberespaço, como sua dimensão global e transfronteiriça, sua natureza dual, sua massividade e sua constante evolução, apontando que a segurança desse domínio é complexa e depende de coordenação de esforços entre os variados atores privados e públicos.

Também salienta as vulnerabilidades das infraestruturas nacionais, o problema da atribuição de responsabilidade, as tensões, instabilidades e desconfianças geradas pelo crescente uso militar do ciberespaço, as assimetrias entre os Estados e as dificuldades vinculadas ao exercício da soberania nesse ambiente, reforçando que põem à prova o exercício do poder estatal, já que entende ser o ciberespaço "um domínio global e intangível e um fluxo infinito de dados sobre os quais não se exerce controle nem soberania" (ARGENTINA, 2019d, p. 3, tradução própria). Com isso, afirma que a Argentina:

> [...] promoverá em todos os fóruns em que participar, o uso pacífico do Ciberespaço e apoiará qualquer iniciativa que vise estabelecer valores como a Justiça, o respeito ao Direito Internacional, o equilíbrio e a redução da exclusão digital entre as nações, promovendo o diálogo e a cooperação. O ciberespaço deve tornar-se um domínio onde prevaleça a paz, afastando-o de possíveis conflitos armados (ARGENTINA, 2019d, p. 3, tradução própria).

Diante do panorama apresentado, a Estratégia Nacional de Cibersegurança baseia-se em cinco princípios orientadores:

I) Respeito pelos direitos e liberdades individuais – proteção das pessoas e a garantia dos direitos e liberdades consagrados na Constituição Nacional e nos tratados internacionais.

II) Liderança, construção de capacidades e fortalecimento federal – entendendo que o Estado Nacional deve assumir a liderança e atuar de forma coordenada com as províncias, municípios, setor privado, academia e sociedade civil.

III) Cooperação internacional – tanto em nível regional quanto internacional, unindo forças para resolver as problemáticas.

IV) Cultura da cibersegurança e responsabilidade compartilhada – ação e coordenação com compartilhamento de responsabilidades entre setor público, privado,

academia e a sociedade civil para garantir um espaço seguro e criar uma cultura de cibersegurança.

V) Fortalecimento do desenvolvimento econômico – gerar um ambiente propício para o progresso socioeconômico da nação a partir de um ambiente seguro e do aproveitamento das oportunidades advindas das novas tecnologias.

Com esse alicerce estabelecido, o documento determina oito objetivos específicos e expõe brevemente ações para garantir a concretização desses objetivos. São eles:

I) Conscientização do uso seguro do ciberespaço – promover melhores práticas e incrementar projetos de conscientização a nível nacional.

II) Capacitação e educação sobre o uso seguro do ciberespaço – aquisição de conhecimentos e habilidades, com a formação e capacitação de profissionais, técnicos e pesquisadores, promoção de oficinas e exercícios e atividades de formação transversais no setor acadêmico.

III) Desenvolvimento de um quadro normativo - adequar e criar normas jurídicas, quadros regulamentares, padrões e protocolos para enfrentar os desafios e os riscos provenientes do ciberespaço, garantindo o respeito pelos direitos fundamentais.

IV) Fortalecimento da capacidade de prevenção, detecção e resposta – através da coordenação entre atores nacionais, melhorando as capacidades dos organismos e forças de segurança.

V) Proteção e recuperação dos sistemas de informação do setor público – desenvolvimento de políticas públicas, mecanismos de controle, coordenação entre os atores nacionais, avaliação constante das medidas de segurança e resiliência, fortalecimento dos recursos humanos.

VI) Fomento da indústria da cibersegurança – fomentar as capacidades tecnológicas, atividades de pesquisa e inovação, tanto no nível público quanto no nível privado

VII) Cooperação internacional – participação em organismos internacionais que tratem da segurança cibernética e participar atividade dos espaços acadêmicos e técnicos internacionais que trabalhem com a temática, além de promover acordos regionais e internacionais que contribuam para um espaço cibernético pacífico e seguro.

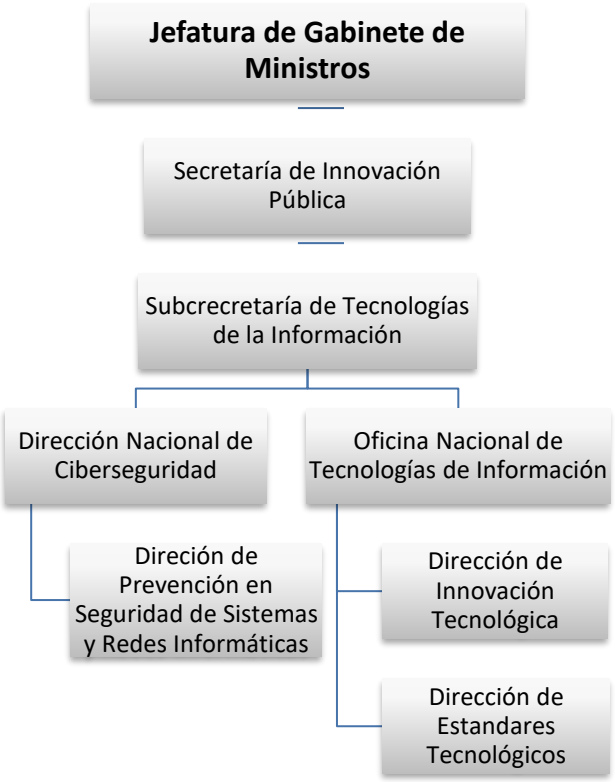
VIII) Proteção das infraestruturas críticas nacionais de informação – promover a definição, identificação e proteção dessas infraestruturas, fortalecer a cooperação público-privada, promovendo esforços coordenados e o intercâmbio de informações.

A Estratégia de Cibersegurança da Argentina também se apresenta como um documento genérico, no entanto, é possível dimensionar quais os princípios norteadores e os pontos centrais da atuação argentina no ambiente cibernético. Percebe-se que o país compreende o ciberespaço como um ambiente no qual a cooperação tem sua relevância expandida, mencionando em diversos pontos a necessidade de estabelecer medidas de cooperação no nível nacional, regional e internacional. Ainda assim, não há nenhuma menção há programas ou projetos específicos que poderiam ser desenvolvidos com seus vizinhos sul-americanos.

Direcionando a atenção à estrutura institucional da Argentina, é possível observar que, assim como o Brasil, a Argentina separa claramente os organismos civis e militares responsáveis pela área da cibersegurança e pela área da ciberdefesa. O país passou por uma reestruturação dos seus organismos nos últimos anos, que gerou mudanças nos organogramas da Chefia de Gabinete de Ministros e do Ministério da Defesa, nos quais se concentra a coordenação das principais ações de cibersegurança e ciberdefesa do país.

A Segurança Cibernética está sob responsabilidade principal da Direção Nacional de Cibersegurança, a qual se insere na Subsecretaria de Tecnologias da Informação (antiga Subsecretaria para a Proteção das Infraestruturas Críticas de Informação e Segurança Cibernética). Essas, por sua vez, se inserem na Secretaria de Inovação Pública (anteriormente denominada Secretaria de Governo de Modernização), no âmbito da Chefia de Gabinete de Ministros, conforme pode ser observado na figura 16.

Figura 16 – Organograma central da Cibersegurança da República Argentina



Fonte: elaboração própria, com base em Argentina (2023d e 2023e).

Entre os objetivos da Secretaria de Inovação Pública está o de "compreender a cibersegurança e a proteção das infraestruturas críticas de informação e comunicações associadas ao Setor Público Nacional e aos serviços de informação e comunicações [...]". Sob sua órbita está a Subsecretaria de Tecnologias da Informação e Comunicações, que possui nas suas funções a de "propor à Secretaria estratégias, padrões e regulamentos para segurança cibernética e proteção de infraestruturas críticas de informação e comunicações associadas do Setor Público Nacional [...]" (ARGENTINA, 2023a, p. 1).

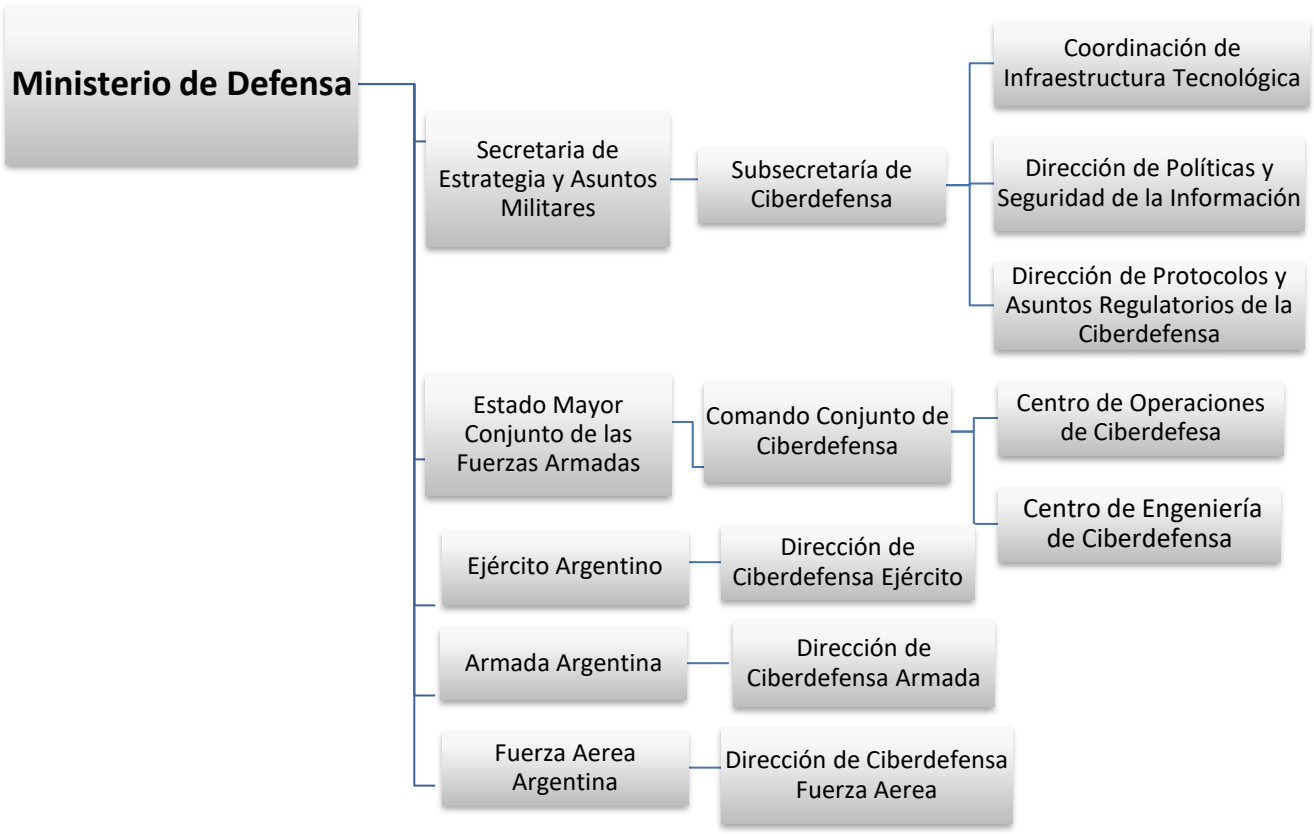
A Direção Nacional de Cibersegurança está alocada no âmbito da Subsecretaria de Tecnologias da Informação e Comunicações e é a responsável principal pelos temas de cibersegurança. Entre suas funções estão: elaborar as políticas de cibersegurança e outras normas de forma coordenada com outros organismos estatais; elaborar planos, programas e projetos com perspectiva federal em matéria de cibersegurança; formular e executar planos de capacitação para o setor público e promover medidas de resiliência dos sistemas; desenvolver o Programa Nacional de Infraestruturas Críticas de Informação; analisar as vulnerabilidades

de softwares da Administração Pública e incorporar na Administração Pública Nacional boas práticas para manter o ambiente digital seguro; e colaborar com outras organizações e centros de pesquisa públicos e privados para a promoção de planos, programas e projetos de inovação tecnológica no domínio da segurança cibernética (ARGENTINA, 2023b).

Já o Escritório Nacional de Tecnologias da Informação fica responsável por dirigir a formulação de políticas e implementação do processo de desenvolvimento tecnológico e inovação para a transformação do Estado Nacional, além de promover a integração de novas tecnologias, a sua compatibilidade e interoperabilidade. No seu âmbito estão a Diretoria de Padrões Tecnológicos e a Diretoria de Inovação Tecnológica (ARGENTINA, 2023c).

Em relação à Defesa Cibernética, no âmbito militar, foi criado, em 2014, o Comando Conjunto de Ciberdefesa (CCCD) que coordena as atividades de ciberdefesa da Argentina (ARGENTINA, 2015a). Ademais, cada uma das três Forças possui unidades específicas para tratar do tema e atuam conjuntamente com o CCCD. Outro organismo que concentra funções na ciberdefesa argentina é a Subsecretaria de Ciberdefesa, principal órgão responsável pela proteção das infraestruturas críticas da Defesa Nacional (ARGENTINA, 2019a). A figura 17 apresenta o organograma central da defesa cibernética da Argentina.

Figura 17 – Organograma central da Ciberdefesa da República Argentina



Fonte: elaboração própria, com base em Guimpel (2020), CCCD (2022) e Argentina (2023d, 2023e).

O CCCD dependente orgânica, funcional e operacionalmente do Estado Maior Conjunto (EMCO) e é liderado por um oficial sênior do Exército Argentino. Seu objetivo central é gerar capacidades para deter ciberataques contra as IC e os ativos de informação do Sistema Nacional de Defesa (ARGENTINA, 2015a). Ademais, conforme Guimpel (2020, p. 46), o CCCD:

> [...] é o principal responsável pelo estabelecimento de padrões e procedimentos para a defesa cibernética, criptografia e informática forense, na supervisão dos centros de resposta de cada força armada, na organização e desenvolvimento de atividades acadêmicas; deve intervir na preparação, revisão e experimentação da Doutrina de Defesa Cibernética; e deve participar da conscientização do pessoal das Forças Armadas e na determinação e supervisão de padrões de segurança e certificação de protocolos relacionados nas Forças Armadas.

