UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS ESTRATÉGICOS INTERNACIONAIS

CÍCERO ARAUJO LISBOA

A SECURITIZAÇÃO DO COMBATE AO CIBERCRIME NO SÉCULO XXI: UM ESTUDO SOBRE A AMÉRICA DO SUL

Porto Alegre
2022

CÍCERO ARAUJO LISBOA

A SECURITIZAÇÃO DO COMBATE AO CIBERCRIME NO SÉCULO XXI: UM ESTUDO SOBRE A AMÉRICA DO SUL

Dissertação submetida ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas do UFRGS, como requisito parcial para obtenção do título de Mestre em Estudos Estratégicos Internacionais.

Orientador: Prof. Dr. Guilherme Ziebell de Oliveira

Porto Alegre

2022

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

CIP - Catalogação na Publicação

Lisboa, Cícero Araujo lisboa
A securitização do combate ao cibercrime no século XXI: um estudo sobre a América do Sul / Cícero Araujo lisboa Lisboa. -- 2022.
149 f.
Orientador: Guilherme Ziebell de Oliveira.

Dissertação (Mestrado) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Porto Alegre, BR-RS, 2022.

1. Securitização. 2. Segurança cibernética. 3. América do Sul. I. Oliveira, Guilherme Ziebell de, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

CÍCERO ARAUJO LISBOA

A SECURITIZAÇÃO DO COMBATE AO CIBERCRIME NO SÉCULO XXI: UM ESTUDO SOBRE A AMÉRICA DO SUL

Dissertação submetida ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais da Faculdade de Ciências Econômicas do UFRGS, como requisito parcial para obtenção do título de Mestre em Estudos Estratégicos Internacionais.

Aprovada em: Porto Alegre, _____de _____de 2021.

BANCA EXAMINADORA:

Prof. Dr. Guilherme Ziebell de Oliveira – Orientador
UFRGS

Prof. Dr. André Luiz Reis da Silva
PPGEEI/UFRGS

Prof. Dr. Eduardo Munhoz Svartman
PPGCP/UFRGS

Prof. Dr. Jéferson Campos Nobre
PPGC/UFRGS

Dr.ª Tamiris Pereira dos Santos
PPGEEI/UFRGS

Dedico esse trabalho a minha mãe, Neiva, que graças a sua insistência, me fez chegar até aqui. Obrigado por tudo que faz por todos nós.

AGRADECIMENTOS

Em primeiro lugar, agradeço à Universidade Federal do Rio Grande do Sul por essa oportunidade de aprendizado e ao Programa de Pós-Graduação em Estudos Estratégicos Internacionais, que me acolheu, mesmo ciente que eu vinha de outra área. Assim, aproveito para agradecer a todos os professores do programa por toda a atenção que recebi nesses dois anos.

Em especial, agradeço ao meu orientador Guilherme Ziebell, que teve muita paciência para me explicar os conceitos das Relações Internacionais, que não eram nada óbvios para um tecnólogo em Segurança da Informação. Aprendi muito em nossos encontros, infelizmente virtuais devido à pandemia, com alguns poucos chopes nessa trajetória – tem a didática de um verdadeiro professor, se um dia seguir por esse caminho, terei essa fonte de inspiração para trabalhar em sala de aula. Conseguimos, com amizade e muito esforço, publicar artigos em eventos e, até mesmo, em uma revista.

Agradeço em especial a minha Flávia Lenzi, parceira de todos os momentos, que além de me emprestar aquele "supercomputador" na reta final deste trabalho, teve a paciência necessária para entender que eu precisava escrever. Não dá para falar em carinho, sem esquecer de todos os lanchinhos, cafés e águas que recebi para que não precisasse parar de trabalhar. Também não posso esquecer do apoio da Mariana e da Giulia.

Gostaria de agradecer também à minha família, em especial aos meus pais, Neiva Edites Araujo Lisboa e Benedito Veiga Lisboa, e à minha irmã Caroline, por compreenderem meus momentos de ausência, necessários para a conclusão deste mestrado. Sabemos como precisamos do tempo de cada um.

Aos colegas de curso que, devido à pandemia, tivemos apenas o contato virtual, mas que tiveram a paciência com quem precisava conhecer a área.

Muito obrigado.

A verdadeira generosidade para com o futuro consiste em dar tudo ao presente.

Albert Camus

RESUMO

Este trabalho busca analisar as ações securitizadas de combate ao crime cibernético implementadas pelos países da América do Sul no século XXI, com o objetivo de verificar se os meios empregados para tanto estão dentro do espectro da securitização. O crime cibernético, que anteriormente tinha como alvo golpes contra indivíduos, têm passado nas últimas duas décadas por uma transformação, em que os ativos críticos dos Estados têm sido alvo de ataques. Dessa forma, os países têm desenvolvido estratégias cibernéticas nacionais, com o objetivo de planejar ações para sua proteção no domínio cibernético, sendo que algumas delas acabam por extrapolar a perspectiva política. Neste cenário, a pesquisa busca, através da análise das estratégias ou políticas nacionais de segurança cibernética dos países da América do Sul, encontrar se existe na região um movimento em direção da securitização cibernética. Além disso, através do viés da segurança cibernética nacional, procura por indícios de aplicabilidade da Teoria dos Complexos Regionais (CRS) à região. Para isso, também analisa *frameworks* criados por organizações internacionais para orientar as nações a criarem suas próprias estratégias cibernéticas. Para responder essas questões, além da introdução e da conclusão, esse trabalho se divide em três capítulos. A pesquisa percebe que, apesar da proximidade, história e características semelhantes, esses países possuem algumas diferenças no trato do cibercrime, além de conduzirem suas ações dentro do espectro político. Assim sendo, não foi possível verificar um padrão uniforme de securitização, indicando que a teoria dos CRS não explica a dinâmica dessa temática na região.

Palavras-chave: Securitização. Segurança cibernética. América do Sul.

ABSTRACT

This work seeks to analyze the securitized actions to combat cyber crime implemented by South America countries in the 21st century, with the objective of verifying if the means used for this are within the spectrum of securitization. Cybercrime, which previously targeted scams against individuals, has undergone a transformation over the past two decades, where critical state assets have been targeted by cyberattacks. Therefore, countries have developed national cyber strategies, with the objective of planning actions for their protection in the cyber domain, some of which end up extrapolating the political perspective. In this scenario, the research seeks, through the analysis of national cybersecurity strategies or policies of South American countries, to find out if there is a movement towards cyber securitization in the region. In addition, through the national cybersecurity bias, it looks for evidence if the Theory of Regional Complexes (TRC) applies in the region. For this, it also analyzes frameworks, which are documents created by international organizations to guide nations to create their own cybernetic strategies. To answer these questions, in addition to the introduction and conclusion, this work is divided into four chapters. The research realizes that, despite their proximity, history and similar characteristics, these countries have some a few differences in dealing with cybercrime, in addition to as well as conducting their actions within the political spectrum. It is not possible to verify a uniform pattern of securitization, indicating that the TRC theory does not explain the dynamics of this theme in the region.

Keywords: Securitization. Cyber security. South America.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Esse trabalho tem como tema as estratégias para o combate aos crimes digitais nos países da América do Sul. As atividades maliciosas na *Internet* aumentam em frequência e gravidade, e à medida que os países se estruturam para defender suas redes e infraestruturas, essa capacidade de combater crimes no ciberespaço ganha cada vez mais relevância internacional (MCKENZIE, 2017). Para se ter uma noção desse crescimento, em 15 anos, o site *Safer Net Brasil* recebeu e processou mais de 4 milhões de denúncias de cibercrimes, envolvendo algo em torno de 800 mil sites hospedados em diferentes países (SAFER NET BRASIL, 2022). Dentre os elementos que servem de motivação para que os países busquem incrementar sua proteção, pode ser destacado o grande volume de recursos financeiros movimentados em tais crimes. Nos Estados Unidos, por exemplo, cerca de US$ 1 trilhão foram perdidos, em 2008, por meio de ataques cibernéticos, valor superior ao produto interno bruto (PIB) de muitos países (VAMOSI, 2012; CENTRAL INTELLIGENCE AGENCY, 2019).

Na obra "1984", criada por George Orwell, a teletela tinha a capacidade de espionar a vida das pessoas e de transmitir essas informações o tempo todo (ORWELL, 2008). Atualmente, podemos nos questionar se não vivemos uma realidade semelhante, principalmente quanto às ameaças a nossa privacidade. No livro *Cypherpunks*, os autores descrevem assim as possibilidades da rede mundial de computadores, a *Internet*:

> [a] rede mundial de computadores apresenta, como muitas tecnologias, uma variedade de usos possíveis. É como a energia elétrica, a semente de uma gama infinita de possibilidades, e semente poderosa: seu potencial ainda está sendo descoberto ao mesmo tempo que seu rumo vai sendo definido pelo caminhar tecnológico e pelo caminhar político (ASSANGE *et al*., 2013, p.9).

A rede mundial de computadores, que inicialmente foi criada para ser uma forma descentralizada de comunicação e, posteriormente, para interligar universidades, transformou-se, com o apoio da tecnologia da informação, no chamado ciberespaço. Através dele, hoje é possível, além de oferecer entretenimento (como filmes, músicas, redes sociais, etc.), controlar infraestruturas críticas, gerir o sistema financeiro, armazenar a propriedade intelectual, prover serviços de governo eletrônico, entre outros. Todas essas possibilidades de uso transformaram o ciberespaço em um ambiente estratégico para os governos, os negócios e a sociedade (TEN; MANIMARAN; LIU, 2010). A despeito de sua relevância, os recursos que mantém o

ciberespaço, os quais são de natureza híbrida - formada por *hardware*[1] e *software*[2] -, apresentam vulnerabilidades que possibilitam que crimes sejam cometidos.

O delito cometido no ciberespaço é conhecido como cibercrime, que é definido como o uso de ferramentas digitais por criminosos para cometer atividades ilegais (SINGER; FRIEDMAN, 2014). O Tratado do Conselho Europeu sobre Crimes Cibernéticos, de 2001, definiu que os delitos do cibercrime compõem um amplo espectro, que vai de atividades criminosas contra dados até infrações contra os direitos autorais (CONSEIL DE L'EUROPE, 2001). Em uma definição mais ampla, a Organização das Nações Unidas (ONU) inclui como atividades de cibercrime o roubo, a fraude, os *malwares*[3] (*worms*,[4] *vírus,*[5] *trojans*,[6] *backdoors*[7]), o acesso não autorizado a sistemas, a pornografia infantil, o *hacking*,[8] o assédio, a exploração sexual e os delitos que envolvem os direitos autorais e de propriedade intelectual (UNITED NATIONS, 2015).

Os efeitos do cibercrime podem ser os mais diversos. Eles podem ser simples, como o acesso a um sistema para observar seu funcionamento ou a desfiguração de sites. Entretanto, eles podem também ser muito graves, principalmente se forem atingidas infraestruturas críticas para o funcionamento dos países (JENSEN, 2012). As infraestruturas críticas são estruturas físicas complexas, muitas vezes baseadas em sistemas cibernéticos, que formam a linha de vida de uma sociedade moderna, e sua operação, segura e confiável, é de suma importância para a segurança nacional e a vida econômica (TEN; MANIMARAN; LIU, 2010). Os países, conforme suas necessidades e visão estratégica, é que determinam quais são as suas infraestruturas críticas. Normalmente elas englobam as redes de energia elétrica, as telecomunicações, os sistemas de transporte público, as estruturas de produção e transporte de gás natural e o petróleo, os sistemas de abastecimento de água, os sistemas financeiros, os bancos e toda e qualquer estrutura, indústria e serviço que são vitais para o bem-estar da

---

[1] É a parte física de um computador, formada por componentes eletrônicos necessários para fazer com que o computador funcione.

[2] Programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador.

[3] Vírus. É um tipo de programa de computador desenvolvido para infectar o computador, podendo prejudicar usuários e sistemas de diversas formas.

[4] É um programa semelhante a um vírus de computador, com a diferença de ser auto-replicante, ou seja, ele se replica e infecta outros computadores.

[5] É um programa de computador projetado para danificar um computador através da corrupção de arquivos dos sistemas, destruição de dados, utilização de recursos e outros modos de interrupção.

[6] Também conhecido como Cavalo de Troia, é um programa malicioso que é instalado em um computador como um programa legítimo. Serve para abrir portas para invasores atacarem o computador.

[7] Pode assumir a forma de uma parte oculta de uma aplicação, ou ser um programa separado, como autenticação, por exemplo, mas que pode ser usado para obtenção de senhas, exfiltrar dados e etc.

[8] São atividades que procuram comprometer, de forma criminosa, dispositivos digitais, como computadores, *smartphones*, *tablets* e redes de dados.

sociedade, da economia e da segurança nacional (LI *et al*., 2005).

O mais famoso ataque cibernético a uma infraestrutura crítica foi o do *Worm Stuxnet*, que ocorreu em 2010 e destruiu grande parte da planta de enriquecimento de urânio do Irã (ZETTER, 2017). Este ataque foi resultado de um conjunto de ferramentas projetado especificamente para atingir os Sistemas de Controle Supervisório (SCADA)[9] do país e para adquirir dados que alimentam a infraestrutura crítica iraniana (SINGER; FRIEDMAN, 2014). Outro caso importante, que ocorreu em 2014, foi o ataque virtual à *Sony Pictures*, no qual o grupo autointitulado "Guardiões da Paz" compartilhou publicamente conteúdos privados - como e-mails trocados entre executivos, endereços e telefones de artistas, pedidos do diretor Steven Spielberg por doações para partidos políticos e filmes que ainda não haviam sido lançados. O *Federal Bureau of Investigation* (FBI) afirma que o grupo, que seria norte-coreano, teria realizado o ataque em resposta à exibição do filme *The Interview* (FEDERAL BUREAU OF INVESTIGATION, 2014), uma comédia em que, por ordem da Agência de Inteligência dos EUA (CIA), dois estadunidenses tentam assassinar o líder da Coreia do Norte, Kim Jong-Un (GONZÁLEZ, 2014).

Diante de tal contexto, muitos países têm demonstrado, ao longo dos últimos anos, sensibilidade sobre o cibercrime. Em 2001, o Conselho da Europa aprovou a Convenção de Budapeste sobre o Cibercrime, assinada pelos países da União Europeia, Estados Unidos, Japão, Canadá, Chile, Argentina, Austrália, Paraguai e República Dominicana, e que tem como objetivo oferecer acesso mais rápido a provas eletrônicas que estejam no exterior do que mediante cooperação jurídica internacional (RICHTER, 2019). Mais recentemente, em 2018, Estados Unidos e Reino Unido também contribuíram para colocar a questão cibernética em destaque, ao emitir uma declaração conjunta, sem precedentes, na qual atribuíam à Rússia a responsabilidade por ataques cibernéticos a empresas e a consumidores de todo o mundo (NATIONAL CYBER SECURITY CENTRE, 2018).

Segundo relatório elaborado pelo Centro de Estudos Estratégicos e Internacionais (CSIS) em parceria com a empresa de *softwares* de cibersegurança *McAfee*, em 2017, o crime cibernético custou quase US$ 600 bilhões ao mundo, cerca de 0,8% do PIB global, colocando-o em terceiro lugar entre os crimes com maior impacto global, atrás apenas da corrupção governamental e do tráfico de drogas (LEWIS, 2018). Além disso, estimativas calculam que, só nos Estados Unidos, passa dos US$ 6 milhões por dia o custo que a inatividade das

[9] Software de supervisão que permite monitorar e operar partes ou todo um processo. Esse processo pode ser industrial como de manufatura, processo contínuo, batelada, elétrico, automação residencial/predial (domótica), entre outros; ou até mesmo sistemas de serviço público como de tratamento de água, esgoto, transporte, etc.

infraestruturas críticas pode gerar em casos de ataque (BAKER; WATERMAN; IVANOV, 2010).

Diante de tal realidade, a preocupação com tais infraestruturas, que são a espinha dorsal dos sistemas de transporte e econômico dos EUA, fez com que, em 2009 o então presidente estadunidense, Barack Obama, definisse a defesa das infraestruturas digitais como uma prioridade para a segurança nacional dos EUA. Em pronunciamento sobre o relatório de revisão das ações federais para a cibersegurança, elaborado pelo *National Security Council* e pelo *Homeland Security*, Obama declara que a prosperidade econômica dos Estados Unidos no século XXI dependeria da segurança cibernética, pois neste meio são controladas as infraestruturas críticas e armazenada a propriedade intelectual estadunidense. Em suas palavras,

> [a] partir de agora, a nossa infraestrutura digital - as redes e computadores de que dependemos todos os dias - será tratada como deve ser: como um ativo nacional estratégico. Proteger essa infraestrutura será uma prioridade de segurança nacional. Garantiremos que essas redes sejam seguras, confiáveis e resilientes. Nós deteremos, preveniremos, detectaremos e nos defenderemos contra ataques e nos recuperaremos rapidamente de quaisquer interrupções ou danos (THE WHITE HOUSE, 2009**,** p.4, tradução nossa).[10]

Nos últimos anos, vários ataques cibernéticos assumiram proporções globais. Em maio de 2017, um ataque *ransomware*[11] paralisou dezesseis hospitais no Reino Unido (AGÊNCIAS, 2017). Esse ataque foi oriundo de uma investida desencadeada pelo vírus intitulado *WannaCry*, responsável por ciberataques em cerca de 74 países. O grupo *hacker Shadow Brokers* revelou que a base desse vírus foi desenvolvida pela Agência de Segurança Nacional dos EUA (NSA) e que ele explorava uma vulnerabilidade do sistema operacional Windows - ou seja, a agência, que já conhecia a vulnerabilidade, poderia ter informado a falha à *Microsoft*, desenvolvedora do *software*, evitando os incidentes (O GLOBO, 2017).

Em 2019, as Forças Armadas israelenses bombardearam um prédio que supostamente serviria de base para um grupo de *hackers* do Hamas. Segundo a imprensa, este foi o primeiro caso de ataque físico realizado como resposta a um possível ataque cibernético (ÉPOCA, 2019). Apesar de a iniciativa ser retratada como novidade, desde 2011, a Estratégia Nacional de Segurança Cibernética dos Estados Unidos considera a possibilidade de uma resposta cinética

[10] Em inglês: From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

[11] *Software* malicioso que infecta o computador, bloqueando seu funcionamento, e exibindo mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar.

contra ataques realizados através do ciberespaço, ou seja, afirma que ataques cibernéticos podem ser retaliados com força militar (THE WHITE HOUSE, 2011). De acordo com o documento,

> Reservamo-nos o direito de usar todos os meios necessários – diplomáticos, informativos, militares e econômicos – conforme apropriado e consistente com a lei internacional aplicável, a fim de defender nossa Nação, nossos aliados, nossos parceiros e nossos interesses. (THE WHITE HOUSE, 2011, p. 14, tradução nossa).[12]

Incidentes cibernéticos não são, todavia, exclusividade dos países mais desenvolvidos tecnologicamente. Os países de menor desenvolvimento tecnológico relativo, como os da América do Sul, também sofrem com o crime cibernético. Em 2018, o Brasil foi o terceiro país mais atingido por ataques cibernéticos no mundo, ficando atrás apenas de China e de Estados Unidos (SYMANTEC, 2019). Além disso, foi o segundo país que mais perdeu financeiramente com ataques cibernéticos no ano de 2017, atrás apenas da China, com cerca de 62 milhões de brasileiros tendo sido vítimas de cibercrime, com perdas que, estima-se, totalizaram US$ 22 bilhões (NORTON, 2018).

Ainda, alguns casos de ataques cibernéticos contra governos e empresas deste continente exemplificam essa problemática. O Brasil foi alvo de um programa de vigilância mantido pelo governo dos EUA, que monitorava e-mails e ligações telefônicas do governo federal. Este fato foi revelado por Edward Snowden, em 2013, e provocou mal-estar diplomático entre os dois países (FERRAÇO, 2014). Essa vigilância americana também provocou a desaprovação de outros países da América do Sul, os quais, em 2013, fizeram uma reunião de emergência, contando com a participação dos presidentes de Uruguai, Paraguai, Argentina, Venezuela, Suriname e Equador, além de um representante do Brasil, depois da qual divulgaram uma nota de repúdio em resposta às ações dos Estados Unidos (RODRIGUES; MÈRCHER, 2017). Nesse mesmo contexto, a Venezuela realizou, no mesmo ano, uma oferta de asilo para Snowden, que, considerado um foragido pelo governo dos Estados Unidos, solicitou asilo a vários países (AGÊNCIA BRASIL, 2013).

Manifestações políticas também podem servir de motivação para a realização de crimes cibernéticos. Na Colômbia, por exemplo, um grupo atacou, em 2001, os *sites* da Presidência da República, do Senado e de outros órgãos do governo, paralisando serviços digitais por várias horas, como uma forma de pressionar as autoridades contra um projeto de lei sobre a

[12] Em inglês: We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.

responsabilização de crimes na *Internet* (OLIVEIRA et al., 2017). Já no Peru, em 2014, o grupo *hacker Sombrero Negro* roubou dados sensíveis das redes das forças armadas, polícia e de outros órgãos do governo. Neste mesmo ano, o grupo *LulzSec*[13] *Peru* roubou e divulgou na *Internet* uma série de mensagens de *e-mails* trocados pelo Conselho de Ministros do Peru, que demonstravam a atuação destes funcionários como lobistas para a indústria, provocando uma crise de confiança na sociedade (RADIO TELEVISION MARTI, 2014).

A América do Sul apresenta também recorrentes casos de vazamento de dados de cidadãos. Em maio de 2008, *hackers* invadiram os sistemas de diversos órgãos da administração pública do Chile e divulgaram, na *Internet*, dados confidenciais de mais de 6 milhões de pessoas (BBC MUNDO, 2008). Em 2010, os dados de todos os contribuintes argentinos ficaram expostos no site da Administração Federal da Receita Pública (AFIP). Esse incidente aconteceu devido a uma falha na validação de dados, que fez com que os cibercriminosos pudessem acessar o documento de identidade nacional (DNI) digitalizado, impressões digitais, fotografia e assinatura holográfica de qualquer contribuinte da República Argentina (BORGHELLO; TEMPERINI, 2013). Da mesma forma, em 2019, dados particulares de cerca de 20 milhões de equatorianos foram vazados na *Internet*, expondo informações como nome, data de casamento, *e-mail*, local de nascimento, telefone celular, entre outros. O incidente desencadeou um debate sobre uma nova lei de privacidade na *Internet* no Equador (CUNHA, 2019). Além disso, os estudos e estatísticas geralmente retratam anualmente o aumento do cibercrime na América Latina como um todo, como é o caso do relatório da agência *TheatMetrix*, que estima, em 2019, um aumento de 20%, em relação ao ano anterior, na fraude de criação de contas (BANCO INTERAMERICANO DE DESARROLLO, 2020).

Estes são apenas alguns casos que colocam em risco a soberania nacional e explicam por que as nações têm desenvolvido estratégias nacionais de segurança cibernética, alinhadas com sua estratégia de defesa nacional, para promover a proteção do ciberespaço. Essas estratégias cibernéticas podem ser elaboradas pelos países através de seus próprios esforços ou seguindo os princípios e boas práticas de *frameworks* de modelos internacionais de segurança cibernética. Esses *frameworks* orientam como os países podem estruturar sua proteção no ciberespaço, podendo divergir tanto em relação à forma, quanto no que diz respeito ao

[13] O grupo possui ramificações em vários países e atraiu as manchetes pelos seus ataques a organizações importantes como o senado norte-americano, a CIA (que teve apenas seu site derrubado) e a InfraGard, ligada ao FBI. Mas não para por aí. O grupo distribuiu na internet 62 mil senhas de procedência desconhecida, invadiu redes produtoras de games Bethesda e Nintendo, atacou também a Sony e até empresas de mídia como a Fox e a PBS.

direcionamento, com alguns sendo voltados para ações de governança[14]e outros mais focados em ações de segurança.[15]

Os países mais desenvolvidos tecnologicamente adotam, em linhas gerais, estratégias de segurança cibernética bem definidas para combater o cibercrime, que incluem medidas como ações legislativas e de governo e o trabalho integrado de forças de segurança (polícias, Forças Armadas e órgãos de inteligência). Desde 2005, por exemplo, os Estados Unidos possuem uma estratégia nacional para proteção no ciberespaço. Na América do Sul, a Colômbia, em 2011, foi o primeiro país a adotar uma estratégia desse tipo. Embora cada vez mais países estejam elaborando suas estratégias cibernéticas, não existe uma maneira uniforme de fazê-lo; cada nação, conforme seus recursos e entendimento, compõem suas próprias ações de proteção. Diligentes com relação ao tema, Organizações Internacionais elaboraram manuais com instruções para que os países desenvolvessem suas próprias estratégias e capacidades de segurança e defesa no ciberespaço, fazendo isso através da publicação de *frameworks,* que têm como objetivo apresentar as chamadas boas práticas[16] em áreas como segurança da informação, gestão de risco, resposta a incidentes de segurança, continuidade de negócios, entre outras, para que as nações possam, dentro de suas capacidades, estabelecer suas próprias estratégias de proteção.

Da mesma forma que as estratégias nacionais apresentam diferenças de implementação em cada nação, os *frameworks* também se diferenciam em sua forma. Alguns sugerem soluções centradas em ações de segurança - como realizar a resposta de incidentes cibernéticos por meio das Forças Armadas -, enquanto outros sugerem que os países busquem se tornar mais robustos através de soluções voltadas para a gestão de risco, *compliance*[17] e educação da população. A despeito de possibilidades, existem ações de caráter criminoso no ciberespaço, tais como realizar campanhas militares e promover a desinformação em eleições -, as quais podem ser tratadas como justificativas para a necessidade de tratar a questão como um tema de segurança. Entre ações mais pontuais adotadas a partir dessa perspectiva, podemos citar (i) operar a defesa

[14] Ações focadas na gestão de riscos e de vulnerabilidades, bem como na conformidade com leis e normas de segurança da informação.

[15] O foco das ações é a resposta judicial e tecnológica aos incidentes cibernéticos, através de organismos de Estado, tais como polícias, forças armadas (pautados pela atividade de inteligência) e leis específicas para o ciberespaço.

[16] A denominação de Boas Práticas consiste em uma série de técnicas identificadas e experimentadas como eficientes e eficazes para a realização de determinada tarefa, atividade ou procedimento. Neste sentido, na área da Segurança da Informação existem uma série normativas que definem as melhores práticas para proteção de dados como: uso de criptografia, armazenamento seguro, entre outros, que podem ser encontrados na série ISO 27000, COBIT, NIST e etc.

[17] Conjunto de disciplinas a fim de cumprir e se fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como evitar, detectar e tratar quaisquer desvios ou inconformidades que possam ocorrer.

de infraestruturas por críticas militares; (ii) realizar uma resposta ofensiva a ciberataques por unidades das Forças Armadas; (iii) o emprego de uma resposta cinética contra ciberataques; (iv) o estabelecimento de unidades de inteligência para lidar com ciberameaças, entre outras (KLIMBURG, 2012).

O contexto da proteção das infraestruturas críticas nos traz alguns exemplos disso. Enquanto os Estados Unidos fazem uso de militares para essa proteção, nos casos do Reino Unido e da Alemanha a participação dos militares é quase nula (KLIMBURG, 2012). Embora existam iniciativas para promover ações de proteção cibernética na América do Sul, como no caso do comprometimento dos países do Mercosul em adotar normas para preservar a soberania desses Estados no ciberespaço, os países da região estão em momentos diferentes da implementação de suas estratégias e adotam abordagens variadas, umas mais e outras menos securitizadas (MERCOSUR, 2014). A Colômbia, por exemplo, faz uso de militares para sua segurança e defesa cibernéticas, enquanto o Brasil divide essas tarefas entre as Forças Armadas e setores civis. Ao contrário destes países, Uruguai e Paraguai, por sua vez, fazem uso de ações de governança para promover sua proteção do ciberespaço (OLIVEIRA *et al.*, 2017).

Diante de tal contexto, se faz necessário um estudo mais focado nos países da América do Sul, que por estarem mais próximos do Brasil são importantes parceiros comerciais e estratégicos, buscando entender como esse grupo de nações pode trabalhar em parceria para promover a proteção cibernética do continente. De forma a compreender a realidade de tais interações na América do Sul, essa dissertação se insere na linha de pesquisa da segurança internacional, e desenvolve uma análise comparativa das ações implementadas pelos países da região, no século XXI, para combater o cibercrime. Essa pesquisa é conduzida a partir da perspectiva da Escola de Copenhague, que entende que a temática da segurança cibernética é passível de ser securitizada pelos Estados.

Após a Guerra Fria, a Escola de Copenhague buscou, em um contexto de reorganização do sistema internacional, ampliar e redefinir as questões abordadas no âmbito dos estudos de segurança internacional, afirmando que uma questão de segurança pode ser considerada como uma ameaça existencial, requisitando medidas urgentes que justificariam ações fora do processo político habitual (KREMER; MÜLLER, 2014). Autores como Nissenbaum (2005) e Hart (2011) aplicam a teoria da securitização desenvolvida pela Escola de Copenhague à cibersegurança, e consideram que o tema deve ser tratado de maneira independente, dada a importância que a questão vem adquirindo no cenário contemporâneo da segurança internacional.

O desenvolvimento dessa pesquisa se mostra relevante sobretudo devido à atualidade

do tema e sua importância frente às novas ameaças cibernéticas vigentes. Ainda, a literatura que busca entender a adversidade imposta pelo cibercrime nos países em desenvolvimento, geralmente não envolvidos no advento das novas tecnologias, se mostra, em grande medida, escassa. Desta forma, a pesquisa busca servir de apoio para os tomadores de decisão, não apenas do Estado brasileiro, mas também de outros países, especialmente aqueles com realidades análogas às dos países do Sul Global e daqueles em desenvolvimento, para que tomem consciência sobre o tema e, assim, possam entender seus desafios e suas possibilidades.

Essa dissertação tem como propósito contribuir para incitar o desenvolvimento de outros estudos sobre segurança cibernética. Para isso, faz a interlocução com outros trabalhos acadêmicos publicados e que são relacionados com a temática, com metodologias criadas em países mais desenvolvidos tecnologicamente e com o material (leis, órgãos, informações e etc.) que compõem as estratégias dos países estudados.

Diante disso e considerando as ações desenvolvidas pelos países da América do Sul para o combate ao cibercrime, este trabalho propõe a seguinte questão de pesquisa: há uma securitização do cibercrime pelos Estados da América do Sul no século XXI? A hipótese de trabalho que sustenta essa pesquisa é a de que, apesar de compartilharem diversas características semelhantes (como aspectos sociais, históricos, políticos e econômicos) e de sua proximidade geográfica, nem todos os países da América do Sul implementam ações securitizadas para promover sua defesa contra o cibercrime, sendo possível verificar níveis diferentes de securitização nos casos em que ela ocorre.

Assim, impulsionada pela pergunta de pesquisa apresentada e pela hipótese de trabalho proposta, esta dissertação tem como objetivo principal compreender as diferenças existentes entre as ações de segurança cibernética desenvolvidas pelos países da América do Sul para combater o cibercrime, bem como sua adequação aos princípios e boas práticas estabelecidos nos *frameworks* de modelos nacionais de segurança cibernética. De forma a atingir tais objetivos, o trabalho apresenta quatro objetivos específicos.