Ligados ao CCCD estão o Centro de Engenharia de Defesa Cibernética, “cuja missão é fornecer suporte de engenharia e gerenciamento do conhecimento das tecnologias do Ciberespaço”; e o Centro de Operações de Defesa Cibernética, que tem como função central “executar as Operações de Defesa Cibernética necessárias para prevenir, detectar, neutralizar e/ou anular qualquer agressão que afete os sistemas de informação ou redes críticas das forças armadas ou outros objetivos cuja proteção seja atribuída oportunamente” (GUIMPEL, 2020, p. 45-46).

A Subsecretaria de Ciberdefesa, criada em 2016, integra a Secretaria de Estratégias e Assuntos Militares. Entre suas responsabilidades estão: auxiliar a Secretaria de Ciência, Tecnologia e Produção para a Defesa no planejamento, concepção e elaboração da política de defesa cibernética; atuar na orientação, direção e supervisão das ações de ciberdefesa levadas a cabo pelos níveis Estratégico Nacional e Estratégico Militar; promover políticas para atrair, recrutar, incentivar e formar recursos humanos para a defesa cibernética; promover vínculos de cooperação e intercâmbio em pesquisa com os campos acadêmico, científico e empresarial; viabilizar acordos de cooperação e assistência técnica em defesa cibernética com organizações públicas e privadas, além de promover a coordenação com as autoridades dos diferentes Poderes do Estado para garantir a proteção das infraestruturas críticas nacionais; atuar na avaliação e aprovação dos planos militares de desenvolvimento de capacidades em ciberdefesa e auxiliar na concepção e fortalecimento dessas capacidades; e atuar de forma coordenada com outros organismos para a concepção de políticas, normas e procedimentos para garantir a segurança da informação (ARGENTINA, 2016a).

Por fim, cabe assinalar que ao analisar as instituições argentinas, pode-se perceber que várias mudanças foram feitas, novos organismos foram criados, outros extintos e outros transformados, demonstrando certa mutabilidade nos órgãos argentinos. A Direção de Mapa de Estado encarrega-se de manter atualizada a estrutura institucional dos ministérios e organismos estatais, ainda assim, algumas informações acessadas em documentos e na literatura especializada difere do apresentado no site do Mapa do Estado em alguns pontos, gerando dúvidas sobre a real organização do país em relação à cibersegurança e a ciberdefesa.

4.4 CONSIDERAÇÕES PARCIAIS: PERSPECTIVAS COMPARADAS E OPORTUNIDADES PARA A CONSTRUÇÃO DE CAPACIDADES CIBERNÉTICAS CONJUNTAS

Analisar os índices internacionais, compreendendo os pilares e indicadores e as pontuações atribuídas aos países sul-americanos – e, mais minuciosamente, Argentina, Brasil e Colômbia –, tornou possível comparar os níveis de capacitação cibernética em que se encontram. Apesar das limitações analíticas – devido, principalmente, às divergências metodológicas e as variadas definições para o conceito de capacidades cibernéticas - os índices fornecem subsídios para avaliar em quais aspectos os Estados precisam avançar, as lacunas que precisam ser preenchidas, bem como em quais tópicos estão mais avançados. Essas percepções podem contribuir para o aprimoramento das estratégias e a formulação de planos de ação mais coerentes para a realidade de cada Estado. Da mesma forma, ao permitir estabelecer comparações, foi possível identificar as similaridades, ou seja, as áreas em que os países se encontram em graus similares e/ou precisam avançar em objetivos semelhantes, além dos elementos nos quais um ou mais países se destacam em relação aos demais, podendo ser encarados como complementaridades.

Como exemplos, percebe-se, nas diretrizes do GCI, que enquanto Brasil é destaque nas medidas legais, a Colômbia teve nesse pilar sua segunda menor pontuação no ranking. Já a Argentina teve sua pior pontuação nas medidas de desenvolvimento de capacidades, enquanto a segunda melhor pontuação do Brasil foi justamente nesse pilar. Além disso, Brasil e Colômbia, com destaques nas medidas organizacionais e nas medidas de cooperação, teriam muito a contribuir com o restante da região nessa área.

Essa análise é ainda mais evidente ao explorar os dados fornecidos pelo NSCI e os dados disponíveis no relatório de cibersegurança da OEA, que se baseia no CCMM e no qual se pode observar países alcançando o nível estratégico – e até mesmo dinâmico - em aspectos específicos do ranking e outros países ainda no nível inicial ou formativo. Por outro lado, em outros fatores é possível observar que as nações enfrentam desafios comuns.

Exemplificando, Colômbia e Brasil estão mais avançados nos aspectos “Gerenciamento de Crise”, “Defesa Cibernética” e “Proteção das Infraestruturas Críticas” em relação à Argentina. Ainda, tanto nas informações do NSCI quanto no relatório da OEA, percebe-se que a Colômbia tem pontuação superior no que diz respeito à implementação da

estratégia de cibersegurança. O país também se destaca, no NSCI, nas medidas de confiança dos serviços eletrônicos e, nesse mesmo índice, tanto Colômbia quanto Argentina receberam pontuação máxima na luta contra o crime cibernético, pontos nos quais Brasil precisaria aprimorar suas capacidades. Além disso, a Argentina recebeu melhor pontuação no gerenciamento de crises cibernéticas e o Brasil se destaca na análise e informações sobre ameaças cibernéticas. Por outro lado, os três países precisam avançar, por exemplo, na resposta a incidentes cibernéticos, na proteção de serviços essenciais e necessitam participar mais ativamente de processos de cooperação e na governança cibernética global.

Analisando mais precisamente os dados de C&T dos países – principalmente quando comparados aos países mais desenvolvidos – é notório o atraso dos países sul-americanos – e latino-americanos, de modo geral. Em termos de C&T e P&D, o Brasil, sendo o maior país da região, é claramente o que mais investe nesse setor em relação a seu PIB. Como exemplo, o país investiu 1,17% em P&D, em 2020, mais que o dobro do segundo colocado na região, a Argentina, que investiu 0,48% somente. A Argentina, por sua vez, possui o melhor índice em termos de pesquisadores (4,82 pesquisadores a cada mil pessoas economicamente ativas).

Comparado com os países mais desenvolvidos, percebe-se o quanto esse investimento é reduzido, já que países com PIB maiores tem investido, pelo menos, 5 vezes mais que a média latino-americana (que é de aproximadamente 0,7%). Israel, por exemplo, investiu, em 2020, 5,5% do seu PIB em P&D; EUA teve quase 3,5% do PIB investido em P&D; ou, ainda, Japão, com cerca de 3,3% de investimento no setor.

A América Latina e o Caribe, região que corresponde a cerca de 8,5% da população mundial, foi responsável por apenas 2,3% do investimento mundial em P&D. Enquanto isso, Estados Unidos e Canadá correspondem a cerca de 4,5% da população mundial e, em 2020, foram responsáveis por 30% do investimento mundial em P&D (INTERNET WORLD STATS, 2022; RICYT, 2022). Em síntese, os dados demonstram o atraso dos países da região nesse setor, o qual é considerado central para a construção de capacidades cibernéticas.

Os documentos de segurança e defesa de Argentina, do Brasil e da Colômbia compreendem a lacuna que possuem em termos de recursos humanos qualificados, mencionando a demanda por aumentar seu arsenal de especialistas, pesquisadores e profissionais capacitados para atuar no setor. Salientam em vários momentos e, inclusive, destacam como prioridade, como eixo estruturante, ação estratégica ou, em outros termos, o desenvolvimento da C&T, da P&D, além da necessidade de promover políticas públicas para a educação cibernética, melhorar a formação e a qualificação de recursos humanos e reter os

talentos para contribuir no desenvolvimento nacional, bem como promover o intercâmbio acadêmico e a coordenação entre o setor público, privado e academia (conforme disposto no Plano de Ação de Educação em Segurança Cibernética proposto pelo Programa de Cibersegurança do Comitê Interamericano contra o Terrorismo da OEA).

Ainda assim, percebe-se que os países enfrentam muitas dificuldades na implementação efetiva dessas propostas, que precisam, sobretudo, serem sustentadas ao longo do tempo, para que possam produzir resultados concretos. Esse pilar é considerado basilar, necessário para sustentar as demais dimensões da construção de capacidade. Assim, conquistar o que Ceballos, Maisonnave e Londoño (2020) definem como soberania tecnológica digital.

Além desse entendimento comum sobre a prioridade dos elementos mencionados, os documentos de segurança e defesa de Brasil, Colômbia e Argentina, apresentam outras convergências e complementaridades em relação aos componentes analisados, apesar da abordagem, em alguns momentos, ser distinta. Os países compreendem a importância da proteção dos direitos fundamentais da sua população, estabelecendo legislações sobre proteção de dados e sobre crime cibernético, além de mencionar em seus documentos a proteção dos direitos humanos, a privacidade, a liberdade de expressão, o acesso à informação e o acesso seguro ao ambiente digital. Sobre suas legislações para a proteção de dados pessoais, vale mencionar que a Argentina foi pioneira na região, instituindo ainda em 2000 sua Lei de Proteção de Dados Pessoais, enquanto Colômbia publicou em 2012 sua lei para regulação da proteção dos dados pessoais. Comparativamente, o Brasil desenvolveu tardiamente sua LGPD, a qual entrou em vigor em 2020.

Além disso, nas suas políticas e estratégias os três países mencionam a diplomacia no campo da segurança e/ou da defesa. A END do Brasil ressalta a diplomacia em defesa como essencial para conciliação de diferenças entre percepções, sendo um instrumento poderoso para evitar e resolver conflitos, ganhando ainda mais importância no mundo cada vez mais interdependente. A Colômbia, por sua vez, salienta especificamente sobre a necessidade de implementar uma diplomacia digital e um curso de formação sobre o tema, embora não conceitue o termo nem aprofunde sobre como essa diplomacia seria implementada. Já a Argentina é o único dos três a conceituar diplomacia cibernética – mesmo que de forma superficial -, embora não discorra especificamente sobre isso em seus documentos.

De modo geral, os três países também abordam a relevância da cooperação cibernética internacional e da necessidade de participarem de fóruns e organizações que discutam a temática, em vista a participarem da elaboração de normativas, promoverem o intercâmbio técnico e combaterem o cibercrime conjuntamente. Ademais, identificam as possibilidades de troca de informações, intercâmbio de experiências e parcerias no âmbito científico e tecnológico. Adicionalmente, todos declaram, em um ou mais documentos estratégicos, a cooperação regional como prioritária.

Especificamente sobre cooperação cibernética, no caso do Brasil, a E-Ciber cita a necessidade de maior integração entre o Brasil e os países latino-americanos, porém sem mencionar a América do Sul particularmente. De modo mais amplo, sem especificar o setor cibernético, os documentos de defesa nacional identificam a América do Sul como entorno estratégico imediato do país e destacam à prioridade dada à cooperação com a região, visando garantir a estabilidade e a paz regional, promover o desenvolvimento econômico e aproveitar as vantagens da cooperação tecnológica e industrial. Apontam também para o intercâmbio acadêmico entre as instituições de ensino dos países sul-americanos.

A Colômbia, em especial, apresenta a cooperação como uma via para a construção de capacidades cibernéticas, devendo ser intensificada "nas áreas operacionais e de inteligência, formação, fortalecimento institucional, troca de informações, segurança cibernética, proteção de infraestruturas críticas e troca de experiências." (COLOMBIA, 2019b, p. 53). Não há menção direita à América do Sul na temática ciber, indicando a cooperação em outras temáticas na sua Política de Defesa e Segurança. No entanto, o país propôs, na Conpes 3701, tornar-se líder regional no setor cibernético e essa liderança perpassaria o "intercâmbio de boas práticas, conhecimentos e experiências, prestando especial atenção à promoção da experiência nacional no processo de desenvolvimento da política de segurança cibernética e defesa cibernética." (COLOMBIA, 2011, p. 28).

A Argentina estabelece a cooperação internacional como um objetivo estratégico e como um princípio orientador da sua estratégia de cibersegurança. Ademais, assim como Brasil, delimita a América do Sul como seu entorno estratégico imediato, bem como defende a construção de uma identidade sul-americana em matéria de defesa, estabelecendo a necessidade de medidas de confiança mútua e de aumentar a cooperação em matéria de defesa na região. Especificamente sobre ciber, indica que a cooperação entre os países sul-americanos se torna essencial para proteger o ciberespaço dos Estados diante das interferências externas que possam ser contrárias aos interesses vitais e estratégicos dos países

e suas populações. Ainda, salienta que projetos regionais conjuntos podem se configurar como formas de diminuir os custos financeiros do desenvolvimento tecnológico e garantir maior autonomia à região. Entretanto, a política de ciberdefesa do país, documento esvaziado em conteúdo, não menciona nenhuma medida de cooperação internacional ou regional.

Por outro prisma, vale mencionar as perspectivas conceituais já mencionada por alguns autores, que pode se tornar um entrave na consecução de medidas cooperativas entre os países, já que partir de modelos de compreensão distintos sobre o ciberespaço dificulta o entendimento no momento de estabelecer os pontos de acordo. Além disso, a não definição de termos importantes também pode resultar em obstáculos, ou até mesmos desconfianças entre os atores. Sobre isso, chama a atenção a não definição de guerra cibernética por Argentina e Colômbia. A Colômbia, entretanto, sequer menciona esse termo nos seus documentos de defesa, diferentemente da Argentina que aborda a possibilidade de ciberguerras ocorrerem e traz o termo guerra eletrônica, também sem defini-la.

Ainda sobre os diferentes entendimentos estratégicos, a Colômbia passou a adotar a "segurança digital" como um conceito amplo em seus documentos, abrangendo, de modo geral, a gestão do risco de segurança digital, a implementação eficaz de medidas de cibersegurança e a utilização eficiente das capacidades de defesa cibernética. Nesse sentido, defende uma mudança de perspectiva, baseada, a partir da Conpes 3854/2016, na gestão de riscos que se traduziria em um esforço preventivo e menos reativo, além de estabelecer o desenvolvimento socioeconômico e a cibersegurança e ciberdefesa como objetivos que devem ser tratados conjuntamente.