Em primeiro lugar, procura-se, a partir da sistematização das características dos diferentes *frameworks*, categorizá-los com relação ao tratamento por eles dispensados às questões de cibersegurança, posicionando-os, assim, em um "espectro de securitização" (variando daqueles que consideram tais questões como pertencentes à esfera política até aqueles que as consideram como localizadas no âmbito securitário). Com isso pretende-se conhecer as ações securitizadas para combate ao cibercrime para, posteriormente, compará-las com as ações dos países da América do Sul. Em segundo lugar, identificar as ações dos países da América do Sul para combate ao cibercrime e verificar como elas se posicionam no espectro de

securitização dos *frameworks* estudados. Após conhecer as ações securitizadas definidas pelos *frameworks*, pretende-se aqui avaliar se as estratégias de proteção desses países são securitizadas ou não. Por fim, compreender as causas que fazem os países adotarem ações não securitizadas para combate ao cibercrime. Depois de analisados os *frameworks* e as estratégias/ações dos países da América do Sul, pretende-se, a partir da consecução desse objetivo, entender as causas da securitização da proteção cibernética na região.

No que concerne aos aspectos metodológicos, esta pesquisa é de natureza aplicada e de caráter exploratório e adota uma abordagem qualitativa. Para compreender as similaridades dos *frameworks*, é utilizada a Teoria Fundamentada como método de pesquisa. Nesse método o pesquisador, mediante procedimentos diversos, reúne um volume de dados referentes a determinado fenômeno e, após compará-los e codificá-los, identifica as similaridades que emergiram desse processo de análise. A coleta de dados foi realizada através da revisão bibliográfica de artigos científicos, livros, anais de congressos, entre outros. Da mesma forma, foi realizada uma revisão documental, na qual foram analisadas as políticas e estratégias nacionais de segurança cibernética de cada país estudado, bem como sua legislação para o cibercrime e os respectivos órgãos que atuam para manter essa estrutura.

Como esse tema estabelece uma associação de interesses entre as áreas de Relações Internacionais e de Tecnologia da Informação, os artigos para a revisão bibliográfica foram selecionados através de bases como *REDALYC*, *LARefêrencia*, *IEEE*, *Scopus, Scielo, Web of Science*, além do Portal de Periódicos CAPES. A etapa de seleção consistiu no levantamento de artigos a partir de palavras-chave, como *Cibercrime*, *Cibercrimen, Cybercrime, Cibersegurança, Cibersecuridad, Cybersecurity, Estratégia de Segurança Cibernética, Cybersecurity Strategies,* etc*,* encontradas em títulos, resumos e palavras-chave das publicações. Cada artigo encontrado foi selecionado com base na leitura dos *abstracts*, que foram avaliados com foco nas questões de pesquisa deste projeto. Os documentos coletados para a revisão documental foram selecionados em sites oficiais dos governos estudados. Foram pesquisadas suas políticas e estratégias para o combate ao cibercrime, suas legislações, bem como os órgãos que sustentam as ações dessas estratégias. Apesar da existência de trabalhos acadêmicos sobre a construção de modelos nacionais de segurança cibernética, essa pesquisa optou pela utilização de *frameworks* criados por Organizações Internacionais, pois essas possuem trabalhos criados por especialistas em cibersegurança de diferentes nações, com o intuito de promover boas práticas de segurança cibernética entre países. Com esse critério, o Quadro 1 apresenta os *frameworks* analisados nesta pesquisa.

Quadro 1- Frameworks selecionados

TÍTULO DO *FRAMEWORK*	ORGANIZAÇÃO
Guide to developing a national cybersecurity Strategy: Strategic engagement in cybersecurity	International Telecommunication Union (ITU)[18]
National Cyber Security Framework Manual	*Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)*[19]
National Cyber Security Strategies: An Implementation Guide	*European Union Agency for Cybersecurity (ENISA)*[20]
NIST Cybersecurity Framework	*National Institute of Standards and Technology (NIST)*[21]
Cybersecurity Risks, progress, and the way forward in Latin America and the Caribbean	*Organization of American States (OAS)*[22]

Fonte: Elaborado pelo autor

Esses *frameworks* foram analisados segundo as técnicas da Teoria Fundamentada. Seus métodos se baseiam em diretrizes sistemáticas, ainda que flexíveis, para coletar e analisar os dados visando à construção de teorias "fundamentadas" nos próprios dados (CHARMAZ, 2011). Para que essa codificação forneça os dados para essa pesquisa, ela ocorre em três fases progressivas, que conceitualmente vão se aperfeiçoando. São elas a Codificação Aberta, na qual se identificam as ideias principais em segmentos de texto; a Codificação Axial, em que se relacionam os códigos gerados na codificação aberta em categorias e subcategorias; e, a Codificação Seletiva, na qual se conceitua as categorias principais de forma hierárquica, com o objetivo de criar um conceito chave - chamado de *core category*. Tal codificação é realizada

[18] I*nternational Telecommunication Union* (ITU), é a agência especializada das Nações Unidas (ONU) em tecnologias de informação e de comunicação, com a cooperação do NATO CCD COE, do Banco Mundial, da Universidade de Oxford e do setor privado.

[19] NATO CCD COE, é um centro de defesa cibernética credenciado pela OTAN, que reúne um grupo de pesquisadores, analistas e educadores do exército, governo, academia e indústria.

[20] A ENISA tem como missão contribuir para a política cibernética da UE, aumentar a confiabilidade dos produtos, serviços e processos de TIC com esquemas de certificação de segurança cibernética, promover a cooperação entre os Estados-Membros e os organismos da UE, além de ajudar o continente a se preparar para os desafios cibernéticos de amanhã.

[21] NIST, órgão do governo dos EUA dedicado a promover a competitividade industrial dos Estados Unidos por meio do avanço da ciência, padrões e tecnologias de medição de forma aumentar a segurança econômica e a qualidade de vida.

[22] Trabalho desenvolvido pela Organização dos Estados Americanos (OEA) e pelo Banco Interamericano de Desenvolvimento (BID), baseado no framework do NIST, apresenta cinco dimensões com diferentes ações para medir as estratégias nacionais de segurança cibernética nas Américas.

com o uso do software NVivo, utilizado para realizar a análise de dados por meio da Teoria Fundamentada.

Os *frameworks* foram conduzidos à Teoria Fundamentada para que fossem desenvolvidas as propriedades das categorias até que não surgissem mais propriedades novas. Desta forma, as categorias ficaram saturadas com dados e, assim, tornou-se possível classificá-las graficamente. A análise das informações dos *frameworks*, resultando da aplicação das técnicas de codificação da Teoria Fundamentada, possibilitou encontrar as possíveis similaridades entre esses *frameworks*.

Sendo assim, de forma a atingir os objetivos propostos, este trabalho está estruturado em três capítulos, além desta introdução e da seção de conclusão. O primeiro capítulo trata de contextualizar os diversos elementos que compõem esta dissertação: o ciberespaço, seu histórico, sua definição e seus elementos; as infraestruturas críticas, definições e exemplos; a discussão sobre a Teoria da Securitização da Escola de Copenhague e os Complexos Regionais de Segurança; a segurança e a defesa cibernéticas, suas definições, suas diferenças, o contexto de suas aplicações com a Escola de Copenhague; e os aspectos que definem o cibercrime, aprofundando sua definição teórica e os tipos de crimes virtuais.

O segundo capítulo apresenta uma análise dos *frameworks* estudados neste trabalho, fazendo uma classificação destes em relação à securitização, com o objetivo de encontrar neles as soluções securitizadas para combate ao cibercrime e compará-los em relação às estratégias dos países da América do Sul. Por fim, no terceiro capítulo, são analisadas as diversas estratégias cibernéticas dos países da América do Sul, elencando suas ações, similaridades e analisando-as em relação à securitização, buscando também compreender as causas que fazem os países adotarem ações não securitizadas para combate ao cibercrime. Ao final é apresentada uma conclusão do trabalho, trazendo novamente a questão de pesquisa, retomando os temas estudados e apresentando as conclusões do trabalho realizado. Por fim, são apresentados os elementos de causaram alguma dificuldade para a realização desta dissertação e suas considerações finais.

2 FUNDAMENTOS TEÓRICOS

Este capítulo tem como objetivo apresentar os elementos teóricos que embasam essa pesquisa. Sendo assim, são apresentados o ciberespaço e seus elementos, histórico e como alguns países o definem. Em seguida, o conceito de infraestruturas críticas, destacando sua importância para a segurança dos Estados, bem como exemplos de legislações que tratam da sua proteção com foco no espaço cibernético. O terceiro elemento apresentado trata de explicar os conceitos da segurança e defesa cibernéticas e suas implicações nas estratégias nacionais de segurança, além de discorrer sobre as ameaças que podem ser exploradas por vulnerabilidades. Para que sejam apresentados e aprofundados os elementos da securitização, na sequência é apresentada a Escola de Copenhague, seu histórico e conceitos. O quinto elemento trata da Teoria da Securitização, necessária para explicar como a Escola de Copenhague pensa a segurança internacional. Em seguida, apresenta-se o elemento da securitização cibernética, discutindo-se, a partir de uma perspectiva histórica, os primeiros passos da segurança cibernética, além da visão acadêmica e estratégica de Estados sobre a securitização do ciberespaço. O sexto elemento versa sobre a teoria dos Complexos regionais de segurança. Por fim, é discutido como essa teoria é definida no âmbito da América do Sul.

2.1 O CIBERESPAÇO

A palavra ciberespaço apareceu pela primeira vez em um conto chamado "*Burning Chrome*", publicado em 1982 pelo escritor estadunidense William Gibson e, mais tarde, novamente, em seu romance "*Neuromancer*", de 1984 (GIBSON, 1982; 1984). Nos anos seguintes, o termo acabou relacionado com computadores ligados *online*. Fora da literatura, o mundo virtual começou a ser desenvolvido nos anos finais da década de 1960, no âmbito militar, em um projeto conhecido como ARPANET, que tinha como objetivo conectar computadores através de uma rede de computadores descentralizada (LUKASIK, 2011). Segundo Dodge e Kitchin (2003), o termo ciberespaço significa literalmente "espaço navegável" e é derivado da palavra grega *kyber* (para navegar), se referindo ao espaço conceitual dentro das tecnologias de informação e comunicação (TIC), ao invés de uma tecnologia. O ciberespaço não é um ambiente homogêneo, mas consiste em outros espaços digitais navegáveis em rápida expansão, em que cada um fornece uma forma diferente de interação digital e comunicação.

Para Lawrence Lessig (2006, p.9), a Internet é o meio pelo qual nos comunicamos por meio do uso dos *e-mails* e no qual as páginas *web* são publicadas, ou seja, é o espaço usado

para realizar atividades cotidianas, como encomendar produtos em lojas (físicas e/ou virtuais) ou buscar por informações (de horários de cinema até artigos acadêmicos). Por sua vez, o espaço cibernético está estabelecido acima desse meio, associado à experiência da interação humana e da comunicação via Internet. Ou seja, se trata do "mundo virtual" no qual as pessoas interagem através das redes de computadores.

Com a relevância cada vez maior do ciberespaço, os países também descrevem como seria esse ambiente em suas estratégias de segurança cibernética. A estratégia cibernética da Alemanha, por exemplo, define o ciberespaço como

> a área virtual de todos os sistemas de tecnologia da informação do mundo que estão ou podem estar interconectados no nível dos dados. O ciberespaço como uma rede acessível ao público é baseado na internet, que pode ser expandida por meio de quaisquer outras redes de dados (GERMANY, 2021, p. 125, tradução nossa).[23]

Em 2008, os EUA, por meio do Pentágono, definiram o seu entendimento do ciberespaço como sendo um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas informáticos, processadores e controladores incorporados (THE UNITED STATES, 2019, p.55, tradução nossa). Atualmente, a estratégia cibernética dos Estados Unidos define que o ciberespaço é fundamental para o crescimento do país, sendo componente integral para todas as facetas da vida estadunidense, incluindo a economia e a defesa (THE WHITE HOUSE, 2018a).

Em 2011, a Colômbia publicou a política *Lineamentos de Política para Ciberseguridad y Ciberdefensa*, que define o ciberespaço como "o ambiente físico e virtual composto por computadores, sistemas de computador, programas de computador (software) e redes de telecomunicações, dados e informações, no qual os usuários interagem entre si" (REPÚBLICA DE COLOMBIA, 2011, p. 38, tradução nossa). No entanto, a falta de uma linguagem comum para as questões do ciberespaço traz algumas divergências entre os países sobre seu alcance e proteção. Segundo Raud (2016), a China utiliza uma terminologia diferente do ocidente - a palavra "cibernético", por exemplo, quase não é utilizada. Enquanto a visão dos países do ocidente parte da ideia de que o ciberespaço é um domínio global que abrange o uso de eletrônicos, redes interdependentes, a internet, e dados de telecomunicações, na China, o termo mais próximo de ciberespaço seria traduzido como "os componentes necessários para conectar

[23] Em inglês: Cyberspace is the virtual area of all information technology systems in the world which are or could be interconnected at data level. Cyberspace as a publicly accessible network is based on the internet, which can be expanded by means of any other data networks.

um dispositivo a uma rede para fins específicos de comunicação via protocolos como o HTML, e-mail e assim por diante" (GILES; HAGESTAD, 2013, p.7, tradução nossa). Neste sentido, a Rússia acompanharia a mesma compreensão, definindo o ciberespaço apenas com um subconjunto do "espaço de informação", que seria uma esfera de atividade relacionada com a formação, criação, conversão, transferência, uso e armazenamento de informação e que tem um efeito sobre a consciência individual e social, sendo um domínio para se comunicar com toda a população mundial (GILES; HAGESTAD, 2013).

Para evitar possíveis conflitos teórico-conceituais entre essas diferentes visões, essa pesquisa utiliza a definição de Singer e Friedman (2014), que considera que o ciberespaço, antes de tudo, é um ambiente de informação composto por dados digitalizados que são criados, armazenados e compartilhados, não se tratando de um lugar físico e, portanto, desafiando a medição física. No entanto, não se trata de um ambiente puramente virtual, compreendendo os computadores, os sistemas e toda infraestrutura que permite seu fluxo, incluindo a Internet, redes de computadores, *intranets*[24], celulares, cabos de fibra óptica e comunicações baseadas em satélites, abrangendo também as pessoas por trás desses equipamentos (SINGER; FRIEDMAN, 2014). Por fim, vale destacar algumas características que são importantes para entender o ciberespaço: (i) a inexistência de fronteiras, o que viabiliza que um ataque possa ser disparado de qualquer lugar do planeta; (ii) a possibilidade do anonimato, que dificulta o rastreamento de ataques; (iii) a maior facilidade e os menores custos de realização de ataques cibernéticos em comparação com a proteção no ciberespaço. Dessa forma, pode-se começar a entender como os ataques cibernéticos podem ser perigosos para as pessoas e as estruturas mais complexas, como as infraestruturas críticas, tema do próximo tópico.

2.2 AS INFRAESTRUTURAS CRÍTICAS

As infraestruturas críticas são estruturas físicas, instalações, serviços, bens e sistemas que se forem interrompidos ou destruídos (total ou parcialmente), podem ocasionar um sério impacto social, econômico e político, bem como à segurança nacional. As mais conhecidas são, geralmente, as infraestruturas de comunicações, energia, finanças, transportes e águas (SANTOS; CARVALHO; CAVALCANTE, 2010). No entanto, os países, conforme suas necessidades e visão estratégica, é que determinam quais são as suas infraestruturas críticas,

[24] A *intranet* é uma rede de computadores privada que faz uso dos protocolos da Internet para funcionar, entretanto, seu uso é exclusivo de determinada organização como, por exemplo, uma empresa, universidade, etc, sendo acessível apenas por pessoas vinculadas a essas instituições.

sendo sua operação, segura e confiável, de suma importância para o Estado e a vida econômica e soberania de uma nação (TEN; MANIMARAN; LIU, 2010).

Nos Estados Unidos, a Ordem Executiva 13010, de 1996, que trata da Proteção da Infraestruturas Críticas naquele país, descreve essas estruturas como "infraestruturas nacionais vitais cuja incapacidade ou destruição teriam um impacto debilitante na defesa ou na segurança da economia" (CLINTON, 1996, p. 3, tradução nossa). Como são os países que avaliam e determinam quais são suas infraestruturas críticas, nos Estados Unidos são 16 setores que merecem atenção para proteção, o químico, o de comunicações, o de barragens, o de serviços de emergência, o de serviços financeiros, o de instalações governamentais, o de tecnologia da informação, o de sistemas de transporte, o de instalações comerciais, o de manufatura, o de indústria de defesa, o energético, o de alimentos e agricultura, o de saúde e saúde pública, o de reatores nucleares e o sistema de água e esgoto (CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, 2019).