Adicionalmente, a Colômbia parte de uma estrutura institucional diferenciada, ao passo que ambos os campos da cibersegurança e da ciberdefesa estão sob responsabilidade central do Ministério da Defesa do país. Isso porque tanto o CCOC, integrante da estrutura das Comando Geral das Forças Militares e responsável pela defesa cibernética, quanto o CCP, no âmbito da Polícia Nacional, responsável pela segurança cibernética, fazem parte da estrutura institucional do Ministério da Defesa. Ademais, o ColCERT também é um grupo do Ministério da Defesa, que coordena a ciberdefesa e a cibersegurança do país, integra militares e civis e atua de forma coordenada com outras entidades e órgãos envolvidos no setor, como o MinTIC, CSIRTs, entidades judiciais, acadêmicas, setor privado, entidades gestoras das IC e outros.

Já Brasil e Argentina possuem estruturas distintas para tratar dos temas da cibersegurança e da ciberdefesa. Conforme Oliveira et al. (2017), de modo geral, os países sul-americanos estruturam sua segurança e sua defesa cibernética de formas diferentes. Alguns atribuem tanto a defesa quanto à segurança cibernética à esfera militar, outros delegam ambas à esfera civil e outros tratam esses temas separadamente, atribuindo a defesa cibernética à esfera militar e a segurança cibernética à esfera civil. No entanto, cabe destacar que mesmo havendo, na teoria, responsabilidades diferenciadas para as instituições civis e as miliares, na prática, as instituições se interligam constantemente, até mesmo pela própria dificuldade em se delinear precisamente os assuntos de segurança cibernética e os assuntos de defesa cibernética, já que as áreas acabam se interligando em vários momentos (PAGLIARI; AYRES PINTO; VIGGIANO, 2020; GRASSI; AYRES PINTO, 2022b).

Além disso, percebe-se, de modo geral, na América do Sul, a militarização da temática cibernética, com as Forças Armadas acumulando funções. Sobre isso, Solar (2020, p. 1, tradução própria) defende que "militarizar o ciberespaço em ambientes políticos frágeis pode se tornar um tanto arriscado para o governo democrático", assim como, "casar a proteção do espaço digital com forças armadas altamente politizadas pode se tornar um desafio ao tentar configurar uma Internet segura e igualitária"[102].

Ainda sobre a estrutura institucional dos países, a Escola Nacional de Defesa Cibernética (EnaDCiber) do Brasil merece destaque, como o braço acadêmico do ComDCiber e com potencial para promover o intercâmbio entre civis e militares nacionais e de países vizinhos. Outras instituições também precisam ser mencionadas como importantes espaços para essas trocas acontecerem, como a Escola Superior de Defesa (ESD), a Escola Superior de Guerra (ESG) e a Escola de Comando e Estado-Maior do Exército (ECEME) no Brasil; a Escola Superior de Guerra da Colômbia; e a Escola Superior de Guerra e o Instituto de Ciberdefesa das Forças Armadas da Argentina. Além disso, instituições civis também devem promover esse intercâmbio e, como mencionado nos documentos e relatórios analisados, promover cursos específicos sobre cibersegurança e ciberdefesa, como o Mestrado em Ciberdefesa e Cibersegurança existente na Universidade de Buenos Aires (UBA).

Por fim, é perceptível que os países sul-americanos precisam avançar em diversos aspectos para alcançar melhores níveis de desenvolvimento, segurança e defesa cibernética.

---

[102] *"[...] militarising cyberspace in fragile political and policy settings can become somewhat risky for democratic governing. [...] marrying the protection of the digital space to highly politicised armed forces might turn into a challenge when trying to set up a secure and egalitarian internet*." (SOLAR, 2020, p. 1)

Diante disso, processos de cooperação com os vizinhos sul-americanos tornam-se via possível para superar entraves na construção de capacidades, já que, a partir da avaliação e das comparações realizadas, puderam ser observadas similaridades e complementaridades na construção de cibercapacidades dos países, bem como em direcionamentos estratégicos para o setor. Nesse sentido, apesar dos obstáculos a serem superados, contemplam-se oportunidades para os Estados traçarem estratégias cooperativas também no campo cibernético.

5 CONSIDERAÇÕES FINAIS

A pesquisa desenvolvida nesta tese de doutorado teve por intuito investigar as potencialidades para o desenvolvimento de processos de cooperação cibernética na América do Sul com vistas à construção de capacidades cibernética pelos Estados. Isso porque identificou-se que grande parte dos estudos sobre cibernética nas Relações Internacionais partem de perspectivas que frisam as desconfianças, as ameaças latentes e as possibilidades de conflitos e, diante disso, a construção de capacidades passa a ser perseguida por um prisma competitivo e de modo individualizado.

No entanto, novos pontos de vista vêm ganhando força nesse campo, os quais destacam as perspectivas cooperativas, o desenvolvimento da diplomacia na área e realçam que a era digital demanda respostas diferenciadas e inovadoras. Esses estudos partem da concepção de que o ciberespaço transcende as tradicionais fronteiras físicas e torna os atores ainda mais interdependentes, principalmente devido à interconectividade das redes e a transnacionalidade desse ambiente. Ainda, considerando as características do ciberespaço, medidas de transparência e de confiança tornam-se fundamentais para evitar uma progressiva militarização do ciberespaço, a escalada de conflitos e a instabilidade do sistema.

Nesse sentido, compreendendo o contexto sul-americano, no qual, historicamente, diversas iniciativas de cooperação foram construídas, inclusive abrangendo agendas sobre segurança e defesa cibernética; e analisando as fragilidades estruturais que esses países enfrentam - e que travam o avanço de programas e projetos em diversas áreas, dificultam sua construção de capacidades, fazem com que fiquem mais expostos frente às crescentes ameaças cibernéticas e mais vulneráveis diante às interferências de potências estrangeiras -, chegou-se a problemática delimitada para o desenvolvimento da pesquisa. Essa problemática envolve a construção de capacidades cibernéticas na América do Sul a partir de uma perspectiva cooperativa.

Diante disso, a pergunta de partida foi determinada da seguinte forma: Quais as potencialidades para a construção de capacidades cibernéticas na América do Sul por meio de processos cooperativos regionais se analisado o contexto geopolítico regional e, particularmente, se comparadas as políticas e estratégias cibernéticas da região? Adicionalmente, surgiu um questionamento secundário ou auxiliar, sendo este: Quais obstáculos os países da América do Sul enfrentam – e que precisariam, portanto, serem

superados - para o desenvolvimento de processos cooperativos para a construção de capacidades cibernéticas?

Dentro da delimitação proposta, a pesquisa foi desenvolvida em 3 módulos, os quais foram subdivididos em 8 partes. Assim, na primeira parte, partiu-se de uma análise teórica e conceitual, na qual foi possível discutir como se configura o ciberespaço, suas principais características, dinâmicas geopolíticas e as ameaças provenientes, além de apresentar conceitos introdutórios à temática. Sobre isso alguns elementos cabem destaque.

Por suas características, entre elas a transversalidade, a possibilidade de anonimato, a velocidade da ação, o baixo custo - comparativamente aos recursos tradicionais de poder - e o grande fluxo de informações que perpassa esse meio, o ciberespaço e os recursos cibernéticos tornaram-se centrais nas dinâmicas de poder e controle no século XXI. Ademais, são particularmente importantes para os países do Sul Geopolítico – do qual os países sul-americanos fazem parte - também por contribuírem para o desenvolvimento dos Estados e possibilitar, entre seus resultados, maiores margens de segurança e poder no sistema internacional, principalmente diante das interferências de potências externas em seus territórios.

Adicionalmente, cabe destacar que os aspectos gerais que conformam esse espaço não devem ser identificados como “fatalidades tecnológicas”, uma vez que, como um espaço artificial, criado pelo ser humano, suas características são consequências de escolhas políticas e podem, portanto, serem modificadas e remodeladas no futuro.

Diante da relevância desse novo domínio para as relações de poder, atores estatais e não-estatais utilizam as ferramentas cibernéticas para influenciar, exercer controle e alcançar seus objetivos estratégicos. Assim, espionagens, sabotagens, interferências híbridas, crimes e ataques cibernéticos diversos - inclusive, direcionados às infraestruturas críticas - são algumas das ameaças enfrentadas no ciberespaço. Isso leva a discussões sobre o grande potencial de danos a partir dessa esfera e, diante disso, surgem questionamentos sobre como os Estados devem abordar esses novos recursos à disposição da política, sobretudo, diante da possibilidade de realização de conflitos nesse espaço. Essas discussões têm levado, inclusive, a complexas proposições sobre limites de atuação, estabelecimento de fronteiras e controles e a delimitação do território soberano do ciberespaço.

Após as contextualizações realizadas na primeira parte desse módulo, a segunda parte trouxe as capacidades cibernéticas para o centro da discussão, abordando conceitos,

identificando seus componentes e relacionando a construção de capacidades à preservação da segurança dos Estados e à obtenção ou manutenção de poder no sistema internacional. Além disso, explorou os estudos que três importantes centros internacionais de pesquisa têm conduzido, nos quais estabelecem dimensões e indicadores para avaliar as capacidades cibernéticas dos Estados. Os três índices selecionados foram: o *Global Cybersecurity Index* da UIT da ONU; o *National Cybersecurity Index*, do *think tank* e-Governance Academy; e o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações, desenvolvido pelo GCSCC da Universidade de Oxford, o qual é a base para o relatório de cibersegurança na América Latina e o Caribe, desenvolvido pelo OEA em parceria com o BID.

Os aportes trazidos por esses institutos e seus índices auxiliam na compreensão dos componentes necessários para a construção de capacidades e, através da avaliação e classificação dos Estados, permitem identificar as lacunas que estes precisam superar, orientando a formulação e o aperfeiçoamento de suas estratégias na área. Apesar disso, eles trazem compreensões e resultados distintos sobre o tema, já que partem de metodologias diferenciadas. Isso também é consequência da falta de consenso sobre os conceitos no âmbito cibernético - particularmente no que se trata de capacidade cibernética e dos componentes que a estruturam. Ainda assim, os índices são de extrema relevância para o avanço dos estudos sobre a temática, trazendo contribuições significativas que são, inclusive, utilizadas por países sul-americanos para avaliar seus avanços e nortear suas estratégias no setor.

Nesse primeiro módulo da investigação, portanto, pode-se compreender o contexto geopolítico que envolve o ambiente cibernético, as ameaças envolvidas e a importância da construção de capacidades pelos Estados. Essas capacidades, entretanto, não podem ser compreendidas apenas como competências técnicas e desenvolvimento tecnológico, pois este é um campo dinâmico que envolve múltiplos fatores, os quais precisam ser sustentados ao longo do tempo para gerarem resultados efetivos aos Estados. Nesse sentido, a construção de capacidades cibernéticas envolve medidas legais, técnicas, organizacionais, políticas e diplomáticas. Fundamenta-se na educação (em todos os níveis), na conscientização, na formação e no treinamento do capital humano, no investimento em ciência, pesquisa e desenvolvimento tecnológico nacional, bem como na promoção de um ambiente digital confiável e seguro. Abrange a formulação de políticas e estratégias coerentes à realidade do Estado, a criação de organismos e a coordenação entre os diversos setores - privado, público e acadêmico - que estão envolvidos nos processos cibernéticos nacionais. Também abrange a

capacidade de se inserir de forma ativa nas discussões internacionais sobre a temática e cooperar com outros atores internacionais.

O processo de construção de capacidades, conforme discutido, é crucial para os países do Sul Geopolítico e, nesse contexto, os países sul-americanos. Para isso, medidas de cooperação poderiam configurar-se como elementares na busca por superar as lacunas tecnológicas, de infraestrutura e as dificuldades orçamentárias que possuem. As iniciativas cooperativas poderiam resultar em compartilhamento de experiências e informações, propiciar o intercâmbio entre especialistas, acadêmicos, militares e profissionais de modo geral, visando o treinamento, a formação e a capacitação dos – também escassos - recursos humanos desses países. Ainda, torna-se relevante coordenar posições para fazer frente e aumentar o poder de barganha desses países nas instâncias internacionais de discussão e tomada de decisão sobre padrões, normas e processos de governança cibernética.

Assim, o segundo módulo desta tese buscou justamente tratar da cooperação internacional em matéria de cibersegurança e ciberdefesa e aproximar essa discussão do cenário sul-americano. Em vista disso, abordou-se o campo da diplomacia cibernética, a qual se conforma como um campo da diplomacia, crucial nas relações internacionais contemporâneas, voltando o uso dos recursos diplomáticos para proteger os interesses nacionais e garantir a estabilidade do ciberespaço, incluindo na agenda temas relacionados ao crime cibernético, capacidades cibernéticas, construção de confiança e governança da internet e outros. A diplomacia cibernética facilita a criação de canais de comunicação e negociação entre os Estados, o estabelecimento de parcerias e a coordenação de suas atuações para que alcancem seus interesses na arena internacional. Nessa direção, países mais desenvolvidos, como os Estados Unidos, já estão desenvolvendo documentos estratégicos e organizando sua agenda frente à temática, visando fortalecer sua liderança na área.

Da mesma forma, fóruns e organismos internacionais, como a ONU e a UIT, a OTAN, a OEA, a UE e, inclusive, a UA e os BRICS, têm trazido para a agenda de discussão ou intensificado seu diálogo sobre questões cibernéticas. De modo semelhante, a Unasul iniciou planos de ação sobre ciberdefesa, ainda em 2012, e o Mercosul tem buscado desenvolver – ainda que muito timidamente - acordos na área da segurança da informação e da segurança cibernética.

Em relação ao contexto sul-americano, buscou-se compreender as diversas ameaças que esse grupo de países enfrenta, delineando a especial importância de construírem

capacidades cibernéticas. A América do Sul é considerada uma região estratégica e que tem, diante disso, sofrido os diversos impactos da acirrada competição geopolítica e tecnológica internacional. O subcontinente é rico em recursos estratégicos, desde recursos biológicos e ambientais, minerais e energéticos. Esses recursos são estratégicos por serem cruciais para o processo de acumulação capitalista, para a indústria, para a geração de energia, para o desenvolvimento científico-tecnológico, para as comunicações e transportes ou simplesmente para a manutenção da vida humana.