A partir dos atentados de 11 de setembro a preocupação com a proteção das infraestruturas críticas se tornou uma tendência e, em 2020, foi sancionada a estratégia do Brasil (BRASIL, 2020). No entanto, a estratégia brasileira não é tão específica quanto a estadunidense em relação aos setores que serão protegidos. Assim, o Brasil define de forma abrangente que as infraestruturas de comunicações, energia, transportes, finanças e de águas possuem uma dimensão estratégica para a soberania nacional (BRASIL, 2020). Em relação às ações adotadas pelo país para proteção das infraestruturas críticas descritas na estratégia destacam-se a criação de grupos técnicos compostos por especialistas, a identificação das possíveis ameaças e vulnerabilidades dessas infraestruturas, a análise de riscos continuada, e a conscientização e capacitação, entre outras (BRASIL, 2020).

Embora muitas dessas indústrias não estejam envolvidas especificamente com tecnologia, várias delas possuem os sistemas cibernéticos como sua espinha dorsal, o que significa que um incidente de segurança nos seus sistemas pode ter impacto sobre a confiança das operações seguras dos sistemas físicos que dependem deles. Isso fez com que muitos países criassem órgãos e estruturas para proteção de suas infraestruturas. É o caso do *Centro Nacional de Protección de Infraestructuras y Ciberseguridad* (CNPIC) da Espanha, criado em 2011, através da Lei 8, que estabelece medidas para a proteção das infraestruturas críticas (GOBIERNO DE ESPAÑA, 2011), assim como do *Cybersecurity & Infrastructure Security Agency* (CISA) dos Estados Unidos, criado em 2018. Entre outros exemplos de instituições com a missão de proteger essas estruturas temos o *Centre for Protection of National Infrastructure* (CPNI), do Reino Unido, o *Cyber and Infrastructure Security* (CISC), da Austrália, e o *Centro*

de Respuesta a Incidentes de Seguridad Informática (D-CSIRT[25]), do Uruguai, que foi criado em 2015 e está sob o comando das Forças Armadas do país. Para responder aos incidentes cibernéticos, esses centros precisam conhecer as técnicas de segurança e defesa cibernéticas, tema do próximo tópico deste capítulo.

2.3 SEGURANÇA E DEFESA CIBERNÉTICAS

Para tratar sobre segurança cibernética, é necessário conhecer o conceito de segurança da informação, que é definido pela norma internacional ISO/IEC 27000:2018 como a preservação da confidencialidade, integridade e disponibilidade da informação (CID) (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018). Diante disso, a informação pode ter muitas formas, armazenada em papel ou meio eletrônico, e podendo ser transmitida através da voz, em meios físicos e eletronicamente através dos meios digitais – como filmes, músicas, entre outros (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018). Em uma visão mais ampla, pode-se definir a segurança da informação como uma área do conhecimento que estuda a proteção dos ativos[26] de informação contra acessos não autorizados, alterações indevidas e sua indisponibilidade. Dessa forma, a área de conhecimento trata de criar regras que devem incidir sobre todo o ciclo de vida da informação (manuseio, armazenamento, transporte e descarte), buscando identificar ameaças, vulnerabilidades e seus possíveis controles (SÊMOLA, 2014).

As ameaças são agentes ou condições que afetam as informações e seus ativos por meio da exploração de vulnerabilidades, causando a perda dos atributos de confidencialidade, integridade e disponibilidade, acarretando impactos nos negócios e/ou processos de uma organização. As vulnerabilidades, por outro lado, são fragilidades presentes em ativos de informação que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação.

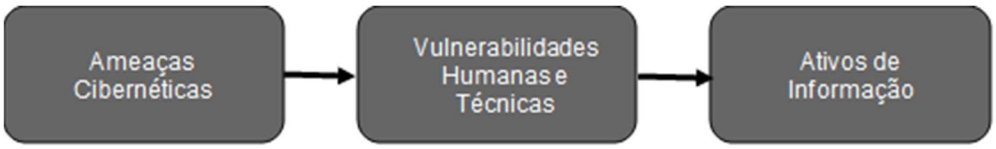
---

[25] O Grupo de Resposta de Incidentes de Segurança (*Computer Security Incident Response Team* - CSIRT), se trata de uma organização que recebe, analisa e responde incidentes de segurança de computadores. São grupos técnicos que têm por objetivo manter a segurança da informação das organizações, que podem ser empresas ou, até mesmo, dedicadas às estruturas dos países. O CSIRT pode exercer tanto funções reativas (geração de alertas de segurança, gestão de vulnerabilidades e de incidentes e tratamento de vírus, entre outros, quanto proativas (auditoria, manutenção de ferramentas, aplicações e infraestrutura de segurança, detectar intrusões, e etc). A Equipe de Resposta a Emergência de Computadores (*Computer Emergency Response Team* - CERT), ou, também trabalha na proteção, detecção e resposta a incidentes, no entanto, é encontrada, geralmente, em governos, comércio e na academia, ao contrário do CSIRT que é genérico e, normalmente, adotado por empresas. A diferença mais marcante está no escopo dos deveres e responsabilidades de cada um, o CERT trabalha com a comunidade da internet para solucionar incidentes 24h por dia. No caso do CSIRT, seus serviços podem ter um cliente definido, que pode variar os serviços conforme a contratação.

[26] Considera-se um ativo tudo aquilo que tem valor para um indivíduo, uma organização ou um governo.

Vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, ou seja, precisam de um agente causador, que são as ameaças (SÊMOLA, 2014). Exemplos disso são os erros de codificação ou a configuração incorreta de sistemas, aplicativos ou equipamentos, que, consequentemente, podem levar a ameaças, como acessos indevidos e vazamentos de dados, entre outros. A Figura 1, abaixo, sintetiza as relações existentes entre ameaças, vulnerabilidades e ativos de informação, conforme discutidas acima.

Figura 1 - Relação entre ameaças, vulnerabilidades e ativos de informação



Fonte: Elaboração própria

A segurança cibernética se destina à proteção do ciberespaço, e os recursos que mantêm esse ambiente são oriundos de ativos de tecnologia de informação e comunicação, formados através de um ambiente de natureza híbrida – *hardware* e *software* – e interligados por inúmeras redes de computadores. O ciberespaço, nesse contexto, é entendido como o "[a]mbiente complexo resultante da interação de pessoas, *software* e serviços na Internet, suportado por instrumentos físicos de tecnologia da informação e comunicação (TIC) e redes conectadas e distribuídas pelo mundo inteiro" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015, p. 9).

No entanto, quando se estuda o ciberespaço, existem questões de segurança não atendidas pela atual segurança da informação, como a de Internet, a de redes e as chamadas "melhores práticas recomendadas" de segurança de TIC, bem como as lacunas entre esses domínios e a falha de comunicação entre organizações e provedores no ciberespaço (ABNT, 2015). Dessa forma, a segurança cibernética se baseia na segurança da informação, na segurança da Internet e na segurança de TIC como blocos de construção fundamentais. No entanto, sua definição considera que a proteção do ciberespaço deve levar em conta aspectos físicos, sociais, financeiros, políticos, emocionais, profissionais, psicológicos, educacionais ou outros tipos ou consequências de falhas, danos, erros, acidentes, prejuízos ou quaisquer eventos considerados indesejáveis neste ambiente (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015)As ações de segurança cibernética visam proteger a sociedade, os governos

e as empresas dos novos desafios do ciberespaço, tais como o *cyberbullying*,[27] a espionagem cibernética, o ciberterrorismo e o ataque cibernético entre países (VON SOLMS; VAN NIEKERK, 2013).

Os exemplos citados demonstram o quão heterogêneas podem ser as ameaças do ciberespaço. Devido a isso, alguns países, como Austrália (AUSTRALIAN GOVERNMENT, 2020), Colômbia (REPÚBLICA DE COLOMBIA, 2016), Espanha (GOBIERNO DE ESPAÑA, 2019) e Estados Unidos (THE WHITE HOUSE, 2018), desenvolveram estratégias de segurança cibernética, alinhadas com suas estratégias nacionais de segurança, para promover a proteção da privacidade, da sociedade, dos negócios, da propriedade intelectual e das suas infraestruturas críticas. Essas estratégias propõem uma série de ações, como conscientização da população, educação de profissionais, políticas de desenvolvimento de uma indústria *ciber* e o estabelecimento de órgãos responsáveis – em suma, estabelecem os objetivos para que uma nação tenha um ciberespaço mais seguro.

Isto posto, torna-se difícil enquadrar as ações de interrupção, sabotagem e crime cibernético na mesma categoria de ações previstas numa estratégia de segurança cibernética, como o que ocorreu contra a Estônia,[28] por exemplo (MCGUINNESS, 2017). Essas ações ofensivas recaem sobre a responsabilidade das Forças Armadas, compreendendo, assim, a defesa cibernética. Essa preocupação fez com que as Forças Armadas de alguns países decidissem elaborar uma doutrina militar para a proteção do ciberespaço. Por exemplo, em 2019, a França atualizou os documentos *Politique Ministérielle de Lutte Informatique Défensive* e *Éléments Publics de Doctrine Militaire de Lutte Informatique Offensive*, os quais

[27] É o *bullying* realizado por meio das tecnologias digitais. Consiste no ato de difamar, ameaçar, humilhar ou provocar ato que seja mal-intencionado a outros, podendo ocorrer nas redes sociais, plataformas de mensagens, jogos ou através de celulares. Podem ser citados como exemplos o compartilhamento de fotos constrangedoras de uma pessoa nas redes sociais e o envio de mensagens maldosas se fazendo passar por outra pessoa (UNICEF, 2022).

[28] Em maio de 2007, o governo da Estônia decidiu retirar um monumento histórico de guerra soviético, que comemorava os soldados do Exército Vermelho que combateram os nazistas na Segunda Guerra Mundial, do centro da capital do país, Tallinn. A retirada da estátua, conhecida como Soldado de Bronze, provocou confrontos nas ruas de Tallinn, deixando ao menos um morto e vários feridos. Além disso, a retirada do monumento também provocou uma crise nas relações entre a Estônia e a Rússia, pois o governo russo classificou com um insulto a atitude do governo estoniano contra os soldados que morreram ao livrar a região dos nazistas. Desta forma, o governo da Estônia considera que ataques cibernéticos começaram logo após a estátua ser removida, fazendo com que a comunicação dos sites do país com o resto do mundo ficasse interrompida. Os sites do governo, bem como sites de empresas e bancos do país foram "bombardeados" por uma enorme quantidade de requisições de acesso, acima da capacidade de processamento dos servidores, tornando esses sites indisponíveis. Os ataques começaram no final de abril daquele ano, coincidindo com a retirada do monumento, e, conforme o Ministério da Defesa da Estônia, os contínuos ataques cibernéticos contra os sites do país vinham de todas as partes do mundo, no entanto muitos deles estariam vindo de sites hospedados na Rússia. Além disso, segundo o ministério, instruções em russo sobre como realizar ataques estariam circulando em sites da Rússia. Apesar das acusações, a Rússia não cooperou com as investigações, que ficaram por conta de especialistas da OTAN e de outros países da União Europeia (MYERS, 2007; MCGUINNESS, 2017).

descrevem a doutrina do Ministério da Defesa francês sobre a guerra cibernética defensiva e ofensiva (DELERUE, 2019). O segundo documento define a guerra cibernética ofensiva militar como

> Todas as ações militares realizadas no ciberespaço, em apoio ou não a outras capacidades militares. As armas cibernéticas visam, de acordo com o direito internacional, produzir efeitos contra um sistema de computador adversário para alterar a disponibilidade ou a confidencialidade dos dados (RÉPUBLIQUE FRANÇAISE, 2019, p. 5, tradução nossa).[29]

A título de comparação, e para demonstrar que essa é uma tendência entre os países, em 2014, o Ministério da Defesa do Brasil lançou a Doutrina Militar de Defesa Cibernética do Brasil, que estabelece os fundamentos da defesa cibernética nas Forças Armadas do país. De acordo com o documento, tais fundamentos são o

> 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, 2014b, p. 18).

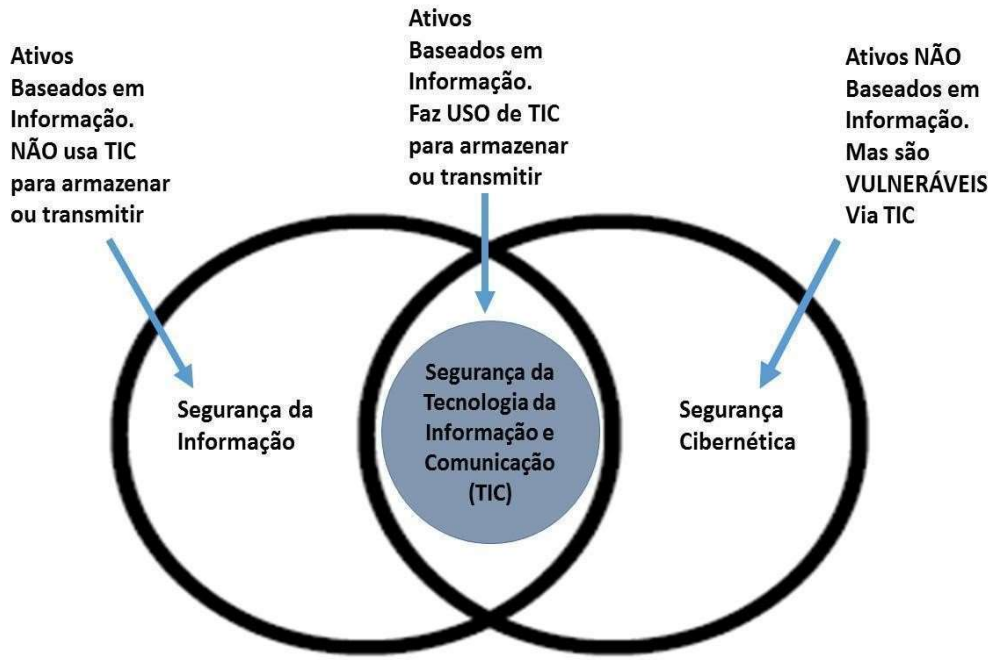
Segundo Villa e Reis (2006), o conceito de segurança cibernética está mais ligado a questões defensivas, fazendo referência ao combate e à prevenção dos chamados crimes cibernéticos na esfera pública – ou seja, no nível político. Já as ações defensivas, ofensivas e exploratórias realizadas no ciberespaço, dentro de um contexto de planejamento militar, são coordenadas por um órgão militar. Assim, considerando-se os aspectos táticos e operacionais do ciberespaço, são as forças armadas que têm a responsabilidade de aplicar a estratégia, com a finalidade de prevenir ou responder em caso de ataques cibernéticos contra a soberania nacional. Muitos países já possuem sua força ciber formalizada, como o Brasil (ComDCiber) e os Estados Unidos (USCYBERCOM), além do IDF *Cyber Defense* de Israel, do *Defence Cyber Agency* (DCA) da Índia, do *Comando Conjunto Cibernético* (CCC) da Colômbia, do *Comando Conjunto de Ciberdefensa* da Argentina, do *Australian Signals Directorate* (ASD) da Austrália, do *Commandement de la cyberdéfense* (COMCYBER) da França, entre outros.

Por fim, com base no tipo de ativo e na necessidade do uso, ou não, de TIC, é possível dizer que a segurança da informação é baseada em qualquer tipo de ativo de informação, não

[29] Em francês: La lutte informatique offensive à des fins militaires (LIO) recouvre l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels. L'arme cyber vise, dans le strict respect des règles internationales, à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données.

precisando, necessariamente, estar armazenado em ativos de TIC. No caso da segurança de TIC, os ativos de informação são baseados em TIC para transmissão e armazenamento (computadores, redes, pendrives, smartphones, etc.). Na segurança cibernética, por outro lado, os ativos não precisam ser baseados em informação, sendo, contudo, vulneráveis através de recursos de TIC (pessoas, infraestruturas críticas, etc.). A Figura 2 demonstra, de forma sintetizada, a intersecção e/ou correlação entre a segurança da informação, a segurança de TIC e a segurança cibernética, e suas dependências em relação aos ativos de informação.

Figura 2 - Correlação entre Segurança da Informação, Segurança de TIC e Segurança Cibernética



Fonte: Elaborada pelo autor a partir de Von Solms e Van Niekerk (2013, p. 101).

A percepção de que o ciberespaço se tornou um domínio a ser protegido, em que até mesmo doutrinas militares surgissem, inseriu a possibilidade da securitização desse ambiente. Dessa forma, o próximo tópico deste capítulo apresenta a perspectiva teórica da Escola de Copenhague, que é considerada uma teoria abrangente, sendo capaz de inserir o tema da segurança cibernética na realidade das discussões das Relações Internacionais.

2.4 A ESCOLA DE COPENHAGUE

Com o fim da II Guerra Mundial, a teoria realista das Relações Internacionais se

estabeleceu como referência teórica predominante, assumindo a proposta de que os Estados são guiados pelo interesse de aumentar o próprio poder no sistema internacional. Além disso, outra característica Realista importante seria o princípio da soberania, ou seja, a inexistência de um ator superior aos demais, não havendo, hierarquicamente, um poder coercitivo para resolver litígios ou manter a ordem do sistema, como existe na política interna (WALTZ, 1979; ACHARYA; BUZAN, 2019). No entanto, a teoria Realista foi alvo de muitas críticas, entre outros motivos, pois se mostrou incapaz de prever (e mesmo explicar de forma satisfatória) os destinos da Guerra Fria, incentivando a formulação de novas teorias – inclusive na subárea de estudos de segurança internacional (TANNO, 2003).

É justamente nesse contexto de reformulações teóricas que, a partir da criação do *Copenhagen Peace Research Institute*, é fundada a Escola de Copenhague, em 1985. Surge com a missão de ampliar e redefinir as questões a serem abordadas no âmbito dos estudos de segurança internacional. Sua perspectiva teórica pode ser considerada abrangente, pois sustenta que as ameaças à segurança não provêm apenas da esfera militar, mas também das esferas ambiental, política, econômica e societal (KREMER; MÜLLER; GMBH, 2016).

A Escola de Copenhague buscava trazer à discussão certos aspectos de uma perspectiva construtivista, que entende que a realidade material e social se desenvolve respondendo a determinados problemas, se fundamentando em interpretações guiadas por ideias e percepções da realidade, que são construídas no interior da sociedade e guiam as ações dos agentes, moldando suas visões de mundo e sendo por elas moldadas (DUQUE, 2009). Desta forma, seus conceitos de securitização e segurança social têm sido aplicados a uma série de contextos e problemas empíricos, que incluem, por exemplo, conflitos étnicos (ROE, 2014), tráfico de drogas (JACKSON, 2006) e combate ao HIV (ELBE, 2006), entre outros. Assim, em busca de conceitos que se apliquem à questão da cibersegurança e que possam aproximá-la das discussões das Relações Internacionais, o próximo item apresenta uma das principais contribuições da Escola de Copenhague, a Teoria da Securitização.

2.4.1 Teoria da Securitização

Conforme visto, a Escola de Copenhague busca ampliar sua atenção em áreas e/ou contextos sociais que não foram alcançados por outras teorias de Relações Internacionais. Assim, entre suas contribuições, o conceito de securitização apresenta-se como um dos mais relevantes, e se caracteriza pela ideia de que as temáticas que são estabelecidas como objetos de segurança ganham *status* de ameaça em determinado contexto social e são construídas a

partir de um processo de interpretação social acerca do problema. Desta forma, acabam sendo projetadas por meio de uma agenda política que transforma a questão em um problema de caráter securitizado (SILVA; PEREIRA, 2019). A construção desse processo fica caracterizada, inicialmente, pela politização da questão, na qual o tema ganha viés de relevância pública, devendo o Estado resolver o problema por meio de políticas públicas. Em seguida, a acentuação do problema pode levar a uma etapa mais elevada, na qual a questão passa a ser tratada como uma ameaça direta à ordem social e política, logo, colocando em risco a própria sobrevivência estatal, tornando-se uma ameaça à segurança nacional ou internacional (BUZAN; WAEVER; DE WILDE, 1998).

Segundo Buzan e Waever (1995), a segurança define algo como ameaçador, exigindo, portanto, uma resposta urgente. A securitização, portanto, deve ser estudada no discurso com estrutura retórica e semiótica em particular que consegue trazer um efeito suficiente para fazer com que o público tolere violações de regras que, de outra forma, teriam que ser obedecidas. Ou seja, a segurança, nesse contexto, é enquadrada como algo que estaria acima - ou para além - da política (BUZAN; WAEVER; DE WILDE, 1998). Assim, a securitização é uma questão que não é debatida como uma questão política, mas sim tratada em ritmo acelerado e de maneiras que possam violar regras legais e normas sociais (BUZAN; WÆVER; DE WILDE, 1998). Através de um conceito geral de segurança, a Escola de Copenhague constrói um discurso de segurança nacional que implica na ênfase da autoridade que enfrenta as ameaças e inimigos, sendo capaz de tomar decisões e de adotar medidas emergenciais para enfrentá-los. Assim sendo, a segurança tem uma força discursiva e política, alcançando a securitização através do estabelecimento de um ameaça existencial capaz de trazer efeitos políticos substanciais (BUZAN; WAEVER; DE WILDE, 1998). Para Barry Buzan, Ole Waever e Jaap de Wilde (1998), o discurso de segurança costuma ser usado para legitimar ações extraordinárias, que vão além do escopo normativo existente. Dessa forma, a abordagem do ato de fala para a segurança requer uma distinção entre três tipos de unidades envolvidas na análise de segurança, que são: objetos de referência, agente securitizador e atores funcionais (BUZAN; WAEVER; DE WILDE, 1998, p. 36).

O objeto de referência é aquilo que é existencialmente ameaçado, em linhas gerais o Estado - no entanto, a Escola de Copenhague abre espaço para que unidades não estatais sejam consideradas como objetos referentes da securitização, podendo ser indivíduos, grupos sociais, organizações, grupos transnacionais, etc. (BUZAN; WAEVER; DE WILDE, 1998). O agente securitizador, por sua vez, é o ator político que é capaz de demonstrar que determinado tema precisa ser reconhecido pelo público como uma ameaça existencial, a fim de chamar atenção

para a necessidade de se tomarem ações de emergência para proteger um determinado objeto referente (BUZAN; WAEVER; DE WILDE, 1998). Por fim, os atores funcionais são os agentes que influenciam de forma significativa a dinâmica das decisões na área de segurança (BUZAN; WAEVER; DE WILDE, 1998), como as agências de inteligência, as Forças Armadas e a indústria armamentista, entre outros.

Para os autores, a securitização é um "ato de fala" (*speech act*), que se baseia na premissa de que o discurso é uma forma de ação que carrega consequências (BUZAN; WAEVER; DE WILDE, 1998, p. 26**)**. Para a Escola de Copenhague, palavras que fazem ameaças à existência trazem consigo a demanda de que medidas sejam tomadas para contrabalanceá-las (DUQUE, 2009). Segundo Wæver (1995), esse aspecto é reforçado quando o agente securitizador é um representante do Estado que se encontra em condições de implementar medidas de securitização:

> O que é, então, a segurança? Com a ajuda da teoria da linguagem, podemos considerar "Segurança" como um ato de fala. Nesse uso, a segurança não interessa como signo que se refere a algo mais real; o enunciado em si é o ato. Ao dizê-lo, algo é feito (como apostar, fazer uma promessa, nomear um navio). Ao proferir "segurança", um representante do estado move um determinado empreendimento para uma área específica e, portanto, reivindica o direito especial de usar todos os meios necessários para bloqueá-lo (WAEVER, 1995, p.73, tradução nossa).[30]

No entanto, os autores destacam que para se estudar a securitização, é preciso conhecer os discursos de securitização, que possuem uma estrutura retórica específica (BUZAN; WAEVER; DE WILDE, 1998). O agente securitizador, nesse tipo de discurso, faz referência à sobrevivência de uma unidade, bem como define a prioridade de ação para conter uma ameaça à sua existência. Dessa forma, a securitização não possui um significado único, mas, sim, se baseia em seu uso por parte do agente securitizador (DUQUE, 2009).

Segundo a Teoria da Securitização da Escola de Copenhague, qualquer assunto público pode ser alocado no *continuum* que varia de temas não-politizados, passando por aqueles politizados até chegar aos securitizados. Quando um tema é politizado, significa que é objeto de políticas públicas e requer decisões governamentais. Já os não-politizados são aqueles que não são objeto de políticas públicas de Estado ou de debates públicos. Por fim, um tema se torna securitizado quando é apresentado como uma ameaça existencial que necessita de ações

[30] Em inglês: What then is security? With the help of language theory, we can regard "security" as a speech act. In this usage, security is not of interest as a sign that refers to something more real; the utterance itselfis the act. By saying it, something is done (as in betting, giving a promise, naming a ship). By uttering "security," a state-representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it.

emergenciais fora dos procedimentos normais da decisão política, podendo ser analisado, de uma maneira geral, como uma versão extrema da politização (BUZAN; WAEVER; DE WILDE, 1998). Segundo os autores, a segurança é:

> o movimento que leva a política além das regras estabelecidas do jogo e enquadra a questão como um tipo especial de política ou acima da política. A securitização pode, portanto, ser vista como uma versão mais extrema de politização. Em teoria, qualquer questão pública pode ser localizada no espectro que vai desde não politizado (ou seja, o estado não lida com isso e não é de nenhuma outra forma tornado uma questão de debate público e decisão) até politizado (o que significa que a questão é parte de política pública, exigindo decisão governamental e alocação de recursos ou, mais raramente, alguma outra forma de governança comunal) para securitizar (o que significa que a questão é apresentada como uma ameaça existencial, exigindo medidas emergenciais e justificando ações fora dos limites normais do procedimento político) (BUZAN; WAEVER; DE WILDE, 1998, p. 23-24, tradução nossa).[31]

Como dito anteriormente, a evolução de um tema nesse *continuum* depende da capacidade do agente securitizador de convencer determinada audiência da ameaça, fazendo uso do discurso e da linguagem apropriada para isso, bem como das condições do contexto social envolvido. Assim sendo, o sucesso da securitização depende do convencimento da audiência receptora desse discurso, além de que sejam capazes de reconhecer os riscos que decorrem das ameaças existenciais. Portanto, a securitização bem-sucedida depende de que a audiência reconheça os riscos envolvidos e que legitime as ações emergenciais necessárias para lidar com eles (SILVA; PEREIRA, 2019). Assim, através do discurso, o agente securitizador sustenta a necessidade dessas medidas, que envolvem a quebra das regras que estão estabelecidas no âmbito político (BUZAN; WAEVER; DE WILDE; 1998).

Para ampliar o entendimento da questão, os autores estabeleceram setores de análise - militar, econômico, ambiental, político e social - que podem impactar, influenciar e afetar uns aos outros (BUZAN; WAEVER; DE WILDE; 1998), sendo que esses estão em níveis sistêmicos, sub-sistêmicos, regionais e locais. A partir disso, a escola de Copenhague apresenta uma resposta muito convincente e prática ao desafio tradicional para uma definição elegante de segurança. Leva a sério o desafio tradicionalista para a coerência, mas rejeita seu foco apenas em questões militares. Em vez disso, prefere explorar a lógica da própria segurança para

[31] Em inglês: "Security" is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Securitization can thus be seen as a more extreme version of politicization. In theory, any public issue can be located on the spectrum ranging from nonpoliticized (meaning the state does not deal with it and it Innot in any other way made an issue of public debate and decision) through politicized (meaning the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance) to securitized (meaning the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure).

descobrir o que distingue a segurança e o processo de securitização de outros assuntos menos pertinentes. Isto posto, o próximo item discute a inserção do conceito de securitização na temática da segurança cibernética.

2.4.2 Securitização cibernética

O conceito de segurança cibernética chegou à agenda pós-Guerra Fria em resposta a uma série de inovações tecnológicas e mudanças nas condições e dinâmicas geopolíticas (HANSEN; NISSENBAUM, 2009). No entanto, no início da década de 1990, a segurança de computadores tinha um viés apenas técnico, ou seja, os analistas de computação da época tratavam apenas de identificar e tratar as vulnerabilidades em computadores, rotulando essa prática de segurança técnica de computadores (NISSENBAUM, 2005). Em 1988, o *Defense Advanced Research Projects Agency* (DARPA) solicitou ao *Computer Science and Telecommunications Board* que abordasse a segurança e a confiabilidade dos sistemas de computação dos Estados Unidos, estruturando-se, a partir daí o *System Security Study Committee,* que era formado por dezesseis indivíduos da indústria e da academia, com a missão de desenvolver uma agenda nacional de pesquisa para ajudar o país a alcançar uma base tecnológica mais confiável até o final do século (NATIONAL RESEARCH COUNCIL, 1991).

Um dos resultados do trabalho do comitê foi, em 1991, a publicação do livro *Computers at Risk: Safe Computing in the Information Age*, que começou a apresentar os primeiros conceitos da segurança cibernética nacional, afirmando, por exemplo, que "[a] nação precisa de tecnologia de computadores que suporte substancialmente maior segurança, confiabilidade e, em particular, segurança" (NATIONAL RESEARCH COUNCIL, 1991, p. 2, tradução nossa). O livro também destacava que novas vulnerabilidades apareciam à medida que os computadores se tornavam mais comuns, inclusive como componentes de equipamentos de transporte ou interligados, cada vez mais, em sistemas financeiros internacionais, de tal forma que ataques nesses ambientes poderiam ter impactos expressivos. Além disso, a obra também alertava para uma possível mudança nos conflitos militares convencionais, uma vez que as ameaças cibernéticas poderiam levar à competição econômica e concentração de informação, não especificando, no entanto, como esse "novo" conflito seria travado (NATIONAL RESEARCH COUNCIL, 1991).

Com o passar dos anos, o progressivo desenvolvimento de novas tecnologias conectadas à Internet elevou o número de vulnerabilidades em sistemas de computadores, confirmando as expectativas apresentadas na obra. Nesse contexto, o número de ameaças cibernéticas cresceu

vertiginosamente e, atualmente, atinge todos os tipos de organizações, incluindo as nações, fazendo com que essa preocupação seja cada vez mais validada por políticos, corporações privadas e a mídia, que chegaram a falar sobre um possível "*Pearl Harbor* eletrônico"[32] provocado por armas eletrônicas que poderiam trazer ameaças graves ao mundo ocidental (LATHAM, 2005). Com os ataques contra as Torres Gêmeas do *World Trade Center*, em 11 de setembro de 2001, foi estimulada ainda mais a atenção dada aos computadores, tecnologia da informação e segurança, com um cuidado especial para as questões digitais, principalmente aquelas ligadas à proteção das infraestruturas críticas, vigilância eletrônica e a atenção com o uso de *hackers* patrocinados por Estados (LATHAM, 2005).

O trabalho do *System Security Study Committee,* em 1991, destacava a existência de um discurso securitizador de que estamos em risco, no qual muitas vezes são referidas frases como "o terrorista do amanhã poderá ser capaz de causar mais dano com um teclado do que com uma bomba" (COUNCIL, 1991, p.7, tradução nossa). Nesse cenário, o tom de urgência e de despertar para o problema é encontrado na política de segurança cibernética dos Estados Unidos de 2003, que destaca, por meio de uma abordagem abrangente, que nos anos anteriores à sua publicação, as ameaças no ciberespaço aumentaram drasticamente devido à crescente melhoria da capacidade técnica e sofisticação dos usuários empenhados em causar estragos ou interrupções (THE UNITED STATES, 2003). Argumentar que incidentes graves se materializarão em um futuro próximo, caso nenhuma ação seja realizada, é elemento-chave do discurso securitizador, que necessita constituir um público muito complacente, que não perceba a magnitude desses perigos, constituindo assim, outro elemento do discurso securitizador (BUZAN; WAEVER; DE WILDE, 1998).