A água, o solo, a biodiversidade, o petróleo e o lítio são alguns dos muitos recursos que intensificam os interesses internacionais perante a região. Esses interesses e a atuação das grandes potências na América do Sul resultam em cenários desestabilizadores, acentuam polarizações e geram instabilidades políticas e econômicas. Diante desses cenários, essas potências são capazes de aumentar a dependência dos países e ampliar a dominação sob a região. Nesse sentindo, os recursos cibernéticos tornam-se chave nas estratégias geopolíticas das grandes potências, já que por meio deles podem atuar de modo mais sutil, indireto e menos conflitivo, difundindo agendas de interesse para manter a influência e alcançar seus objetivos estratégicos. Dessa forma, podem atuar através de fórmulas cooperativas e cooptativas, por meio de acordos econômico-comerciais ou parceria estratégicas em diversas áreas, ou, ainda, utilizando-se de meios subversivos, interferências híbridas, ciberespionagem, recorrendo ao arsenal cibernético a disposição dessas potências.

Para mais, conforme os dados apontados nessa segunda parte do segundo módulo, a América do Sul vem sofrendo fortemente com os crimes cibernéticos, que deixam vulneráveis seus sistemas, suas infraestruturas e os dados dos seus cidadãos. Todos os elementos apontados colocam a América do Sul, seus regimes democráticos e sua soberania, suas dinâmicas econômicas e sua coesão interna em risco. Para além disso, demonstram a urgência de os países sul-americanos desenvolverem suas capacidades a partir de estratégicas diversificadas, inclusive com o estabelecimento de amplos projetos regionais, para fazer frente às ameaças existentes e aumentar o poder regional diante das pressões internacionais.

Partindo disso, a última parte do segundo módulo voltou sua atenção aos processos de cooperação e integração implementados na América do Sul. A região desenvolveu historicamente diversas iniciativas cooperativas, culminando, na primeira década do século XXI, na criação de um organismo regional amplo que uniu os 12 países sul-americanos e promoveu o diálogo em ampla gama de temas. A Unasul possibilitou a coordenação de ações na área da saúde, educação, democracia, tecnologia, infraestrutura, narcotráfico, crime

transnacional e, inclusive, defesa cibernética. Assim, em 2012, no âmbito do CDS, os países iniciaram conversações e propuseram planos de ação que visavam, incialmente, definir conceitos comuns na área. A partir disso, pretendiam estabelecer uma rede de contatos e trocas de informações e experiências, desenvolver programas de educação, capacitação e desenvolvimento tecnológico entre os Estados, promover exercícios conjuntos, implementar uma política regional de defesa cibernética e criar mecanismos regionais para combater as ameaças cibernéticas. Visavam, ainda, estabelecer posições comuns para atuar em bloco nas instâncias internacionais de discussão.

Apesar das ambições dos projetos propostos, o grupo não obteve resultados concretos. A polarização política e s crises econômicas que se acentuaram na região, somadas aos problemas estruturais que esses projetos já enfrentavam, levaram a descontinuidades das iniciativas frente ao desmantelamento da Unasul e a fragilização das demais iniciativas regionais, inclusive do Mercosul. Diante disso, os países têm optado por recorrer a organismos hemisféricos ou extrarregionais, engajando-se em iniciativas que historicamente possuem forte influência dos Estados Unidos e, consequentemente, perpetuando a relação de dependência desses países.

Apesar desse cenário e dos grandes desafios para implementar agendas de cooperação regional no contexto atual, as iniciativas levadas a diante, demonstraram o potencial que a América do Sul possui para o diálogo conjunto em variadas agendas e para a resolução das questões internas sem a necessidade de recorrer a soluções externas à região, aumentando, assim, sua autonomia. Além disso, conforme discutido ao longo do segundo módulo da pesquisa, a realidade geopolítica da América do Sul aproxima esse grupo de países e demonstra os ganhos que podem se originar da maior coordenação regional.

Ainda, como ressaltado, entre as vantagens de projetos conjuntos na área, afirma-se que coordenar ações pode garantir a estabilidade regional, melhorar as condições dos países se desenvolverem neste setor, diminuir os custos envolvidos na construção de capacidades, além de possibilitar, no longo prazo, a redução da dependência em relação às potências do Norte, detentoras e exportadoras das soluções tecnológicas. Ressaltou-se também, como uma iniciativa particularmente interessante, o aprofundamento da cooperação em inteligência, como já o fazem países como Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia (Five Eyes).

Por fim, o último módulo desta tese foi dividido em três partes e buscou examinar como os países sul-americanos se encontram no processo de construção de capacidades, com atenção especial aos três países selecionados para esta pesquisa (Argentina, Brasil e Colômbia) – que, conforme apresentado, estão entre os expoentes cibernéticos regionais, são países que também se destacam no contexto geopolítico e securitário sul-americano e que possuem potencial para liderar processos cooperativos na região. A partir disso, pretendeu-se compreender elementos de similaridade e complementaridade entre os países e analisar pontos de divergências e convergências em suas políticas e estratégias cibernéticas.

Por conseguinte, partiu-se da análise das dimensões e indicadores especificados pelos índices internacionais indicados. Os dados obtidos permitiram a identificação de similaridades e complementaridades no processo de construção de capacidades. Em outras palavras, e conforme detalhado na primeira parte do módulo em questão e nas considerações parciais desse capítulo, existem áreas em que os países se encontram em graus similares de maturidade cibernética e/ou precisam avançar em objetivos semelhantes. Por outro lado, observam-se tópicos nos quais um ou mais países se destacam em relação aos demais, sendo que nesses tópicos também podem desenvolver projetos para intercâmbio de conhecimentos, experiências ou habilidades.

Em um segundo momento, analisou-se os dados relativos à C&T e a discussão sobre o papel da educação, da conscientização e da formação de recursos humanos, devido à compreensão de que esses são pilares estruturantes da construção de capacidades, por sustentarem o desenvolvimento das demais dimensões. Sobre isso, particularmente, constatou-se o atrasou dos países sul-americanos e o longo caminho que precisam percorrer para conquistar sua soberania digital. Esse caminho também pode ser percorrido de forma coordenada para sustentar ganhos mútuos.

Por fim, a terceira parte do módulo três, explorou documentos oficiais de Brasil, Colômbia e Argentina, buscando analisar as temáticas que destacam em suas políticas e estratégias cibernéticas, como definem alguns conceitos da área, a relevância delegada ao fator humano e ao desenvolvimento científico e tecnológico nacional, como estruturam e organizam as áreas de cibersegurança e ciberdefesa e, principalmente, quais perspectivas são dadas ao tema da cooperação internacional e, particularmente, à cooperação com o entorno geopolítico sul-americano.

Novamente, os documentos demonstraram, de modo geral, diversas convergências entre os países, os quais ressaltam, como eixos prioritários de atuação, a formação e a

retenção de recursos humanos qualificados para atuar na área, a promoção da educação cibernética e a conscientização da população em geral, bem como o desenvolvimento da C&T e da P&D nacional. Ressaltam também a importância da atuação conjunta entre o setor público, o setor privado e a academia, bem como com toda a sociedade, através de uma abordagem integrada e promoção de esforços conjuntos.

Em termos de cooperação internacional, os documentos também trouxeram essa abordagem, alguns de forma mais aprofundada e detalhada, outros de modo mais superficial. No entanto, nas estratégias de cibersegurança dos três países a cooperação internacional esteve presente de modo significativo. No Brasil, "cooperação internacional e parcerias estratégicas" é um tópico posto como "eixo transformador" e como ação estratégica a ser desenvolvida. A Colômbia descreveu, na Conpes 3854/2016, como objetivo estratégico "Promover a cooperação, colaboração e assistência em matéria de segurança digital, a nível nacional e internacional". Por sua vez, a Argentina delimitou a cooperação internacional como um dos princípios orientadores. Ademais, os três identificaram a relevância de participarem de organismos internacionais, contribuírem para a consecução de normas internacionais sobre o tema e promoverem o intercâmbio técnico, a troca de informações e experiências e promoverem parcerias visando o progresso científico e tecnológico e o desenvolvimento nacional.

A cooperação cibernética com a América do Sul esteve presente em alguns dos documentos analisados, observando-se, de modo geral, a disposição em cooperar com seu entorno geopolítico, visando garantir a estabilidade, o desenvolvimento e a segurança regional. A Colômbia, particularmente, aponta a intenção de tornar-se um líder regional na área, estimulando a cooperação para a promoção de boas práticas, intercâmbio de conhecimento e experiências, visando o desenvolvimento de políticas de ciberdefesa e cibersegurança na região.

Contudo, também se observaram elementos dissonantes, como nas definições de alguns termos centrais, os quais precisariam ser contornados para não se tornarem entraves em processos cooperativos ou, até mesmo, se tornarem elementos de desconfiança entre os países. Nessa perspectiva, observa-se que o primeiro passo para essa superação, que já estava sendo levado a diante no CDS da Unasul, seria criar um arcabouço comum, primeiramente em termos conceituais e, posteriormente, desenvolver uma política regional, seguida de mecanismos para coordenar ações, promover o diálogo e desenvolver os projetos

identificados como necessários. Iniciativas nessa direção precisariam ser retomadas e poderiam ocorrer em diferentes níveis, de modo a abranger os variados estágios que se encontram os países sul-americanos.

Ademais, a estrutura institucional desses Estados também apresenta distinções. Enquanto Brasil e Argentina possuem estruturas civis para lidar com a segurança cibernética e estruturas militares responsáveis pela defesa cibernética, a Colômbia possui estruturas militares responsáveis por ambas as áreas de cibersegurança e ciberdefesa – inclusive, colocando ambas as áreas no arcabouço da denominada segurança digital. Apesar disso, nos últimos anos, é possível observar que outras instituições civis têm ganhado destaque nas dinâmicas que envolvem a cibersegurança e a ciberdefesa da Colômbia. Isso passa pelo entendimento de que essas novas ameaças requerem constante revisão e desenvolvimento de novas dinâmicas para lidar com os desafios impostos. Mesmo diante disso, os delineamentos das políticas de segurança e defesa colombianas ficam concentrados no âmbito militar.

Em vias de conclusão, apesar das históricas assimetrias regionais, dos múltiplos desafios internos que os países enfrentam e dos diferentes estágios de construção de capacidades cibernéticas que os Estados se encontram, observa-se que o contexto geopolítico os aproxima. Isso porque, visto 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; porém, por outra perspectiva, esses desafios têm o potencial de os aproximar, partindo do entendimento que podem conjugar esforços aspirando diminuir suas debilidades particulares e construir capacidades de forma mais autônoma, ou seja, menos dependente dos países do Norte. Ademais, 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.

Em suma, pode-se dizer que foram comprovadas as hipóteses 1 e 2 desta pesquisa. Ou seja, (1) existem similaridades nos desafios que os países sul-americanos enfrentam e complementariedades no setor cibernético que tornam um processo de cooperação regional um meio viável para a redução das fragilidades individuais na construção de capacidade cibernética. Além disso, (2) observando o cenário regional, defendeu-se que as dinâmicas

cooperativas entre os países sul-americanos nas últimas décadas são demonstrativos do potencial regional para a construção de processos cooperativos também na área cibernética.

No que diz respeito à terceira hipótese, acredita-se que ela tenha não tenha sido inteiramente comprovada. Explica-se: a hipótese afirmava que a polarização e as assimetrias regionais e, particularmente, as distinções nos fundamentos das políticas e estratégias cibernéticas dos Estados (que perpassam as percepções estratégicas dos países acerca do espaço cibernético e sua atuação na área) tornavam-se entraves no desenvolvimento de processos cooperativos mais amplos entre os países. Efetivamente, as assimetrias e polarizações tornam-se empecilhos, bem como as interferências externas à região que podem ser compreendidas como pressões desestabilizadoras no cenário regional. Quanto as percepções estratégicas, essas não são de todo dissonantes, já que foram encontrados também diversos elementos de convergência ao explorar os documentos dos três países objetos de análise mais aprofundada.

Reitera-se, assim, a importância de desenvolver perspectivas que levem em consideração as particularidades do cenário local e regional, que observem as variáveis específicas do contexto analisado, para a formulação de estratégias coerentes para o desenvolvimento de capacidades cibernéticas. Nessa perspectiva, explorando o contexto sul-americano, argumenta-se que podem ser desenvolvidos amplos projetos de cooperação que envolvam as diversas áreas nas quais esse grupo de países enfrenta desafios similares e, assim, colaborarem para encontrar as soluções conjuntamente, Ou, então, nas áreas em que podem identificar complementaridades, ou seja, em que os países possam se ajudar mutuamente nos aspectos em que cada um possui melhores resultados, que dispõe de maiores conhecimentos, experiências ou habilidades, propiciando, assim, um ambiente com ganhos mútuos.

Finalmente, ambiciona-se que esta pesquisa tenha cumprido seu papel principal, demonstrando caminhos possíveis e desafios a serem superados para uma efetiva cooperação sul-americana visando a construção de capacidades cibernéticas, a partir da compreensão de um espaço regional próspero para que medidas cooperativas tomem forma e fortaleçam a região como um polo de poder frente a um cenário internacional cada vez mais competitivo.

Ainda, cabe destacar que além da ampla revisão bibliográfica encontrada nesse trabalho, dos documentos levantados, dos índices internacionais apresentados, da perspectiva distinta que se buscou trazer para a investigação e, claro, das análises e resultados obtidos,

tem-se a expectativa de que essa pesquisa tenha oferecido outras contribuições ao leitor interessado. Assim, além de ensejar que este trabalho sirva de base e traga aportes teóricos e analíticos para acadêmicos e demais interessados em compreender e/ou estudar a temática, espera-se que ele instigue novos olhares para a temática e desperte interesses de pesquisa frente as grandes lacunas que ainda existem e dos múltiplos caminhos de investigação que área pode despertar ao pesquisador atraído pelo tema.