Como exemplo do discurso de securitização, em 2016, Zhao Zeliang, Diretor-geral Departamento de Cibersegurança da Administração do Ciberespaço da China (*Bureau of Cybersecurity of Cyberspace Administration of China*), defendeu, em uma conferência, que Pequim faria todo o possível para proteger a segurança da informação do país e de seus cidadãos, além de defender uma internet segura e controlável (MOREIRA; DURAN, 2020). Nesse sentido, em 2015, o presidente chinês, Xi Jinping, defendeu o conceito de "ciber soberania", que define o direito de uma nação de desenvolver e regular sua internet, constituindo esse ambiente como uma extensão da soberania nacional, com as prerrogativas de

[32] Faz menção ao ataque aéreo surpresa da Força Aérea Japonesa contra a base estadunidense de Pearl Harbor em 1941. O termo, também chamado de "11 de setembro digital" e/ou "cibergedom", trata da hipótese de um ataque cibernético sem precedentes contra uma nação, que seria capaz de inviabilizar suas comunicações, finanças e infraestruturas críticas, podendo ser provocado por uma guerra cibernética ou através de terrorismo digital.

jurisdição, autodefesa, independência e igualdade dos países (MCKUNE; AHMED, 2018).

No caminho da securitização cibernética, em 2016, a China promulgou sua Lei de Cibersegurança, que exige cooperação dos operadores de serviços na internet em investigações policiais e, se necessário, que forneçam códigos-fonte e chaves criptográficas. Além disso, todas as tecnologias a serem utilizadas pelo Estado e pelo Partido Comunista, entre outros setores do governo, devem passar por um escrutínio, para que sejam consideradas seguras para serem vendidas ou implantadas (REPÚBLICA POPULAR DA CHINA, 2016). Também em 2016, o governo chinês emitiu um relatório sobre sua segurança cibernética nacional, afirmando que poderia usar de resposta militar para proteger sua segurança da informação, sem detalhar que tipo de retaliação seria essa (HUGHES, 2021).

Assim como os chineses, em sua estratégia nacional de cibersegurança, os Estados Unidos declaram que haverá punição a todos aqueles que o prejudicarem através do ciberespaço, bem como a seus aliados. Para isso, promete utilizar todos os instrumentos do poder nacional para prevenir, responder e deter atividade cibernética maliciosa. Isso inclui diplomacia, força militar (cinética e cibernética), financeira, inteligência e todas as capacidades de aplicação da lei (THE WHITE HOUSE, 2018). Apesar de alguns países, como Estados Unidos, China e Rússia, sugerirem a utilização de força militar cinética contra ataques cibernéticos, a primeira retaliação documentada desse tipo aconteceu em 2019, quando as Forças Armadas de Israel bombardearam um prédio que supostamente serviria de base para um grupo de *hackers* do Hamas (NEWMAN, 2019).

Um dos ativos mais relevantes para o uso desse poder nacional são as infraestruturas críticas, que, cada vez mais, são dependentes de sistemas computacionais e da internet em suas operações. As estratégias dos países destacam a necessidade de proteção dessas estruturas, como no caso dos Estados Unidos, que ressaltam o potencial destrutivo que as ameaças cibernéticas podem ter se disparadas contra as infraestruturas críticas nacionais (THE WHITE HOUSE, 2018). Como se trata de um tema estratégico pela possibilidade de, em caso de ataques, afetar a vida econômica e social de uma nação, muitos países estabelecem estruturas civis de proteção das infraestruturas críticas, como Espanha e Argentina. Porém, existem aqueles que preferem delegar essas tarefas para suas forças armadas, como no caso do Uruguai e da Colômbia. Nissenbaum (2005), exemplifica que um ataque de vírus na internet que corrompa milhares de computadores pode ser interpretado como um ataque criminoso contra indivíduos, mas que esse mesmo ataque, dentro do conceito da segurança cibernética, pode ser interpretado como um ataque contra a nação e, assim, se encontra dentro do espectro da securitização. Além disso, o abrangente conjunto de adversários capazes de disparar ataques

cibernéticos, que podem ser indivíduos desvinculado de redes e/ou ações criminosas, criminosos comuns, terroristas e nações hostis, também corroboram para esse entendimento da securitização (NISSENBAUM, 2005). Dessa forma, para compreender essa elevação da proteção de infraestruturas críticas por militares, Buzan, Waever e De Wilde (1998), consideram que o essencial para a securitização é a designação de uma ameaça existencial que exige ações emergenciais, bem como a aceitação dessas medidas por um público significativo.

Assim, além da atenção com a proteção de grandes infraestruturas, a segurança cibernética também preocupa o setor privado, que teme que grandes somas de dinheiro sejam roubadas, bem como os detentores de propriedade intelectual, que têm medo de ter seus direitos e receitas comprometidos com compartilhamento de arquivos na Internet. Assim sendo, a falta de cuidados do setor privado com a segurança cibernética pode trazer graves consequências para a economia. Desta forma, a segurança cibernética não é deixada apenas para o mercado liberal, mas implica em uma complexa divisão de responsabilidades público-privada com o devido gerenciamento da autoridade governamental (HANSEN; NISSENBAUM, 2009).

Em 2003, em depoimento ao Senado dos Estados Unidos sobre a plenária "*Pirataria internacional de direitos autorais, um problema crescente com links ao crime organizado e terrorismo*", Jack Valenti, presidente da *Motion Picture Association of Americ*a (MPAA), defendeu que a cópia e distribuição não autorizada de obras proprietárias representava uma ameaça existencial para seus negócios, que poderia causar uma ameaça terrível à economia do país (THE UNITED STATES, 2013). Segundo Nissenbaum (2005), exemplos como esse mostram que não apenas autoridades governamentais e representantes de interesses públicos endossam o movimento de securitização, mas também detentores corporativos de propriedade intelectual, que tentaram se colocar ao lado do discurso da segurança. Segundo Kassab (2013), o ciberespaço vem sendo securitizado por atores estatais e não estatais. Para Buzan, Waever e De Wilde (1998), o peso relativo dos setores deve depender principalmente do grau de securitização, mas também deve considerar a importância relativa dos tipos de questões quando as preocupações setoriais se chocam.

Baseando-se nessa premissa de corresponsabilidade pela segurança cibernética, estratégias cibernéticas como a dos Estados Unidos colocam o setor privado como aquele que detém o maior conhecimento, bem como possui grande parte das redes de computadores e, assim, destaca o setor como o mais bem equipado e estruturado para responder a uma ameaça cibernética em evolução (THE UNITED STATES, 2003). Segundo Nissenbaum (2005), esse envolvimento entre o poder público e o setor privado impulsiona apelos para a securitização, para a proteção dos direitos de propriedade intelectual, bem como para o julgamento de crimes

cibernéticos e para o combate ao anonimato digital.

Segundo Bendrath (2003), o ciberespaço não respeita as restrições do mundo físico, no qual cada ação encontra suas restrições nas leis da natureza. O voo de um míssil balístico, por exemplo, nunca terá suas equações de cálculo de curva alteradas, não importa de que lugar esse míssil seja disparado. O ciberespaço, em contraste, está em um ambiente artificial onde toda a ação/movimentação é possível. A partir de 1993, surgiu a ideia do ciberterrorismo no governo do presidente Clinton após o primeiro ataque ao *World Trade Center* e o atentado na cidade de Oklahoma, em 1995. No entanto, o governo não tinha uma clareza da origem das potenciais ameaças, considerando os possíveis inimigos como "Estados desonestos", incluindo *hackers* juvenis também nessa listagem (BENDRATH, 2003). Após os ataques contra o *World Trade Center*, em 2001, o governo Bush fortaleceu o discurso do ciberterrorismo, compreendendo que ataques terroristas poderiam acontecer através de outros meios (BENDRATH, 2003). A percepção da ameaça do ciberterrorismo acabou tendo sua repercussão política internacional quando o secretário de Defesa estadunidense, Donald Rumsfeld, em seu discurso no Conselho da OTAN, em 2001, disse aos aliados que os Estados Unidos não eram o único país ameaçado por ataques do ciberespaço, mas que todos os países da OTAN estavam em perigo (BENDRATH, 2003).

Em busca de combate ao terrorismo, em 2001, os Estados Unidos publicaram o *USA Patrioct Act*, um decreto que permitia, entre outras medidas, que os órgãos de inteligência interceptassem comunicações (telefônicas e da Internet) de pessoas suspeitas de envolvimento com o terrorismo. Segundo Bendrath (2003), a primeira proposta do decreto tratava a maioria dos crimes cibernéticos como terrorismo, incluindo, até mesmo, atividades de baixo impacto de risco, como a desfiguração de sites. No entanto, a versão publicada do decreto criminaliza qualquer invasão de computadores, mesmo fora dos Estados Unidos, que seja utilizada de maneira que afete o comércio do país ou estrangeiro, bem como interrompa a comunicação interna (US CONGRESS, 2001). Para Bendrath (2003), este ato legislativo seria o equivalente cibernético da "Guerra ao Terror" mundial que os Estados Unidos vêm lutando desde 11 de setembro de 2001, à medida que se expande sistematicamente para além do território estadunidense.

O ato de securitização move objetos referenciais da política normal para medidas extraordinárias, acima da política, para uma forma mais extrema de politização. Nesse cenário, os Estados, em primeiro lugar, percebem que sua segurança está sob ataque e fazem o que podem para exercer controle. Por outro lado, os atores não estatais veem a Internet como sendo atacada e, dessa forma, também estão fazendo a sua parte para securitizar o ciberespaço, como

é o caso dos *hacktivistas*[33] dos grupos *Anonymous*[34] e *Lulzsec*[35], que veem sua liberdade de expressão na Internet sob ameaça. Assim sendo, suas atividades no ciberespaço são consideradas uma resposta ao que eles percebem como uma tentativa de Estados e corporações de utilizar a Internet para seus propósitos (KREMER; MÜLLER; GMBH, 2016).

Segundo a teoria da securitização, apresentada anteriormente, a segurança está dividida em cinco setores distintos, militar, econômico, ambiental, político e social, que são objetos referenciais que se sobrepõem e se influenciam. Dessa forma, Kassab (2013) considera que a segurança cibernética se encaixa bem com as noções ampliadas de segurança da Escola de Copenhague e, assim, atualiza a teoria, considerando o ciberespaço como um setor que deve ser considerado em um nível de análise, pois é um ambiente artificial, criado pelo homem, com a capacidade de estar presente em todos os lugares, nas mais diversas atividades. O quadro 2 descreve a atualização proposta com a inserção do Ciberespaço como setor de segurança, bem como sendo considerado como um nível de análise que precisa ser estudado, dado que, atualmente, está sendo securitizado por atores estatais e não-estatais.

Quadro 2 - Proposta de atualização dos setores da Escola de Copenhague

ABORDAGEM DE SEIS SETORES	NÍVEIS DE ANÁLISE
(1) Militar	(1) Global
(2) Política	(2) Não regional - sub sistêmico
(3) Societal	(3) Regional
(4) Econômico	(4) Local
(5) Ambiente	(5) Ciberespaço
(6) Ciberespaço	

Fonte: Adaptado de Kassab (2013, p. 91, tradução nossa)

Assim sendo, a pesquisa buscou nesse item discutir a existência de uma securitização cibernética, que, normalmente, acaba sendo analisada através do fator do discurso de que uma ameaça precisa ser apresentada como terrível, iminente e existencial. Além disso, a ameaça precisa ser apresentada a uma audiência e deve ser aceita por esse público como fatal para a

[33] Ideologia ou filosofia que sustenta a prática do *hacking*, que pode ser entendida como uma extensão social do desejo de liberdade de informação e do conhecimento próprio da prática do *hacking*.
[34] É um grupo não identificado, uma espécie de coletivo hacker, constantemente são notícia desde seu início - em atividades benéficas à liberdade e ataques considerados "criminosos".
[35] Diferentemente do Anonymous, o LulzSec é um grupo fechado de indivíduos, com funções delimitadas.

própria existência de um objeto referenciado. Segundo Nisembaum (2005), o conceito de securitização pode acabar se aproximando de algo que chama de "insegurança nacional", em que os elementos-chave são a ameaça de ataque militar, o Estado-nação sob ameaça, e as medidas específicas que os líderes tomam para garantir a segurança do Estado. Por outro lado, para a Escola de Copenhague uma ameaça não precisa ser militar e o objeto de referência não necessita ser o Estado.

Nisembaum (2005) afirma que quando Buzan e Waever propõe um quadro construtivista para definir as questões a serem securitizadas, estão menos preocupados em fornecer uma lista de características de ameaças, vulnerabilidades e modos de defesa, e sim, mais interessados em fornecer um relato sistemático das maneiras como um assunto, condições específicas ou eventos são colocados por atores sociais significativos como ameaças à segurança. Desta forma, a partir do histórico de ações elencadas neste item que trata da securitização cibernética, essa pesquisa parte das ideias de discurso de securitização cibernética, adoção de marco legal abusivo (como o *USA Patriot Act*), fortalecimento da capacidade militar cibernética, abuso de direitos civis e das empresas no ciberespaço, o combate ao ciberterrorismo e proteção da propriedade intelectual, além de qualquer iniciativa que vá além do espectro político, como ponto de partida para a busca de codificações relativas à ações de securitização na metodologia de pesquisa empregada no trabalho. O próximo item trata de outra teoria desenvolvida pela Escola de Copenhague, a Teoria dos Complexos Regionais de Segurança, que considera que a temática da segurança deve ser tratada a partir de uma perspectiva regional. Dessa forma, a pesquisa busca entender se esse conceito pode ser aplicado na América do Sul pelo viés do domínio cibernético.

2.4.3 A Teoria dos Complexos Regionais de Segurança e sua aplicação na América do Sul

Essa seção tem por objetivo discutir a teoria dos Complexos Regionais de Segurança (CRS), elaborada por Buzan e Waever (2003), especialmente no que se refere às perspectivas apresentadas sobre a América do Sul. Desenvolvida no âmbito da Escola de Copenhague, a teoria busca, a partir de um enfoque regional, entender as questões de segurança internacional, partindo do pressuposto de que as ameaças, em geral, estão em distâncias mais curtas do que longas. Para os responsáveis pelo desenvolvimento da teoria, os problemas de segurança são inerentes/intrínsecos a uma região, conquanto ainda sob a influência da polaridade do sistema internacional. Para Buzan e Waever (2003), um CRS pode ser definido como "um conjunto de unidades cujos principais processos de securitização, dessecuritização ou ambos, são tão

interligados que seus problemas de segurança não podem ser razoavelmente analisados ou resolvidos separados uns dos outros" (BUZAN; WAEVER, 2003, p. 44, tradução nossa**)**.

Os autores definiram quatro elementos essenciais para descrever um CRS, as fronteiras do complexo; sua estrutura anárquica; a polaridade, ou seja, a distribuição de poder no complexo; e, os padrões de amizade e inimizade presentes na região (BUZAN, WAEVER; 2003). O elemento da territorialidade se mostra presente pois parte do princípio de que a proximidade física possibilita mais interações de segurança entre os vizinhos do que entre Estados situados em regiões distintas. Desta forma, através dessa definição, os processos de securitização e de dessecuritização devem se desenvolver em *clusters*[36] regionais, fazendo com que o aspecto geográfico desempenhe um importante papel nesta teoria. Para os autores, a utilidade de sua aplicação pode ser dividida da seguinte forma: 1) proporciona um nível adequado em estudos de segurança; 2) possibilita organizar estudos empíricos; 3) torna possível a criação de cenários baseados em teoria (BUZAN, WAEVER; 2003).

Os CRS ficaram em destaque após o final da Guerra Fria, refletindo um novo padrão de segurança internacional que pode ser observado nesse período. Assim, os autores exploram a ideia do fim da bipolaridade, uma vez que sem a rivalidade de superpotências influenciando em todas as regiões do planeta as potências locais teriam mais espaço para manobras (DOMBROWSKI; KELLEHER, 2015). Por uma década após a Guerra Fria, tanto a superpotência restante (Estados Unidos), quanto as outras grandes potências (China, União Europeia, Japão, Rússia) tiveram menos incentivos, e mostraram menos interesse em intervir em assuntos de segurança fora de suas próprias regiões (DOMBROWSKI; KELLEHER, 2015). Esse processo de leitura do Sistema Internacional a partir das regiões começa no final dos anos 60 e início dos anos 70, por consequência do surgimento de novos Estados, em decorrência dos processos de descolonização, levando ao empenho pelo desenvolvimento de uma teoria das regiões (KHANNA, 2008).

Segundo Buzan e Waever (2003), para que um grupo de Estados ou outras entidades sejam qualificados como um CRS, esses devem possuir um grau de interdependência de segurança suficiente tanto para estabelecê-los como um conjunto vinculado entre si quanto para diferenciá-los das regiões de segurança circundantes. Na Teoria dos Complexo Regionais de Segurança, os complexos definem-se como subestruturas do sistema internacional pela intensidade relativa da interdependência de segurança entre um grupo de unidades, e indiferença de segurança entre as unidades/Estados circunvizinhos. No entanto, mesmo

[36] Refere-se a um grupo de Estados cujas preocupações principais de segurança se vinculam tão estreitamente que suas seguranças nacionais não podem ser razoavelmente consideradas separadas umas das outras.

reconhecendo a relevância do sistema internacional, bem como o comportamento das unidades (países do complexo) na dinâmica regional, os autores definem o que chamam de "porosidade das regiões", de forma a descrever que o espaço de um CRS não é compacto, mas em certa medida suscetível ao comportamento/influência de outros agentes na região (BUZAN, WAEVER; 2003).

O CRS é um conceito analítico, no entanto esses Complexos Regionais de Segurança são construídos socialmente, no sentido de que estão contingentes à prática de segurança dos atores. Consequentemente, Buzan e Waever (2003) consideram que um CRS não é uma definição apenas discursiva, que define seus limites territoriais ou se a designação regional dada é aceita na região, como Oriente Médio, por exemplo (BUZAN, WAEVER; 2003). Desta forma, os autores qualificam um CRS de acordo com práticas de securitização dos praticantes, isto é, trata-se, portanto, de um tipo de região muito específica e funcionalmente definida, que pode ou não coincidir com entendimentos mais gerais da região (BUZAN, WAEVER; 2003).

Buzan e Waever (2003) consideram que a ideia de que o poder opera em escala regional é bem conhecida a partir do conceito de equilíbrio regional de poder, que estabelece que potências que não estão diretamente ligadas umas às outras ainda participam da mesma rede de relações. Assim, os CRS podem ser analisados em termos de polaridade, podendo ser unipolares, bipolares, tripolares e, até mesmo, multipolares. Devido a isso, é essencial distinguir as potências regionais das de nível global. Baseados nas ideias de equilíbrio de poder, os autores estabelecem que os Complexos Regionais de Segurança podem ser de dois tipos: padrão ou centrado. No tipo padrão não existe a presença de uma potência global, sendo o poder definido em termos da polaridade regional, tendo uma agenda predominantemente político-militar (BUZAN; WAEVER, 2003, p. 55). Como exemplos de potência regional temos Irã, Iraque, Arábia Saudita, Índia e Paquistão, podendo essa influência variar de unipolar até multipolar. No CRS padrão a unipolaridade significa que a região contém apenas uma potência regional. No caso dos CRS centrados, os autores definem que eles podem ser de três formas: (i) unipolar, quando o polo é uma grande potência; (ii) unipolar, sendo o pólo uma superpotência; (iii) centrado, quando é integrado por instituições, e não por uma potência regional. Contudo, Buzan e Waever (2003) sugerem uma quarta opção, quando um CRS centrado unipolar existe, mas a potência regional não é uma superpotência.

A Teoria do Complexos Regionais de Segurança também contempla a ideia dos chamados subcomplexos regionais de segurança, como um subnível dentro do complexo regional. Um subcomplexo tem essencialmente a mesma definição que os CRS, no entanto está incorporado em um CRS maior. Os subcomplexos representam padrões distintos de

interdependência de segurança que, entretanto, estão contidos em um padrão mais amplo que define o CRS como um todo. Buzan e Waever (2003) utilizam o Oriente Médio como exemplo mais claro, no qual subcomplexos distintos podem ser observados no Levante (Egito, Israel, Jordânia, Líbano, Síria) e no Golfo (Irã, Iraque).

Para Buzan e Waever (2003), o CRS da América do Sul é categorizado como padrão, apresentando dois sub complexos relevantes, o Cone Sul e o Norte-andino, os quais possuem ameaças com fontes distintas e que se juntam à medida que se desenvolvem. Segundo a Teoria dos Complexos Regionais, o continente apresenta questões especiais que são a relação com um vizinho dominante de grande poder e o processo de uma possível divisão de um CRS, que seriam as partes norte e sul da América do Sul. Segundo os autores, existem questões de maior relevância para o futuro da região que passam pelo cerne de cada um dos subcomplexos, que seriam a guerra contra as drogas na Colômbia e o futuro do Mercosul no Cone Sul (BUZAN, WAEVER; 2003).

A relação do continente com os Estados Unidos é marcada pela penetração, não sobreposição, sendo considerado pelos autores como uma potência extrarregional que, no entanto, não molda a região, nem mesmo a regulamenta, pois a América do Sul tem sua própria dinâmica (BUZAN, WAEVER; 2003). Durante o século XX, os EUA tiveram uma atuação focada na América Central e no Caribe, onde intervieram abertamente cerca de 40 vezes, não havendo qualquer intervenção declarada na América do Sul. Entretanto, mesmo que o engajamento estadunidense não seja constante, ele acaba influenciando as dinâmicas regionais de segurança (BUZAN, WAEVER; 2003).

Em relação aos subcomplexos da América do Sul, no do Cone Sul possui relevância a aproximação entre Brasil e Argentina, buscando estabelecer na região um ambiente estável e economicamente desenvolvido. Para Buzan e Waever (2003), essa amizade entre os dois maiores países da região é um elemento chave para a consolidação do subcomplexo, uma vez que é alcançado através da cooperação política e da construção da confiança mútua. Segundo os autores, o fato de o MERCOSUL reunir as duas maiores potências do Cone Sul, estabelece um projeto de desenvolvimento que seria capaz de proteger esse subcomplexo da marginalização do mundo globalizado, além de diminuir à atuação dos Estados Unidos na região (BUZAN; WAEVER, 2003).

Por outro lado, o subcomplexo Norte-andino apresenta evolução diferente da apresentada no Cone Sul, que é classificado pelos autores como uma região de conflitos latentes. Isso se deve à história conflituosa de formação dos países dessa sub-região, bem como à influência do narcotráfico, que acaba colocando essas democracias sob pressão (BUZAN;

WAEVER, 2003). Para os autores, a guerra contra o narcotráfico na Colômbia seria a principal agenda de segurança na América do Sul. Além disso, ela provocaria o enfraquecimento do Estado pela ação de grupos domésticos, muitos com capacidade militar, que acabariam por fazer esse conflito chegar até as fronteiras dos países vizinhos, como Venezuela, Bolívia, Argentina e Brasil. Assim sendo, a securitização do combate às drogas na região através do Plano Colômbia, seria um exemplo da interferência dos Estados Unidos no subcomplexo Norte-andino.

Segundo Pergher (2011), a Colômbia coloca-se como um caso essencial para analisar os dois subcomplexos da América do Sul, pois sua dinâmica de segurança extrapola os países do complexo Norte-andino, mas também os países do Cone Sul, bem como para os efeitos da interferência dos Estados Unidos na região e seu papel na influência da agenda de segurança da América do Sul. Desta forma, essa pesquisa procura nas estratégias cibernéticas nacionais dos países da região a existência de indícios de que a teoria dos CRS pode ser aplicada no continente por meio da existência da perspectiva da securitização cibernética.

2.5 SÍNTESE DO CAPÍTULO

Este capítulo apresentou os conceitos que amparam essa pesquisa, descrevendo o ambiente do ciberespaço, seu funcionamento e os diferentes entendimentos que os países possuem dele. Em seguida, os conceitos das infraestruturas críticas, segurança e defesa cibernéticas foram descritos, além do esclarecimento de inúmeros verbetes sobre a tecnologia da informação e da cibersegurança presentes em notas de rodapé. Por fim, o trabalho elenca os conceitos de securitização e a Teoria dos Complexos regionais presentes na Escola de Copenhague.

Os conceitos ligados à segurança cibernética são fundamentais para o entendimento do próximo capítulo desta pesquisa, que se trata, por vezes, de linguagem técnica relativa à segurança de computadores e sua aplicação à segurança nacional. Já os conhecimentos proporcionados pela Escola de Copenhague auxiliam a pesquisa no entendimento sobre a perspectiva da securitização nos objetivos, princípios, marcos regulatórios, e outras ações dos países para garantir sua proteção no domínio cibernético. O próximo capítulo apresenta os *frameworks*, que são guias geralmente destinados à orientação de países na criação de suas estratégias nacionais de segurança cibernética.

3 ESTUDO DOS FRAMEWORKS

Esse capítulo apresenta uma análise dos *frameworks* estudados neste trabalho, fazendo uma classificação destes em relação à sua securitização, com o objetivo de encontrar neles as soluções securitizadas propostas para combate ao cibercrime. Para isso, foram estudados documentos produzidos por organizações internacionais preocupadas com a temática da segurança cibernética nacional, isso porque muitos países ainda não produziram sequer uma política de segurança cibernética para conduzir suas ações de proteção no ciberespaço. Exemplo disso são os países da América Latina - dos 32 estudados pela Organização dos Estados Americanos (OEA), apenas sete possuem uma estratégia de segurança cibernética ou um plano para proteção das infraestruturas críticas elaborado (ORGANIZATION OF AMERICAN STATES, 2020). Assim sendo, os documentos foram preliminarmente analisados para entender seu objetivo principal (gestão/governança ou militar) e, posteriormente, verificar se o *framework* possui características voltadas à securitização do domínio cibernético.

3.1 METODOLOGIA DE PESQUISA PARA ANÁLISE DOS *FRAMEWORKS*

Os *frameworks* foram estudados segundo as técnicas da Teoria Fundamentada através do software NVivo. Nessa metodologia de pesquisa os dados são analisados visando a construção de teorias "fundamentadas" nos próprios dados (CHARMAZ, 2011). A codificação dos documentos dessa pesquisa ocorreu em três fases progressivas, que conceitualmente foram se aperfeiçoando. Em primeiro lugar, tendo como base a temática da securitização cibernética desenvolvida no Capítulo 2 deste trabalho, foram codificados todos os temas que envolviam a segurança cibernética, como a proteção de infraestruturas críticas, o cibercrime e seus diferentes tipos de delitos, as iniciativas de criação de estruturas, os objetivos, além das iniciativas de gestão e governança descritas nos documentos. Nessa primeira etapa, chamada de codificação aberta, foram criados 152 códigos entre os quatro documentos analisados. Muitos códigos eram comuns aos documentos, como o cibercrime, que aparece em todas as publicações. No entanto, sempre que um novo tema ou ideia foi verificado nos textos, foi feita a sua codificação, fazendo com que novas abordagens da segurança cibernética fossem surgindo.

Finalizada a leitura e análise dos documentos, foi iniciada a codificação Axial, na qual os códigos gerados na codificação aberta foram relacionados em categorias e subcategorias, de forma que os códigos fossem agrupados em temas que os relacionassem. Por exemplo, os temas envolvidos com o crime cibernético, como tipos de delitos, iniciativas de combate, etc., foram agrupados em uma categoria intitulada Combate ao Cibercrime. As iniciativas relacionadas

com a segurança cibernética nacional, como a criação de um marco regulatório ou de um conselho nacional, foram agrupadas em uma categoria voltada para essa temática. Com a reorganização do estudo realizada pela codificação Axial, o número de códigos "raiz" diminuiu para 36, conforme o quadro 3 abaixo. Os subcódigos são resultado do agrupamento de códigos encontrados na Codificação Aberta, que podem ser reunidos em categorias que possam formar um conceito ou, simplesmente, ser agrupados com temas que tenham proximidade conceitual.

Quadro 3 - Resultado da Codificação Axial dos frameworks estudados

CODIFICAÇÃO AXIAL	
CÓDIGOS RAIZ	**SUBCÓDIGOS**
1 Ações defensivas no ciberespaço	1.1 Defesa Cibernética
	1.2 Medidas de proteção técnica
	1.3 Melhorar habilidades
	1.4 Prevenção cibernética
	1.5 Resiliência cibernética
	1.6 Atividades de monitoramento
2 Ações ofensivas no ciberespaço	2.1 Agressão entre Estados
	2.2 Ameaça de ataque Cibernético
3 Ataque cinético proveniente de resposta de ataque cibernético	
4 Combate ao Cibercrime	4.1: Acesso ilegal às informações em computadores, sistemas e redes
	4.2: Ameaças de ataque cibernético
	4.3: Análise conjunta de desafios do cibercrime
	4.4: Ataque DDoS
	4.5: Atribuição de ataques
	4.6: Ciberbullying
	4.7: Cooperação com polícias internacionais
	4.8: Criação de um centro de operações de Seg. cibernética
	4.9: Defacement
	4.10: Desenvolver conhecimento e experiência em cibercrimes
	4.11: Disseminação de malware
	4.12: Espionagem industrial
	4.13: Exploração de crianças na Internet
	4.14: Falsificação

	4.15: Fraude
	4.16: Função policial
	4.17: Interrupção de serviços
	4.18: Pharming
	4.19: Phishing
	4.20: Pirataria
	4.21: Pornografia infantil
	4.22: Proteção do ISP
	4.23: Ransomware
	4.24: Roubo de propriedade intelectual
	4.25: Sabotagem de sistemas
	4.26: Spam
	4.27: Vazamento de dados
	4.28: Vulnerabilidades do Dia Zero
	4.29: Botnet
	4.30: Discurso de ódio
	4.31: Exposição de conteúdo impróprio
	4.32: Extorsão
	4.33: Mineração de bitcoins
5 Conscientização, Treinamento, Educação	5.1 Capacitação técnica acadêmica
	5.2 Criação de uma cultura cibernética
	5.3 Foco na área educacional
	5.4 Provedores devem conscientizar clientes
	5.5 Integração com universidades
	5.6 Realização de fóruns
6 Cooperação Internacional	6.1 Cooperação bilateral
	6.2 Cooperação para investigar e processar crimes cibernéticos
	6.3 Importância da segurança cibernética para as Relações Internacionais
	6.4 Cooperação Regional
	6.5 Cooperação técnica internacional
7 Cooperação Nacional	7.1 Cooperação intersetorial
	7.2 Cooperação intragovernamental
8 Diplomacia cibernética	
9 Direito Internacional	

10 Dissuasão cibernética	
11 Espionagem cibernética	11.1 Perda do crescimento econômico
	11.2 Destruição da economia nacional
	11.3 Roubo de propriedade intelectual comercial
12 Exercícios cibernéticos	
13 Gestão de risco	13.1 Adoção de medidas de recuperação por empresas
	13.2 Foco em infraestruturas críticas
	13.3 Gerenciamento de risco de segurança cibernética
	13.4 Identificar ativos e serviços críticos
14 Gestão de vulnerabilidades	14.1 Recompensa por detecção de vulnerabilidades
15 Governança cibernética	15.1 Gerenciamento de crises
	15.2 Governança na Internet
	15.3 Realização de fóruns de governança cibernética
16 Guerra cibernética	16.1 Capacidade cibernética militar
	16.2 Criação de um comando cibernético militar
17 Importância econômica	17.1 Perda de receita
18 Importância com os valores democráticos	
19 Inteligência e contrainteligência	
20 Liberdade de expressão e direitos humanos	
21 Linguagem cibernética comum	
22 Parceria público-privado	22.1 Cooperação intersetorial
	22.2 Parceria pública-privada para Infraestruturas críticas
	22.3 Parceria para responder a incidentes
23 Pesquisa e desenvolvimento	23.1Criação de centros de pesquisa
24 Plano de recuperação de ataques	
25 Poder nacional	25.1 Poder cibernético nacional
	25.2 Soft Power
26 Promoção de indústria de cibersegurança nacional	
27 Proteção de dados e preservação da privacidade	
28 Proteção das infraestruturas críticas	28.1 Continuidade dos serviços
	28.2 Criação de um centro para proteção da IC nacionais
	28.3 Criação de estratégia de proteção de IC
	28.4 Identificar os proprietários e os serviços críticos