A presente tese trouxe para a discussão alguns desses tópicos, mas também indicou diversas possibilidades de agendas de pesquisa que podem e precisam ser desmembradas e aprofundadas. A construção de capacidades no Sul Geopolítico a partir da compreensão das particularidades de cada país, traçando panoramas e buscando soluções que levem em consideração o contexto em que se encontram é um caminho de pesquisa que tem muito a ser explorado. Compreender e comparar as diferentes estratégias desenvolvidas pelos Estados, estudar tópicos relacionados à geopolítica cibernética e às relações de poder no ciberespaço, analisar as agendas de discussão nos fóruns e organismos internacionais, os direcionamentos que têm sido dados no âmbito da governança internacional e outras questões referentes à cooperação cibernética internacional e, particularmente, um campo com análises ainda muito escassas no Sul Geopolítico, mas que vem tomando espaço na agenda política-estratégica de países mais desenvolvidos, é a diplomacia cibernética. Essas são apenas algumas agendas levantadas ao longo desta tese dentro de um campo de pesquisa bastante fértil como são os estudos cibernéticos nas Ciências Sociais e Humanas e, particularmente, nas Relações Internacionais.

REFERÊNCIAS

LIVROS E CAPÍTULOS DE LIVROS:

AYRES PINTO, Danielle Jacon; FREITAS, Riva Sobrado de; PAGLIARI, Graciela de Conti. Fronteiras virtuais: um debate sobre segurança e soberania do estado. p. 40-53. In.: AYRES PINTO, Danielle Jacon; FREIRE, Maria Raquel; CHAVES, Daniel. **Fronteiras Contemporâneas Comparadas: desenvolvimento, segurança e cidadania**. Macapá: Editora da UNIFAP, 2018.

BRITO, Amanda; CASTRO, Maria Carolina de. O Mapeamento Documental da Segurança e da Defesa Cibernética da República Popular da China. In: AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria. **A Geopolítica das Estratégias em Defesa Cibernética: Como os EUA, China, Rússia e Israel Protegem seu Ciberespaço**. Rio de Janeiro: Alpheratz, 2021.

BUSSO, Anabella. Los desafíos de América de Sur frente a Estados Unidos en la segunda década del siglo XXI. In: PASSOS, Rodrigo Duarte Fernandes dos; FUCCILLE, Alexandre (Org.). **Visões do Sul: crise e transformações do sistema internacional**. Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2016.

CARTER Lionel; BURNETT, Douglas R. Subsea Telecommunications. In: SMITH, Hance D.; VIVERO, Juan Luis Suárez de; AGARDY, Tundi S. (Ed.). **Routledge Handbook of Ocean Resources and Management.** London: Routledge, 2018.

CASARÕES, Guilherme. Eleições, política externa e dos desafios do novo governo brasileiro. In: SERBIN, Andrés; PEDROSO, Carolina Silva; PONT, Andrei Serbin (Ed.). **América Latina y el Caribe en un mundo en transición: actores extrarregionales y estrategias latinoamericanas**. Pensamiento Propio, Buenos Aires, n. 49-50, ano 24, 2019.

CHENOU, Jean-Marie; FUERTE, Juan Sebastián Rojas. The Difficult Path to the Insertion of the Global South in Internet Governance. In: OPPERMANN, Daniel (ed.). **Internet Governance in the Global South: History, Theory, and Contemporary Debates**. São Paulo: NUPRI/USP, 2018.

CHOUCRI, Nazli. **Cyberpolitics in international relations**. Cambridge, MA: MIT Press, 2012.

CURRAN, Kevin; CONCANNON, Kevin; MCKEEVER, Sean. Cyber terrorism attacks. In: JANCZEWSKI, Lech J.; COLARIK, Andrew M. **Cyber warfare and cyber terrorism**. New York, 2008.

FRIEDMAN, George. **A próxima década**. Ribeirão Preto: Novo Conceito, 2012.

GADY, Franz-Stefan; AUSTIN, Greg. **Russia, the United States and cyber diplomacy**: opening the doors. New York: EastWest Institute, 2010.

GRANATO, Leonardo. **Brasil, Argentina e os rumos da integração: o Mercosul e a Unasul**. Curitiba: Appris, 2015.

GULLO, Marcelo. **Argentina-Brasil: a grande oportunidade**. Rio de Janeiro: MauadX, 2006.

HERRERA, Geoffrey L. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In: CAVELTY, Myriam Dunn; MAUER, Victor; KRISHNA-HENSEL, Sai Felicia (Ed.). **Power and security in the information age: investigating the role of the state in cyberspace.** Burlington: Ashgate Publishing Company, 2007.

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

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

MARIANO, Karina P.; RIBEIRO, Karina P. Regionalismo na América Latina no século XXI. In SALATTI, Rafael (ed.). **Cultura e direitos humanos nas relações internacionais: reflexões sobre cultura.** São Paulo: Cultura Acadêmica, 2016.

MONIZ BANDEIRA, Luiz Alberto. **Geopolítica e política exterior: Estados Unidos, Brasil e América do Sul.** Brasília: Fundação Alexandre de Gusmão, 2009.

NYE JR, Joseph S. **The future of power**. New York: Public Affairs, 2011.

OLIVEIRA, Marcos Aurelio 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.

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: OLIVEIRA, Marco Aurélio (Org.). **Defesa Cibernética e Mobilização Nacional**. Recife: Ed. UFPE, 2020. P. 153-174.

PARIKH, Riddhita. An Introduction to Cybercrime and Cybersecurity The Whys and Whos of Cybersecurity. In: VAJJHALA, Narasimha Rao; STRANG, Kenneth David (Ed.). **Cybersecurity for Decision Makers**. Boca Raton: CRC Press– Taylor & Francis Group, 2023.

PECEQUILO, Cristina Soreanu. **Os Estados Unidos e o século XXI**. São Paulo: Elsevier, 2012.

QUIVY, Raymond; CAMPENHOUDT, Luc Van. **Manual de investigação em ciências sociais.** 2.ed. Lisboa: Gradiva, 1998.

RIGGIROZZI, Pía; TUSSIE, Diana. The rise of post-hegemonic regionalism in Latin America. In RIGGIROZZI, Pía; TUSSIE, Diana. (ed.). **The Rise of Post-Hegemonic Regionalism.** Dordrecht: Springer, 2012.

RISK STEERING COMMITTEE. **DHS Risk Lexicon**. Washington, DC: Department of Homeland Security, September 2010.

SANAHUJA, José A. Regionalismo post-liberal y multilateralismo en Sudamérica: el caso de UNASUR. In SERBIN, Andrés; RAMANZINI JUNIOR, Haroldo. (ed.). **El regionalismo "post–liberal" en América Latina y el Caribe: Nuevos actores, nuevos temas, nuevos desafíos.** Anuario de la Integración Regional de América Latina y el Gran Caribe. v. 9, p. 19-70, 2012.

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

SCHMITT, Michael N. (Ed.). **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge University Press, 2017.

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

DISSERTAÇÕES, TESES E TRABALHOS DE CONCLUSÃO DE CURSO:

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro**. 203 p. Tese (Doutorado em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

CERQUEIRA FILHO, Carlos Roberto de Almeida. **Os arquivos de Snowden: o episódio e os reflexos no Brasil.** 53 p. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) - Escola Superior de Guerra, Rio de Janeiro, 2014.

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.

GRASSI, Jéssica Maria. **Parceria estratégica entre Brasil e Argentina: cooperação nuclear e integração sul-americana no século XXI**. 167p. Dissertação (Mestrado em Integração Contemporânea da América Latina) - Universidade Federal da Integração Latino-Americana (UNILA), Brasil, 2019.

GUIMPEL, Luis Pablo. **A estrutura da Defesa Cibernética na República Argentina e na República Federativa do Brasil, entre os anos 2014 e 2019: um estudo comparado**. 55p. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) - Departamento de Estudos da Escola Superior de Guerra, Rio de Janeiro, 2020.

PEIXOTO JUNIOR, Henrique Lúcio da Cruz. **A Geopolítica da Amazônia: os recursos naturais estratégicos e a presença do Exército Brasileiro**. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.

PINTO, Rafael Cesar Ilha. **A ascensão e o definhamento da Unasul: contingência, trajetória e o protagonismo presidencial**. 315 p. Tese (Doutorado em Ciência Política) – Universidade Federal de Rio Grande do Sul, Porto Alegre, 2019.

PORTELA, Lucas Soares**. Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI**. 147 p. Dissertação (Mestrado em Ciências Militares) - Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2016.

RODRIGUES, Bernardo Salgado. **Geopolítica dos recursos estratégicos sul-americanos no século XXI.** 146 p. Dissertação (Mestrado em Economia Política Internacional) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2015.

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**. 318 p. Tesis (Doctorado en Comunicación) – Universidad Nacional de La Plata, La Plata, Provincia de Buenos Aires, 2020.

SOUZA, Tamires Aparecida Ferreira. **Cooperação em defesa e a região sul-americana: o papel do Conselho de Defesa Sul-americano, da UNASUL**. 171 p. Dissertação de Mestrado em Estudos Estratégicos Internacionais. Universidade Federal do Rio Grande do Sul (UFRGS), Brasil, 2015.

VACZI, N. **Hybrid Wafare: How to Shape Special Operations Forces**. 103 p. Dissertação (Mestre em Ciência e Arte Militar) - Faculdade da Escola de Comando e Estado-Maior do Exército dos Estados Unidos, Fort Leavenworth, Kansas, 2016.

ARTIGOS EM PERIÓDICOS, ANAIS DE EVENTOS ACADÊMICOS E SIMILARES:

AGUIRRE, Mariano; CHAVEZ, Rebecca Bill; ROBLEDO, Marcos. **América Latina ante las crisis de la globalización y el multilateralismo**. Friedrich Ebert Stiftung, Analisis, jan., 2020.

AMIN, Guido. Setor Estratégico Cibernético. In: RAMOS, Carlos Eduardo Franciscis, et al. (Org.). **XXI Ciclo de Estudos Estratégicos – Ciberespaço: a nova dimensão do campo de batalha**, p. 30-44, jul., 2019.

AMIN, Mario Miguel. A Amazônia na geopolítica mundial dos recursos estratégicos do século xxi. **Revista Crítica de Ciências Sociais,** n. 107, p. 17-38, 2015.

ANTONIO, Juan Manuel Aguilar. La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. **Revista de Estudios en Seguridad Internacional**, v. 6, n. 2, p. 17-43, 2020.

ARAÚJO, Flavia Loss de; NEVES, Bárbara Carvalho. Regionalismo, crise venezuelana e a pandemia do COVID-19: o impacto da fragmentação regional no cenário atual (2013-2020). **Conjuntura Austral**, v. 12 n. 58, p. 19-37, abr./jun., 2021

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.

AYRES PINTO, Danielle Jacon; MORAES, Isabela. As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit. **Revista de Estudios Sociales**. n. 74, p. 71-82, out./dez., 2020.

BARRINHA, André; RENARD, Thomas. Cyber-diplomacy: the making of an international society in the digital age. **Global Affairs**. v.3, n. 4-5, p. 353-364, 2017.

BARRINHA, André; RENARD, Thomas. Power and diplomacy in the post-liberal cyberspace. **International Affairs**, v. 96, n. 3, p. 749-766, mai., 2020.

BARROS, Pedro Silva; GONÇALVES, Julia de Souza Borba; SAMURIO, Sofía Escobar. Desintegração econômica e fragmentação da governança regional na América do Sul em tempos de Covid-19. **Boletim de Economia e Política Internacional** (BEPI), n. 27, p. 125-144, mai./ago., 2020.

BERDU, Guilherme Paul. A política externa brasileira frente à espionagem dos EUA. **Cadernos do Tempo Presente**, n. 25, p. 3-30, set./out. 2016.

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.

BORRERO, Rodrigo Cortés. Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. **Revista de Derecho, Comunicaciones y Nuevas Tecnologias**, n. 14, jul./dez., 2015.

BRAGATTI, Milton Carlos; SOUZA, Nilson Araújo. UNASUL: iniciativa de integração regional? Instituição de regionalismo pós-liberal ou contra-hegemônico? Concertação ou coordenação de interesses comuns? (os debates conceituais sobre um processo em construção). **Conjuntura Austral**, v. 7, n. 35, p. 43-51, 2016

BRICEÑO-RUIZ, José. Da crise da pós-hegemonia ao impacto da Covid-19: o impasse do regionalismo latino-americano. **Revista Cadernos de Campo**, n. 29, p. 21-39, jul./dez., 2020.

BRUNN, Stanley D. Towards an understanding of the geopolitics of cyberspace: Learning, re-learning and un-learning, **Geopolitics**, v. 5, n. 3, p. 144-149, 2000.

BRYANT, William D. Resiliency in Future Cyber Combat. **Strategic Studies Quarterly,** v. 9, n. 4, p. 87-107, 2015.

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

CARMO; Corival Alves do; PECEQUILO, Cristina Soreanu. O Brasil e o vácuo de liderança regional: o avanço sino-americano (2011-2016). **Austral: Revista Brasileira de Estratégia e Relações Internacionais**, v. 5, n. 9, p. 54-75, jan./jun., 2016.

CASTILLO, Rubén Darío Laverde; BEJARANO, Miguel Hernández. Ciberseguridad y Ciberdefensa en Colombia. **Revista Avenir**, v. 4, n. 2, p. 25-362020.

CASTRO, Therezinha. Amazônia – Geopolítica do confronto e geoestratégia da integração. **A Defesa Nacional**, n. 755, jan./mar., 1992.

CAVELTY, Miriam Dunn. Europe's cyber-power. **European Politics and Society**, v. 9, n. 3, p. 304-320, 2018.

CEBALLOS, Luis Dario; MAISONNAVE, Marcelo Andrés; LONDOÑO, Carlos Rafael Britto. Soberanía tecnológica digital en Latinoamérica. **Revista Propuestas para el Desarrollo**, ano IV, n. IV, p. 151-167, out. 2020.

CHARAP, S. The ghost of hybrid war. **Survival**, v. 57, n. 6, p. 51-58, 2015.

CLAVERO, Juan Alberto. Posverdad y exposición selectiva a fake news. Algunos ejemplos concretos de Argentina. **Contratexto**, n. 29, p. 167-180, jan./jun., 2018.

COLLETT, Robert. Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. **Journal of Cyber Policy**, v. 6, n. 3. p. 1–20, 2021.

COSTA, Alan Denilson Lima. Centro de Defesa Cibernética. In: RAMOS, Carlos Eduardo Franciscis, et al. (Org.). **XXI Ciclo de Estudos Estratégicos – Ciberespaço: a nova dimensão do campo de batalha**, p. 87-97. jul., 2019.

COSTA, Hugo Bras Martins da; DUARTE, Rubens de Siqueira. Sul Global versus Sul Geopolítico: um debate quanto à pertinência analítica dos conceitos. Austral: Brazilian **Journal of Strategy and International Relations**, 2023. (no prelo)

CREESE, Sadie; DUTTON, William H.; ESTEVE-GONZÁLEZ, Patricia; SHILLAIR, Ruth. Cybersecurity capacity-building: cross-national benefits and international divides. **Journal of Cyber Policy**, v. 6, n. 2, p. 214- 235, 2021.

DAVENPORT, Tara. Submarine Communications Cables and Law of the Sea: Problems in Law and Practice. **Ocean Development & International Law**, v. 43, n. 3, p. 201-242, 2012.

DEMCHAK, Chris; DOMBROWSKI, Peter. Rise of Cybered Westephalian Age. **Strategic Studies Quarterly**, vol. 5, n. 1, p. 32-61, 2011.

DOUZET, Frédérick. Understanding cyberspace with geopolitics. **Hérodote**, v. 152-153, n.1-2, p. 3-21, 2014.

FERNANDES, H. M. M. As novas guerras: o desafio da guerra híbrida. **Revista de Ciências Militares**, Lisboa, v. 4, n. 2, p. 13-40, nov., 2016.

FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão dos conflitos do século XXI. **Relações Internacionais**, mar., p. 53-69, 2012(a).

FERNANDES, José Pedro Teixeira. Utopia, Liberdade e Soberania no Ciberespaço. **Revista Nação e Defesa,** Portugal: Instituto de Defesa Nacional, n. 133. p. 11-31, 2012(b).

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.

FUCCILLE, Alexandre. O Brasil e o Conselho de Defesa Sul-Americano da UNASUL: Um novo modelo de defesa sub-regional?. **VIII Congresso Latinoamericano de Ciencia Política – Asociación Latinoamericana de Ciencia Política (ALACIP),** jul. 2015.

GARCÍA, Jairo Andrés Cáceres. Colombia, estrategia nacional en ciberseguridad y ciberdefensa. **Air & Space Power Journal**, v. 29, n. 1, jan./abr., 2017.

CASTAÑO, Carlos Alberto Gómez; SEGOVIA, Luciano May; VELASCO, Carlos Wilber Franco. **Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional**, Universidad de los Andes, Colombia nov., 2020. Disponível em: https://sistemas.uniandes.edu.co/maestrias/mesi/proyectos/proyecto.php?id=40

GONÇALVES, Rubén Miranda; BRAGATTI, Milton Carlos. Cooperación en el área de defensa en la UNASUR: un balance del Consejo de Defensa Sudamericano y sus limites. **Revista Jurídica da Presidência**, v. 20 n. 120, p. 46-61, fev./mai., 2018.

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. A construção de capacidades na América do Sul. **Campos Neutrais – Revista Latino-Americana de Relações Internacionais**, v. 4, n. 2, p. 52-64, mai./ago., 2022(a).

GRASSI, Jéssica Maria; AYRES PINTO, Danielle Jacon. O Sistema de Defesa Cibernética do Brasil: Dinâmica Civil-Militar e Maturidade Democrática. **Revista Nação & Defesa**, Instituto de Defesa Nacional, Portugal, n. 163, p. 69-91, dez., 2022(b).

GRASSI, Jéssica Maria Grassi; KERR OLIVEIRA. Parceria estratégica Brasil-Argentina no século XXI: cooperação bilateral e desdobramentos para a integração sul-americana (2003-2014). **Oikos**, v. 21, n. 3, p. 116-132, 2022.

GRASSI, Jéssica Maria. **Os crescentes riscos à segurança e defesa dos cabos submarinos e dos dados que trafegam através deles**. Coluna GEPPIC – Grupo de Estudos em Estudos Estratégicos e Política Internacional Contemporânea, 2022. Disponível aqui: https://geppic.ufsc.br/coluna-geppic/

GUTIÉRREZ-COBA, Liliana; RODRÍGUEZ-PÉREZ, Carlos. Estrategias de posverdad y desinformación en las elecciones presidenciales colombianas 2022. **Revista de Comunicación**, v, 22, n. 2, p. 225-242, 2023.

HAESBAERT, Rogério. Região, regionalização e regionalidade: questões contemporâneas. **Antares**. n.3, jan./jun., 2010.

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

HOMBURGER, Zine. The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace, **Global Society**, v. 33, n. 2, p. 224-24, 2019.

JESUS, Ana Beatriz Castro de; OLIVEIRA NETO, Thiago; ARAÚJO DA SILVA, Fredson Bernardino. Breves reflexões sobre o triângulo geopolítico do lítio sul-americano. **Revista Geopolítica Transfronteiriça**, v. 7, n. 2, 2023.

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

KLIMBURG, Alexander. Mobilising Cyber Power. **Survival**, v. 53, n. 1, p. 41-60, 2011.

LIFF, Adam P. Cyberwar: A New 'Absolute Weapon'? the Proliferation of Cyberwarfare Capabilities and Interstate War. **Journal of Strategic Studies**, v. 35, n. 3, p. 401-428, 2012.

LIMA, Maria Regina Soares. Relações interamericanas: a nova agenda sulamericana e o Brasil. **Lua Nova**, n. 90, p. 167-201, 2013.

LOBATO, Luísa Cruz; KENKEL, Kai Michel. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, vol. 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, 2020.

MEYER, Paul. Diplomatic alternatives to cyber-warfare a near-term agenda. **The RUSI Journal**, v. 157, n.1, p. 14-19, 2012.

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. **Conjuntura Austral**, v. 13, n. 61, p. 33–46, 2022.

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. **Revista Brasileira de Estudos Estratégicos**, v. 13, n. 26, p. 25-49, 2021.

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.

OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo. Propaganda Computacional Na Prática: Os Casos de Estados Unidos, França, Colômbia e Venezuela. **XI Encontro Nacional Da Associação Brasileira de Estudos de Defesa** (online), 1–18, 2021.

OLIVEIRA, Renata Peixoto de; CÁCERES, Cynthia Centurión. (Re)configuración o vieja configuración geopolítica hemisférica: la integración de la Región Andina en el comienzo del siglo XXI. **Revista Andina de Estudios Políticos**, v. IV, n. 2, p. 1-17, 2014.

OPPERMANN, Daniel. O cenário de cibersegurança depois de Snowden e consequências no Brasil. **Janus – Anuário de Relações Exteriores**, Lisboa, jun., 2014.

ORJI, Uchenna Jerome. The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? **Masaryk University Journal of Law and Technology**, v.12, n. 2, p. 91–130, 2018.

PAGLIARI, Graciela de Conti. Conselho de Defesa Sul-Americano e a adoção de medidas de fortalecimento da confiança. **Carta Internacional**, v. 10, p. 23, 2015.

PAGLIARI, Graciela de Conti; VIGGIANO, Juliana. Transparência em Defesa: um panorama das medidas de construção de confiança sul-americanas. **Revista Brasileira de Estudos de Defesa**, v. 7, n. 1, 2020.

PALACIOS, José Miguel. Cooperación entre servicios de inteligencia: la dimensión regional. **Revista de Relaciones Internacionales, Estrategia y Seguridad**, v. 16, n. 1, p. 13-28, jan./jun., 2021.

PAUTASSO, Diego; NOGARA, Iago Soares; UNGARETTI, Carlos Renato; RABELO, Ana Maria Prestes. As três dimensões da guerra comercial entre China e EUA. **Carta Internacional**, Belo Horizonte, v. 16, n. 2, p. 1-23, 2021.

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.

PAWLAK, Patryk. Capacity Building in Cyberspace as an Instrument of Foreign Policy. **Global Policy**, v. 7, n. 1, p. 83–92, 2016.

PEREIRA DA SILVA, Armstrong; ABI-RAMIA, Rodrigo de Paula; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria. Onde estivemos e para onde vamos: desafios e perspectivas contemporâneas à integração sul-americana. **Revista de Estudos Internacionais**, v. 13, n. 2, p. 164-192, 2022.

PÉREZ, Yuly Pérez. **Importancia de la Ciberseguridad en Colombia**. Especialización en Seguridad Informática, Universidad Piloto de Colombia, jan., 2017. Disponível em: http://repository.unipiloto.edu.co/handle/20.500.12277/2676

POOL, Phillip. War of the Cyber World: The Law of Cyber Warfare. **International Lawyer**, v. 47, n. 2, p. 299–323, 2013.

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.

PUIG, Juan Carlos. Integración y autonomía de América Latina en las postrimerías del siglo XX. **Integración Latinoamericana**. Buenos Aires, n. 109, p.40- 62, jan./fev., 1986.

RIBEIRO, Fábio Pereira. Cooperação Estratégica em Inteligência Formação da Defesa Regional: uma Contribuição dos Serviços de Inteligência. **Cadernos PROLAM/USP**, v. 1, ano 5, p. 113-128, 2006.

RID, Thomas. Cyber War Will Not Take Place. **Journal of Strategic Studies,** v. 35, n. 1, p. 5–32, 2012.

RODRIGUES, Bernardo Salgado. Guerra Híbrida na América do Sul: uma definição das ações políticas veladas. **Sul Global**, v. 1, n. 1, p. 139-168, 2020.

RODRIGUES, Martha Raquel; LAZARINI, Raíssa Gouveia Ferreira; MADEIRA, Letícia Lacerda; MENON, Gustavo. A criação da ALBA-TCP como alternativa na integração latino-americana. **Revista Lutas Sociais**, v. 26, n. 48, p. 85–106, 2022.

SAINT-PIERRE, Héctor Luis; PALÁCIOS JÚNIOR, Alberto Montoya Correa. As medidas de confiança no Conselho de Defesa Sul-americano (CDS): análise dos gastos em Defesa (2009–2012). **Revista Brasileira de Política Internacional**, v. 57n. 1, p. 22-39, 2014.

SANTOS JUNIOR, João Benedito *et al*. Novas Ameaças e a Cibersegurança: Uma Análise do Sistema Brasileiro de Defesa Cibernética frente ao Caso Da Espionagem durante o Governo Dilma Rousseff. **XVI Congresso Acadêmico sobre Defesa Nacional**. Rio de Janeiro, 25 e 31 de agosto de 2019.

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

SHELDON, John. B. Geopolitics and Cyber Power: Why Geography Still Matters. **American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy**, V. 36, n. 5, p. 286-293, 2014.

SOUZA, Nilson Araújo de. América Latina: as ondas de integração. **Oikos**, v. 11, n. 1, p. 87-126, 2012.

STONE, John. Cyber War Will Take Place! **Journal of Strategic Studies,** v. 36, n. 1, p. 101–108, 2013.

TEIXEIRA, Carlos Gustavo Poggio; DATYSGELD, Mark William. Os clientes diplomáticos e econômicos da espionagem digital estadunidense: Análise das ações contra o Conselho de Segurança da ONU e a Petrobras. **Estudos Internacionais**: Revista de Relações Internacionais da PUC Minas, v, 4, n. 1, p. 71-87. 2017.

TEIXEIRA Jr., Augusto W. M. Geopolítica e Postura Estratégica dos Estados Unidos na Crise da Venezuela. CEEEX - Centro de Estudos Estratégicos do Exército, v. 8, n. 1, p. 7-25, jan./jun, 2020(a).

TEIXEIRA Jr., Augusto W. M. O Entorno Estratégico Brasileiro na Geopolítica das Grandes Potências: a Crise da Venezuela e seus Impactos para o Brasil. **CEEEX - Centro de Estudos Estratégicos do Exército**, v. 15, n. 1, p. 7-24, dez./fev., 2020 (b).

VENTRE, Daniel. Ciberguerra. In: MINISTERIO DE DEFENSA. **Seguridad global y potências emergentes em um mundo multipolar.** XIX Curso Internacional de Defensa. Espanha: Academia General Militar; Universidad Zaragoza, 2012.

VICHI, Leonardo Perin; AYRES PINTO, Danielle Jacon; NERY DE SÁ, André Luiz. A Defesa da Infraestrutura de Cabos Submarinos: por uma interface entre a Defesa Cibernética e a Segurança Marítima no Brasil. **Revista da Escola de Guerra Naval**, v. 26, n. 2, 2020.

VILLAMIL, Ximena Andrea Cujabante; JARA, Martha Lucía Bahamón; VENEGAS, Jair Camilo Prieto; AGUILAR, Jorge Alejandro Quiroga. Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. **Revista Científica General José María Córdova** - Revista colombiana de estudios militares y estratégicos, v.18, n. 30, p. 357- 377, 2020.

WANGLAI, Gao. BRICS Cybersecurity Cooperation: Achievements and Deepening Paths. **China International Studies**, n. 68, jan./fev., 2018.

WIGELL, Mikael. Democratic Deterrence: How to Dissuade Hybrid Interference. **Washington Quarterly**, v. 44, n. 1, p. 49–67, 2021.

WILLETT, Marcus. Assessing Cyber Power. **Survival**, v. 61, n. 1, p. 85-90, 2019.

RELATÓRIOS, NOTAS TÉCNICAS E ARTIGOS ESTRATÉGICOS

AL-KHATIB. Dima. **La cooperación Sur-Sur es esencial para alcanzar los Objetivos de Desarrollo Sostenible.** Organização das Nacões Unidas, 12 de setembro de 2023. Disponível em: https://www.un.org/es/cr%C3%B3nica-onu/la-cooperaci%C3%B3n-sur-sur-es-esencial-para-alcanzar-los-objetivos-de-desarrollo-sostenible

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

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. 19, 2019.

ESET. **Security Report América Latina 2021**. Disponível em: https://web-assets.esetstatic.com/wls/pt/artigos/relatorios/ESET_security_report_2021_PT.pdf

GCSCI – Global Cyber Security Capacity Centre. **Cybersecurity Capacity Maturity Model for Nations (CCMM).** Edição 2021. Disponível em: https://gcscc.ox.ac.uk/CCMM-2021-edition#:~:text=The%20CCMM%202021%20Edition%20and,a%20rigorous%20analysis%20of%20data

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. 16, mai., 2019.

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

KASKA, Kadri. What is the National Cybersecurity Index (NCSI) and how does it work? In: E-Governance Academy. **Upgrading National Cyber Resilience** - National Cybersecurity in Practice 2. Tallin, 2022.

UIT – União Internacional de Telecomunicações / 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.

KALOUT, Hussein; DEGAUT, Marcos. **Brasil, um país em busca de uma grande estratégia**. Secretaria Especial de Assuntos Estratégicos, Relatório de Conjuntura, n.1, maio, Brasília, 2017.

HERCZYNSKI, Pawel. La perspectiva integral de la UE para afrontar las amenazas del ciberespacio. In: BID; OEA. **Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe**. Observatorio de la Ciberseguridad em América Latina y el Caribe, Report Ciberseguridad 2020.

HOHMANN, Mirko; PIRANG, Alexander; BENNER, Thorsten. **Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach.** Global Public Policy Institute (GPPi), Report, 06 mar., 2017.

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.

OEA – Organização dos Estados Americanos. **Educação em Segurança Cibernética: Planejamento do futuro por meio do desenvolvimento da força de trabalho.** Programa de Cibersegurança do Comitê Interamericano contra o Terrorismo, White Paper Series, n. 5, 2020.

SHERMAN, Justin. **Cyber defense across the ocean floor: The geopolitics of submarine cable security.** Report. Atlantic Council, Cyber Statecraft Initiative, set., 2021.

RICYT - Red Iberoamericana de Indicadores de Ciencia y Tecnología. **El estado de la ciencia: Principales Indicadores de Ciencia y Tecnología Iberoamericanos / Interamericanos 2022**. Red Iberoamericana de Indicadores de Ciencia y Tecnología (RICYT). Ciudad Autónoma de Buenos Aires, Argentina, 2022.

SUNAK, Rishi. **Undersea Cables: Indispensable, insecure**. Report. Policy Exchange. London, 2017.

TOSSD - Total Official Support for Sustainable Development. **TOSSD Reporting Instructions**. April 2023. Disponível em: https://www.tossd.org/docs/reporting-instructions.pdf

VAN RAEMDONCK, Nathalie. **Cyber Diplomacy in Latin America**. UE Cyber Direct, Digital Dialogue, 26 jun. 2020. Disponível em: https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america.

DOCUMENTOS OFICIAIS:

Argentina:

ARGENTINA, Ministerio de Defensa. **Directiva de Política de Defensa Nacional**. Ministerio de Defensa, Buenos Aires, 2021. Disponível em: http://www.saij.gob.ar/703-nacional-aprobacion-directiva-politica-defensanacional-dn20180000703-2018-07-30/123456789-0abc-307-0000-8102soterced#.

ARGENTINA, Ministerio de Defensa. **Libro Blanco de la Defensa**. Ministerio de Defensa, Buenos Aires, 2015(a). Disponível em: https://info.undp.org/docs/pdc/Documents/ARG/libro_blanco_2015.pdf.

ARGENTINA, Ministerio de Defensa. **Política de Ciberdefensa**. Anexo I da Resolución 1380/2019. Ministerio de Defensa, Buenos Aires, 25 de outubro de 2019(a). Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/219968/20191029#:~:text=RESOL%2

D2019%2D1380%2DAPN%2DMD&text=CONSIDERANDO%3A,la%20libertad%20de%20sus%20habitantes

ARGENTINA, Ministerio de Defensa. **Resolución 1380/2019**. Ministerio de Defensa, Buenos Aires, 25 de outubro de 2019(b). Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/219968/20191029#:~:text=RESOL%2D2019%2D1380%2DAPN%2DMD&text=CONSIDERANDO%3A,la%20libertad%20de%20sus%20habitantes.

ARGENTINA, República. **Decreto 42/2016.** Modificação, Buenos Aires, 07 de janeiro de 2016. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

ARGENTINA, República. **Decreto 480/2019**. Presidencia de la Nación Argentina. Buenos Aires, 2019(c). Disponível em: https://www.argentina.gob.ar/normativa/nacional/decreto-480-2019-325052/texto

ARGENTINA, República. **Decreto 577/2017**. Comité de Ciberseguridad. Presidencia de la Nación Argentina. Buenos Aires, 28 de julho de 2017. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000- 279999/277518/norma.htm.

ARGENTINA, República. **Disposición 3/2023**. Jefatura de Gabinete de Ministros. Buenos Aires, 04 de julho de 2023(a). Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/289746/20230706.

ARGENTINA, República. **Estrategia Nacional de Ciberseguridad de la República Argentina**. Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización, Buenos Aires, 2019(d). Disponível em: http://www.enre.gov.ar/web/bibliotd.nsf/203df3042bad9c40032578f6004ed613/1e2bd1ba24f72e9b03258408003abee3/$FILE/anexo%201.pdf.

ARGENTINA, República. **Glosario de Términos de Ciberseguridad**. Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización, Buenos Aires, 2019(e). Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/res1523-2.pdf.

ARGENTINA, República. **Ley 25.326 de Protección de Datos Personales**. Senado y Cámara de Diputados. Buenos Aires, 30 de outubro de 2000. Disponível em: https://e-legis-ar.msal.gov.ar/htdocs/legisalud/migration/html/14402.html.

ARGENTINA, República. **Resolución 580/2011.** Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Buenos Aires, 20 de março de 2011. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm.

Brasil:

BRASIL, Ministério da Defesa do. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014(a). Disponível em: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

BRASIL, Ministério da Defesa do. **Doutrina Militar de Defesa Cibernética**. Brasília, 2023. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_doutrina_militar_defesa_cibernetica_2_edicao_2023.pdf.

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.

BRASIL, Ministério da Defesa do. **Livro Branco de Defesa Nacional**. Brasília, 2012(a). Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf.

BRASIL, Ministério da Defesa do. **Livro Branco de Defesa Nacional**. Brasília, 2020(a). Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf.

BRASIL, Ministério da Defesa do. **Política Cibernética de Defesa**. Brasília, 2012(b). Disponível em: https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf.

BRASIL, Ministério da Defesa do. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, 2012(c). Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf.

BRASIL, Ministério da Defesa do. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, 2020(b). Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf.

BRASIL, Presidência da República. **Decreto nº 8793, de 29 de junho de 2016.** Fixa a **Política Nacional de Inteligência.** Brasília, em vigor a partir de 29 de junho de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm.

BRASIL, Presidência da República. **Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação.** Brasília, em vigor a partir de 26 de dezembro de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm

BRASIL, Presidência da República. **Decreto nº 10.222, de 5 de fevereiro de 2020**. **Estratégia Nacional de Segurança Cibernética.** Diário Oficial da União, Ed. 26, seção 1, p. 6, em vigor a partir de 06 de fevereiro de 2020(c). Disponível em: http://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

BRASIL, Presidência da República. **Decreto nº 10569, de 9 de dezembro de 2020. Estratégia Nacional de Segurança das Infraestruturas Críticas**. Brasília, em vigor a partir de 9 de dezembro de 2020(d). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm

BRASIL, Presidência da República. **Lei nº 12.965, de 23 de abril de 2014**. **Marco Civil da Internet do Brasil**. Brasília, em vigor a partir de 23 de abril de 2014(b). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL, Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.** Brasília, em vigor a partir de 14 de agosto de 2020(e). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BRASIL, Presidência da República. **Portaria nº 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação.** Diário Oficial da União, Ed. 190, seção 1, p. 3, em vigor a partir de 26 de setembro de 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663

MANDARINO Jr., Raphael; CANONGIA, Claudia. (Org.) **Livro Verde: Segurança Cibernética do Brasil.** Departamento de Segurança da Informação e Comunicações. Brasília: GSIPR/SE/DSIC, 2010.

TCU - Tribunal de Contas da União. **TC 001.873/2020-2**. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/187320202.PROC/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520?uuid=e052e8c0-3e39-11eb-a2e2-479b45fdaccf.

Colômbia:

COLOMBIA, Congreso de. **Ley 1581 de 2012**. **Regulación de la Protección de Datos Personales de los Individuos.** Em vigor a partir de 17 de outubro de 2012. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

COLOMBIA, Consejo Nacional de Política Económica y Social de. **CONPES 3701: Directrices de política sobre ciberseguridad y ciberdefensa.** Bogotá, 14 de julho de 2011. Disponível em: https://www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf .

COLOMBIA, Consejo Nacional de Política Económica y Social de. **CONPES 3854: Política Nacional de Seguridad Digital.** Bogotá, 22 de janeiro de 2016. Disponível em: https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf.

COLOMBIA, Consejo Nacional de Política Económica y Social de. **CONPES 3975: Politica Nacional para la Transformación Digital e Inteligencia Artificial.** Bogotá, 8 de noviembre de 2019(a). Disponível em: https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/11134.pdf

COLOMBIA, Consejo Nacional de Política Económica y Social de. **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.

COLOMBIA, Ministerio de Defensa Nacional de. **Política de Defensa e Seguridad**. Bogotá, janeiro de 2019(b). Disponível em: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Prensa/Documentos/politica_defensa_deguridad2019.pdf

COLOMBIA, Ministerio de Tecnologías de la Información y las Comunicaciones da. **Agenda Estratégica de Inovación: Ciberseguridad**. Bogotá, mar., 2014. Disponível em: https://www.cncs.gov.pt/content/files/colombia_inovation_agenda_articles-6120_recurso_2.pdf.

COLOMBIA, República de. **Decreto 1874 de 30 de diciembre de 2021**. Disponível em: https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201874%20DEL%2030%20DE%20DICIEMBRE%20DE%202021.pdf

Outros documentos:

AMORIM, Celso. **Los desafios del escenario estratégico del siglo XXI para América del Sur.** Conferencia del Ministro de Estado de la Defensa, Celso Amorim, en el Ministério de Defensa de Argentina. Buenos Aires, 13 de septiembre de 2013.

CONVENÇÃO DE BUDAPESTE – **Convenção sobre Cibercrime**. Budapeste, 21 de novembro de 2001. Disponível em: https://rm.coe.int/16802fa428

GFCE - Global Forum on Cyber Expertise. **Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building**. 24 de novembro de 2017. Disponível em: https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf

MERCOSUL. **III Reunión Ordinaria de la Comisión Ciberseguridad del Grupo Agenda Digital del Mercosur (GAD).** Acta Nº 03/22. Reunião realizada por videoconferência, día 4 de novembro de 2022.

MERCOSUL. **Reunión de Autoridades y Expertos en Seguridad Informática y de las Telecomunicaciones del MERCOSUR**. Acta Nº 01/13. Caracas, 17 de setembro de 2013.

OEA – 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 D.C., Estados Unidos de América, 2004. Disponível em: https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

UNASUL – União das Nações Sul-Americanas. **Acta de la VI Reunión de la Instancia Ejecutiva del Consejo de Defensa Suramericano.** Asunción, 4 de junho de 2012(a).

UNASUL – União das Nações Sul-Americanas. **Plan de Acción**. Consejo de Defensa Suramericano, 2013.

UNASUL – União das Nações Sul-Americanas. **Plan de Acción**. Consejo de Defensa Suramericano, 2014.

UNASUL – União das Nações Sul-Americanas. **Plan de Acción**. Consejo de Defensa Suramericano, 2015.

UNASUL – União das Nações Sul-Americanas. **Plan de Acción**. Consejo de Defensa Suramericano, 2016.

UNASUL – União das Nações Sul-Americanas. **Plan de Acción**. Consejo de Defensa Suramericano, 2017.

UNASUL – União das Nações Sul-Americanas. **Primera Reunión para la Conformación de un Grupo de Trabajo para Evaluar la Factibilidad de Establecer Políticas y Mecanismos Regionales para hacer frente a las Amenazas Cibernéticas o Informáticas en el Ámbito de la Defensa**. Lima, 15 de maio de 2012(b).

UNIÃO AFRICANA. **African Union Cybersecurity Expert Group holds its first inaugural meeting.** Press Release. Directorate of Information and Communication Addis Ababa, Ethiopia, 12 December 2019. Disponível em: https://au.int/sites/default/files/pressreleases/37873-pr-press_release-_african_union_cybersecurity_expert_group_holds_its_first_inaugural_meeting.pdf

U.S. – United States of America. **Cyber Diplomacy Act**. Washington, D.C., 20 de abril, 2021. Disponível aqui: https://www.congress.gov/bill/117th-congress/house-bill/1251/text.

NOTÍCIAS E ARTIGOS EM JORNAIS:

CGI.br. **IX.br completa 15 anos de operação, consolidado entre os maiores Pontos de Troca de Tráfego Internet do mundo.** CGI.br, 03 jul., 2019. Disponível em: https://www.cgi.br/noticia/releases/ix-br-completa-15-anos-de-operacao-consolidado-entre-os-maiores-pontos-de-troca-de-trafego-internet-do-mundo/. Acesso em: 02 set. 2023.

CHAPLEAU, Philippe. 770 nouveaux cyber-combattants vont être recrutés par les armées. **Journal Ouest-France**, setembro de 2021. Disponível em: https://www.ouest-france.fr/politique/defense/770-nouveaux-cyber-combattants-vont-etre-recrutes-par-les-armees-bfdb59dc-109e-11ec-9056-0987937f47bd. Acesso em: 13 mar. 2022.

CRIALES, José Pablo. La inseguridad irrumpe en la campaña electoral argentina aupada por las noticias falsas en redes sociales. **El País**. Buenos Aires, 11 de agosto 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. Acesso em: 12 out. 2023.

EFRONY, Dan. The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence. **Just Security**, 16 de julho de 2021. Disponível em:

https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/#:~:text=Like%20the%20GGE%2C%20the%20OEWG,on%20the%20relevant%20issues%20discussed. Acesso em: 08 ago. 2023.

ENRIQUEZ, Matías. Elecciones 2023: No creas en todo lo que te llega. **Perfil**, 11 de setembro de 2023. Disponível em: https://www.perfil.com/noticias/opinion/elecciones-2023-no-creas-en-todo-lo-que-te-llega.phtml. Acesso em: 12 out. 2023.

GSI - Gabinete de Segurança Institucional da Presidência da República do Brasil**. Governo aprova nova estrutura do GSI.** Notícias. 2023. Disponível em: https://www.gov.br/gsi/pt-br/centrais-de-conteudo/noticias/2023-1/governo-aprova-nova-estrutura-do-gsi. Acesso em 31 out. 2023.

NICAS, Jack. Argentina's Currency Plummets Under Attack from Far-Right Candidate. **The New York Times**, 10 de outubro de 2023. Disponível em: https://www.nytimes.com/2023/10/10/world/americas/argentina-peso-javier-mile.html. Acesso em: 12 out. 2023.

RAULS, Leonie. How Latin American Governments Are Fighting Fake News. **Americas Quartely**, 19 de outubro de 2021. Disponível em: https://americasquarterly.org/article/how-latin-american-governments-are-fighting-fake-news/. Acesso em: 12 out. 2023.

SCOTT, Karen. Laws governing undersea cables have hardly changed since 1884 – Tonga is a reminder they need modernising. **The Conversation**, 21 de janeiro de 2022. Disponível em: https://theconversation.com/laws-governing-undersea-cables-have-hardly-changed-since-1884-tonga-is-a- reminder-they-need-modernising-175312. Acesso em: 03 fev. 2022.

SAMAMA, Pascal. Recherche Cyber-Combattants: L'armée Annonce 770 Recrutements Supplémentaires. **BFM Business**, setembro de 2021. Disponível em: https://www.bfmtv.com/economie/recherche-cyber-combattants-l-armee-annonce-770-recrutements-supplementaires_AN-202109080375.html. Acesso em: 13 mar. 2022.

SITES CONSULTADOS:

ARGENTINA, Jefatura de Gabinete de Ministros de. **Objetivos de la Dirección Nacional de Ciberseguridad.** Disponível em: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/objetivos-de-la-direccion. Acesso em: 28 out. 2023(b).

ARGENTINA, Jefatura de Gabinete de Ministros de. **Oficina Nacional de Tecnologías de Información.** Disponível em: https://www.argentina.gob.ar/jefatura/innovacion-publica/onti. Acesso em: 28 out. 2023(c).

ARGENTINA, Mapa de Estado de. **Jefatura de Gabinete de Ministros**. Coordinación Mapa del Estado, Dirección Nacional de Diseño Organizacional. Atualizada en 25/10/2023(d).

Disponível em: https://mapadelestado.jefatura.gob.ar/estructura.php. Acesso em: 28 out. 2023.

ARGENTINA, Mapa de Estado de. **Ministerios – Ministerio de Defensa**. Coordinación Mapa del Estado, Dirección Nacional de Diseño Organizacional. Atualizada em 25/10/2023(e). Disponível em: https://mapadelestado.jefatura.gob.ar/estructura.php. Acesso em: 28 out. 2023.

CCCD - Comando Conjunto de Ciberdefensa de Argentina. **Cuadro Orgánico**. 2022. Disponível em: https://www.fuerzas-armadas.mil.ar/Comando-Conj-Ciberdefensa/organizacion.html. Acesso em: 15 out. 2022.

CEPAL - Comissão Econômica para a América Latina e o Caribe. **Departamento Nacional de Planeación (DNP) de Colombia**. Observatorio Regional de Planificación para el Desarrollo de América Latina y el Caribe. Disponível em: https://observatorioplanificacion.cepal.org/es/instituciones/departamento-nacional-de-planeacion-dnp-de-colombia. Acesso em 20 out. 2023.

COLOMBIA, Ministerio de Defensa Nacional de. **Estructura Organica**. Disponível em: https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://ce0a04a5c2498890570e035edfe056b1. Acesso em: 20 out. 2023.

CSIRTAmericas. **CSIRTAmericas**. Disponível em: https://csirtamericas.org/en. Acesso em: 06 ago. 2023.

CYBIL PORTAL. **About Cybil**. Disponível em: https://cybilportal.org/about-the-gfce/. Acesso em: 27 ago. 2023.

DLA Piper. **Data Protection Law in the World.** Disponível em: https://www.dlapiperdataprotection.com/index.html?t=world-map&c=AR&c2=BR. Acesso em: 27 out. 2023.

GCSCC - **Global Cyber Security Capacity Centre**. University of Oxford. Disponível em: https://gcscc.ox.ac.uk/home-page. Acesso em: 31 de maio de 2023.

IBP – Instituto Brasileiro de Petróleo e Gás. **Maiores reservas provadas de petróleo em 2020**. Disponível em: https://www.ibp.org.br/observatorio-do-setor/snapshots/maiores-reservas-provadas-de-petroleo-em-2020/. Acesso em 25 set. 2023.

INTERNET WORLD STATS. **Internet Usage and Population in South America**. Março, 2022. Disponível em: https://www.internetworldstats.com/stats15.htm. Acesso em: 18 fev. 2023.

ITU - **International Telecommunication Union**. United Nations, 2020. Disponível em: https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020. Acesso em: 18 fev. 2023.

MERCOSUL. **Agenda Digital**. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/. Acesso em: 06 ago. 2023.

NCSI - National Cyber Security Index. **Description of indicators.** Disponível em: https://ncsi.ega.ee/indicators/. Acesso em: 31 mar. 2023.

OEA – Organização dos Estados Americanos. **Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio.** Disponível em: https://www.oascybercbms.org/es. Acesso em: 06 ago. 2023(a).

OEA – Organização dos Estados Americanos. **Programa de Ciberseguridad**. Disponível em: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp. Acesso em: 06 ago. 2023(b).

ONU – Organização das Nações Unidas. **Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session**. 24 de julho de 2023. Disponível em: https://media.un.org/en/asset/k1o/k1ovl7bhl9#:~:text=The%20Open%2Dended%20Working%20Group,the%20context%20of%20international%20security. Acesso em: 09 set. 2023

OTAN – Organização do Tratado do Atlântico Norte. **Cyber defense**. Disponível em: https://www.nato.int/cps/en/natohq/topics_78170.htm. Acesso em: 01 ago. 2023.

PARLAMENTO EUROPEU. **La política común de seguridad y defensa**. Disponível em: https://www.europarl.europa.eu/factsheets/es/sheet/159/la-politica-comun-de-seguridad-y-defensa. Acesso: 23 set. 2023.

RICYT - Red de Indicadores de Ciencia y Tecnología Iberoamericana e Interamericana. **Reportes comparativos.** Disponível em: http://www.ricyt.org/category/indicadores/. Acesso: 30 set. 2023.

USGS - United States Geological Survey. **Lithium Statistics and Information**. U.S. Geological Survey, Mineral Commodity Summaries, January 2023. Disponível em: https://www.usgs.gov/centers/national-minerals-information-center/lithium-statistics-and-information. Acesso em: 26 set. 2023.

APÊNDICE A – PRINCIPAIS CONCEITOS RELACIONADOS À CIBERNÉTICA NAS RELAÇÕES INTERNACIONAIS

Termo	Autor	Definição
Ciberespaço / Espaço cibernético	Fernandes (2012a, p. 12)	"[...] rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores."
	Singer e Friedman (2014, p. 13, tradução própria)	"[...] o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line. [...] não é apenas um lugar físico [...] não é puramente virtual."
	Kuehl (2009, p. 28, tradução própria)	"[...] é um domínio global dentro do ambiente de informação, cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação."
Ciberpoder / Poder cibernético	Nye Jr. (2011, p. 123, tradução própria)	"[...] um conjunto de recursos relacionados a criação, controle e comunicação da informação eletrônica e computacional – infraestrutura, redes, software e habilidades humanas. Isso inclui não apenas a Internet de computadores em rede, mas também Intranets, tecnologias móveis e comunicações espaciais."
Cibercapacidade / Capacidade cibernética	Pawlak (2016, p. 84, tradução própria)	"[...] desenvolvimento de recursos humanos, arranjos organizacionais e estruturas legais e institucionais [que] visa, em última análise, uma transformação social e política profunda."
	Hurel (2021, p. 09)	"[...] conjunto de iniciativas que visa empoderar indivíduos, sociedades e governos para desfrutarem dos benefícios da digitalização".
Ciberdefesa / Defesa cibernética	Oliveira *et al* (2017, p. 13).	"[...] 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."
Cibersegurança / Segurança cibernética	Oliveira *et al* (2017, p. 14).	"[...] aborda questões políticas, gestão de riscos, melhores práticas de garantia e tecnologias usadas para proteger o ambiente cibernético de um país e suas organizações. De forma mais direta, a segurança cibernética trata de temas relacionados à segurança pública."
	Pawlak (2016, p. 84, tradução própria)	"[...] uma forma de capacitar indivíduos, comunidades e governos para atingirem os seus objetivos de desenvolvimento, reduzindo os riscos de segurança digital decorrentes do acesso e utilização de tecnologias de informação e comunicação"
Ciberataque / Ataque cibernético	Lobato e Kenkel (2015, p. 27, tradução própria)	"[...] uma ação humana que explora as vulnerabilidades da esfera virtual, conseguindo prejudicar os sistemas informacionais ou mesmo, à luz da dependência on-line da vida moderna, da vida diária material."

[continua]

Cibercrime / **Crime cibernético**	Parikh (2023, p. 61, tradução própria)	"[...] são crimes cometidos quando um computador, rede ou qualquer outro meio de tecnologia de informação e comunicação foi usado para cometer um crime. Esses crimes podem incluir uma série de crimes, como crimes económicos, uso indevido da identidade de uma pessoa e download de arquivos ilegais ou pornografia." Podem ser divididos em duas categorias: * Crimes na internet – como ameaças, fraude, difamação, etc. * Crimes da internet – como hacking, implantação de vírus e roubo relacionado à propriedade intelectual.
Ciber-hacktivismo ou Cibervandalismo	Cavelty (2010, p. 1, tradução própria)	"[...] envolve modificação virtual ou destruição de conteúdo, por exemplo, invadir websites ou desativar um servidor por sobrecarga de dados. [...] os efeitos de tais incidentes são limitados no tempo e relativamente inofensivos."
Ciberespionagem / **Espionagem cibernética**	Rid (2013, p. 82, tradução própria)	"[...] refere-se à coleta clandestina de inteligência pela interceptação de comunicações entre computadores, bem como pela invasão das redes de computadores de outras pessoas para exfiltrar dados."
Cibersabotagem / **Sabotagem cibernética**	Rid (2013, p. 57, tradução própria)	"[...] uma tentativa deliberada de enfraquecer ou desabilitar um sistema econômico ou militar. Toda sabotagem é de natureza predominantemente técnica, mas pode, é claro, usar facilitadores sociais. Os meios usados na sabotagem nem sempre levam à destruição física e à violência aberta. [...] Se a violência é usada, os alvos principais são as coisas, não os humanos [...]. A sabotagem tende a ser de natureza tática e raramente terá efeitos operacionais ou mesmo estratégicos.
Ciberterrorismo / **Terrorismo cibernético**	Curran, Concannon e McKeever (2008, p. 1, tradução própria)	"[...] é um ataque premeditado e politicamente motivado contra informações, sistemas de computadores, programas de computador e dados que resultam em violência contra alvos não combatentes por parte de grupos subnacionais ou agentes clandestinos."
Resiliência / **Resiliência Cibernética**	Risk Steering Committee (2010, p. 26, tradução própria)	"Capacidade de sistemas, infraestruturas, governo, negócios, comunidades e indivíduos de resistir, tolerar, absorver, recuperar, preparar ou se adaptar a uma ocorrência adversa que cause dano, destruição ou perda."
	Bryant (2015, p. 89, tradução própria)	"existem três elementos de sucesso contra a tempestade que se aplicam à resiliência no domínio do ciberespaço: flexibilidade, uma superfície de ataque reduzida e a capacidade de responder dinamicamente a ataques."
Ciberdiplomacia / **Diplomacia Cibernética**	Barrinha e Renard (2017, p. 5, tradução própria)	"[...] o uso de recursos diplomáticos e o desempenho de funções diplomáticas para proteger os interesses nacionais no que diz respeito ao ciberespaço", incluindo em sua agenda a segurança cibernética, crimes cibernéticos, construção de confiança e capacidades, liberdade e governança da Internet."
Ciberguerra / **Guerra cibernética**	Libicki (2009, p. 117, tradução própria)	"[...] uma campanha de ataques cibernéticos lançada por uma entidade contra um estado e sua sociedade, principalmente, mas não exclusivamente, com o objetivo de afetar o comportamento do estado-alvo." *[continua]*

	Ayres Pinto e Grassi (2021, p. 124)	"[...] ataques cibernéticos coordenados, efetuados com propósitos políticos e militares, que venham a afetar as infraestruturas críticas ou os organismos de defesa de uma nação, ou que visem ferir a soberania de um Estado. Esses ataques, para serem considerados atos de guerra cibernética, deveriam equivaler a um ato de violência física contra o Estado atacado."
Interferências híbridas	Wigell (2021, p. 51, tradução própria)	"[...] concebida como uma abordagem flexível em que as ferramentas e táticas podem variar, mas serão sempre adaptadas para manipular as clivagens existentes e semear dissensões internas nos países e alianças alvo. [...] com o objetivo de destruir 'a coesão política de um adversário a partir de dentro, empregando um híbrido cuidadosamente elaborado de meios e métodos não militares que amplificam as polarizações políticas, ideológicas, econômicas e outras polarizações sociais dentro da sociedade de um adversário, levando assim ao seu colapso interno.' Enquanto mantêm as relações diplomáticas intactas e, portanto, sem quebrar qualquer limiar oficial de guerra, o agressor mobiliza oposicionistas e radicais dentro do Estado alvo através de uma série de meios que vão desde campanhas de desinformação até à corrupção de atores políticos e ao financiamento de movimentos subversivos, cuidadosamente sincronizados para agravar o efeito."
Infraestruturas Críticas	Fernandes (2012a, p. 58)	"i) comando das redes de distribuição de energia elétrica; ii) comando das redes de distribuição de água potável; iii) comando das redes de gestão dos caminhos de ferro; iv) comando das redes de gestão do tráfego aéreo; v) comando das redes de informação de emergência; vi) comando das redes bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registado em nome dos cidadãos; vii) comando das redes de comunicações em geral e em particular (incluindo as redes de estações de rádio e de televisão); viii) comando dos links com sistemas de satélites artificiais (incluindo fornecedores de sistemas telefônicos, de sinais para tv, de previsões de tempo e de sistemas gps); ix) comando da rede do Ministério da Defesa (incluindo também outros ministérios-chave, como o do Interior e da Justiça, e o próprio Banco Central); x) comando dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral."

Fonte: elaborado pela autora, a partir das fontes referenciadas.