	28.5 Identificar as partes interessadas públicas
	28.6 Proteger as infraestruturas críticas de informação
	28.7 Modernização da infraestrutura
	28.8 Parceria público-privada
	28.9 Avaliar o risco cibernético
	28.10 Uso militar para proteger IC
29 Proteger propriedade intelectual nacional	29.1 Roubo de propriedade intelectual de infraestruturas críticas
30 Relacionamento com cadeia de suprimentos	
31 Resposta a incidentes	31.1 Criação de um CERT nacional
	31.2 Criação de um CERT policial
	31.3 Criação de CERT's setoriais
	31.4 Criação de um CERT para as redes do governo
	31.5 Monitorar atividades
	31.6 Estabelecer limiares legais de atuação
	31.7 Estabelecer mecanismos de notificação de incidentes
	31.8 Ativar um plano de resposta multisetorial
32 Segurança cibernética nacional	32.1Adotar o uso de certificados digitais
	32.2 Adotar segurança no processo de desenvolvimento
	32.3 Conceito de ciberespaço
	32.4 Conhecer e comunicar os atores envolvidos
	32.5 Criação de legislação, regulamentos e normativas
	32.6 Criação de um ambiente de confiança no ciberespaço
	32.7 Coordenação cibernética nacional
	32.7.1 Criação de um conselho nacional de segurança cibernética
	32.7.2 Definir um responsável pela gestão cibernética
	32.8 Definição de requisitos mínimos de segurança da informação
	32.9 Desenvolver políticas nacionais de cibersegurança
	32.10 Estabelecer auditorias de requisitos mínimos de Segurança da informação.
	32.11 Integrar um plano de teste da estratégia de cibersegurança nacional
	32.12 Monitorar a estratégia nacional
	32.13 Pensar em posicionar-se como líder no setor
	32.14 Promover a gestão de identidade
	32.15 Requisitos para uso seguro do 5G
	32.16 Compartilhamento de informações entre os atores

	32.17 Estimular o uso da criptografia
33 Segurança da informação	33.1 Segurança cibernética
	33.2 Segurança de rede
	33.3 Segurança na internet
	33.3.1 Proteger a propriedade intelectual
	33.3.2 Exploração infantil
34 Garantia da Soberania Nacional	34.1 Ameaça à prosperidade
	34.2 Proteção das infraestruturas críticas
35 Terrorismo cibernético	
36 Uso pacífico do ciberespaço	

Fonte: Elaborado pelo autor com dados extraídos com o *software* Nvivo

Por fim, a última etapa da Teoria Fundamentada é a chamada Codificação Seletiva, que tem o objetivo de criar conceitos chave - chamado de *core category* - para que possam ser identificados com o argumento/proposta principal da pesquisa. No entanto, essa dissertação não pretende conceituar todos os componentes necessários para a elaboração de uma estratégia nacional de segurança cibernética, mas, sim, encontrar nos documentos as ações securitizadas de proteção do ciberespaço. Assim, dentre as informações coletadas na pesquisa, a Codificação Seletiva levou em consideração as iniciativas extremas de defesa cibernética, como ações ofensivas, restrição de liberdades, proteção de infraestruturas críticas nacionais e uso da capacidade militar para o ciberespaço - ou seja, qualquer ação que extrapolasse o nível político ou que fosse enquadrada como um tipo especial de política. Isto posto, das 36 categorias provenientes da codificação axial, foram elencadas 12 delas para a etapa da codificação seletiva, pois foram as consideradas inseridas no espectro da securitização.

O quadro 4, abaixo, apresenta esses itens, com a respectiva numeração recebida no Quadro 3, bem como demonstra suas subcategorias e em quais *frameworks* eles podem ser encontrados. A porcentagem apresentada leva em consideração a quantidade de referências securitizadas encontradas nos documentos, ou seja, em relação ao universo de todas as ações codificadas dentro do espectro de securitização. Além disso, cabe informar que uma categoria raiz possui seu próprio número de codificações, independentemente de ser uma raiz, de tal forma que o valor percentual apresentado para ela não é um somatório das suas subcategorias.

Quadro 4 - Codificação Seletiva e as ações securitizadas em cada *framework*

CATEGORIA	DESCRIÇÃO	SUBCATEGORIA	ENISA	ITU	OTAN	NIST	OEA
2: Ações ofensivas no ciberespaço	Possibilidade de operações cibernéticas militares.		-	-	3%	-	-
		2.1 Agressão entre Estado	-	-	-	-	-
		2.2 Ameaças de ataque cibernético	-	-	3%	-	-
3: Ataque cinético através de um ataque cibernético	Fazer uso de um ataque convencional contra outra nação como resposta a um ataque cibernético.		-	-	8%	-	-
4: Combate ao Cibercrime	Criação de capacidade para combater o cibercrime e tipificação encontrada nos documentos.		12%	-	9%	-	-
		4.1: Acesso ilegal às informações em computadores, sistemas e redes	-	-	2%	-	-
		4.2: Ameaças de ataque cibernético	6%	9%	2%	31%	-
		4.3: Análise conjunta de desafios do cibercrime	-	-	-	-	-
		4.4: Ataque DDoS	-	-	-	-	-
		4.5: Atribuição de ataques	-	-	2%	-	-
		4.6: Ciberbullying	-	-	-	-	-
		4.7: Cooperação com polícias internacionais	6%	-	1%	-	-
		4.8: Criação de um centro de operações de Seg. cibernética	6%	-	-	-	-
		4.9: *Defacement*	-	-	-	-	-
		4.10: Desenvolver conhecimento e experiência em cibercrimes	6%	-	-	-	-
		4.11: Disseminação de malware	-	-	1%	-	-

		4.12: Espionagem industrial	-	-	4%	-	-
		4.13: Exploração de crianças na Internet	-	-	-	-	-
		4.14: Falsificação	-	-	-	-	
		4.15: Fraude	-	-	-	-	-
		4.16: Função policial	-	-	-	-	-
		4.17: Interrupção de serviços	-	-	-	-	-
		4.18: Pharming	-	-	-	-	-
		4.19: Phishing	-	-	-	-	-
		4.20: Pirataria	-	-	-	-	-
		4.21: Pornografia infantil	-	-	-	-	-
		4.22: Proteção do ISP	-	-	1%		
		4.23: Ransomware	-	-	-	-	-
		4.24: Roubo de propriedade intelectual	-	-	-	-	47%
		4.25: Sabotagem de sistemas	-	-	-	-	-
		4.26: Spam	-	-	-	-	-
		4.27: Vazamento de dados	-	-	-	-	-
		4.28: Vulnerabilidades do Dia Zero	-	-	1%	-	-
		4.29: Botnet	-	-	-	-	-
		4.30: Discurso de ódio	-	-	-	-	-

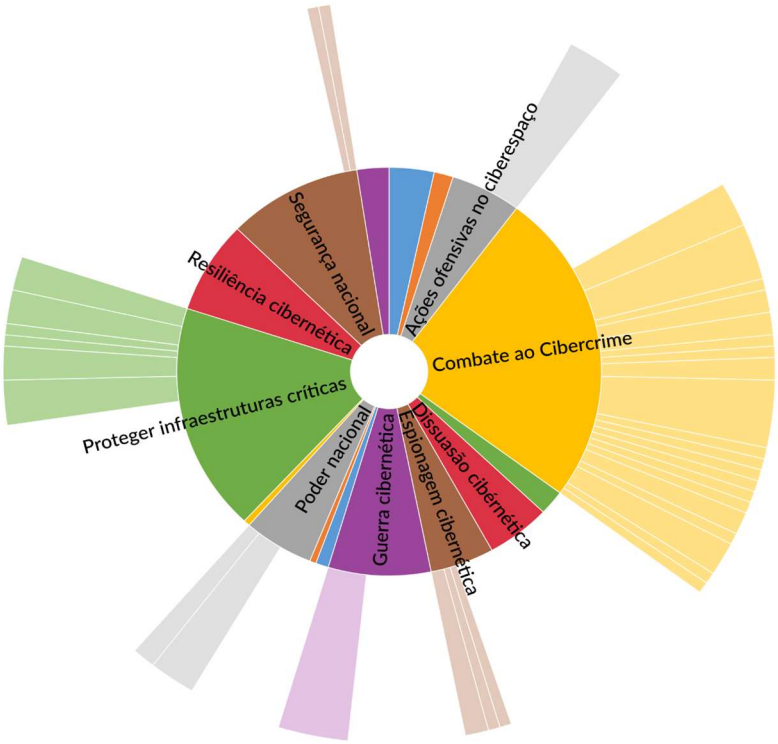
		4.31: Exposição de conteúdo impróprio	-	-	-	-	-
		4.32: Extorsão	-	-	-	-	-
		4.33: Mineração de bitcoins	-	-	-	-	-
10: Dissuasão cibernética	Causar a desistência de uma ação no ciberespaço por medo de uma retaliação extrema, por exemplo, a capacidade de um país retaliar um ataque em um domínio diferente do cibernético.		2%	-	9%	-	21%
11: Espionagem cibernética	Investigar e explorar a estrutura técnica de uma nação, bem como roubar dados ou sabotar sistemas.		-	-	4%	-	-
		11.1: Minar economia nacional	-	-	-	-	-
		11.2: Destruição da economia nacional	-	-	-	-	-
		11.3: Roubo de propriedade intelectual comercial	-	-	-	-	23%
12: Exercícios cibernéticos	Executar exercícios cibernéticos para testar a capacidade de ações ofensivas e defensivas no ciberespaço		24%	26%	2%	-	-
16: Guerra cibernética	Dotar as forças armadas de armas cibernéticas.		-	-	6%	-	-
		16.1: Capacidade militar cibernética			7%	-	-
		16.2: Criação de um comando cibernético	-	-	-	-	-
19: Inteligência e Contrainteligência	Implementar mecanismos de inteligência e contrainteligência cibernéticas		-	-	4%	-	-
25: Poder Nacional	Demonstrar uma força no domínio cibernético para outras nações.		-	-	2%	-	-
		25.1: Poder cibernético nacional	-	-	3%	-	-
28: Proteção das infraestruturas	Utilizar as Forças Armadas para a		26%	30%	7%	69%	9%

críticas	proteção das infraestruturas críticas nacionais.						
		28.10 Uso militar para proteção das IC	-	-	2%	-	-
34: Garantia da soberania nacional	Adotar um discurso de proteção do ciberespaço para proteção da soberania nacional.		8%	35%	12%	-	-
		34.1 Ameaça à prosperidade					
		34.2 Proteção das infraestruturas críticas			2%		
35: Terrorismo cibernético	Atentar para o risco de ações terroristas que possam ser executadas através do domínio cibernético.		4%	-	3%	-	-

Fonte: Elaborado pelo autor com dados extraídos do *software* Nvivo

Conforme demonstrado no quadro 4, grande parte das ações securitizadas são sugeridas pelo *framework* da OTAN, poucas entre os guias da ENISA e do ITU, e nenhuma delas é encontrada nos documentos do NIST e da OEA. Na Figura 3, temos a representação gráfica de todas as ações demonstradas no quadro 4, sendo possível visualizar que o *Combate ao Cibercrime* é a maior categoria encontrada entre todos os *frameworks*, seguido da preocupação com a *Proteção da Infraestruturas Críticas*.

Figura 3 - Representação de todas as ações securitizadas encontradas nos *frameworks*



Fonte: Elaborado pelo autor com dados extraídos do software Nvivo

Em seguida, serão apresentados cada um dos documentos estudados, apresentando-se um breve histórico das organizações que os criaram, sua natureza, bem como os públicos-alvo para os quais os documentos são destinados. Por fim, será apresentado o estudo da Teoria Fundamentada para cada um dos *frameworks* pesquisados, de forma a responder se estão (ou não) próximos de ações securitizadas para proteção do domínio cibernético.

3.2 NIST CYBERSECURITY FRAMEWORK

O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (*National Institute of Standards and Technology* - NIST), foi fundado em 1901 e faz parte do Departamento de Comércio do país, sendo considerado como um dos laboratórios de ciências físicas mais antigos do mundo (THE UNITED STATES, 2017). O Congresso estadunidense estabeleceu o instituto com a missão de desenvolver os EUA na disputa industrial na qual, à época, o país ficava atrás de rivais econômicos como Reino Unido e Alemanha (THE UNITED STATES, 2017).

Publicado em 2014 e atualizado em 2017 e 2018, o *framework* elaborado pelo NIST é um guia sobre como as partes interessadas das organizações (comerciais ou não) e nações podem gerenciar e reduzir o risco de segurança cibernética. O documento possui uma lista de

atividades personalizáveis e específicas das organizações associadas ao gerenciamento de riscos de segurança cibernética, sendo baseado em diretrizes e práticas existentes (NIST, 2018). A versão original do NIST *Cybersecurity Framework* foi voltada para operadoras de infraestrutura crítica, como indústrias químicas, serviços de saúde, água, energia, entre outros. Em 2017, foram aceitos comentários de vários setores da sociedade que permitiram a evolução para uma versão aprimorada (chamada de "1.1"), que foi disponibilizada em 2018, e projetada para empresas e outras organizações para avaliar seus riscos cibernéticos. Segundo o guia,

> Os Estados Unidos dependem de um bom funcionamento confiável por parte da infraestrutura crítica. As ameaças de segurança cibernética exploram o aumento da complexidade e da conectividade de sistemas de infraestrutura críticas, colocando em risco a segurança da nação, da economia, e da saúde e segurança pública. Semelhante aos riscos financeiros e de reputação, o risco de segurança cibernética afeta o resultado final de uma empresa. Isso pode afetar os custos e afetar sua receita. Pode prejudicar a capacidade de uma organização inovar, e de conquistar e manter clientes (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018, p. 1, tradução nossa).[37]

Para melhor tratar desses riscos e fortalecer a resiliência da infraestrutura crítica estadunidense, em 2014 a Lei de Aprimoramento da Segurança Cibernética atualizou o papel do NIST para que ele aprimorasse o desenvolvimento de diretrizes sobre segurança cibernética (UNITED STATES, 2013). Através dessa lei, o Instituto fica responsável por identificar uma abordagem sobre riscos cibernéticos fundamentada no desempenho, incluindo medidas e controles de segurança da informação que possam ser adotados voluntariamente pelos proprietários e operadores de infraestrutura crítica, para ajudá-los a identificar, avaliar e gerenciar os riscos do ciberespaço (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018).

No entanto, o Guia vai além e inclui uma metodologia para proteger a privacidade individual e as liberdades civis quando as organizações de infraestrutura crítica realizam atividades que envolvam segurança cibernética, pois reconhecem que essa proteção desenvolve uma maior confiança pública (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018). O *NIST Cybersecurity Framework* sugere que a ideia de integrar privacidade e segurança cibernética pode beneficiar as organizações ao aumentar a confiança

[37] Em inglês: The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain
customers.

de seus clientes, permitindo um compartilhamento de informações mais padronizado e simplificando as operações que envolvam os trâmites jurídicos (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018).

Para tratar da segurança cibernética, o Guia faz referência a vários padrões, diretrizes e práticas internacionais de Segurança da Informação existentes que se desenvolvem com a tecnologia (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018). Baseando-se nesses padrões, que são gerenciados e atualizados pela própria indústria, as ferramentas criadas no *framework*, bem como as metodologias disponíveis para alcançar os resultados, podem ser ampliadas para além das fronteiras dos Estados Unidos, fazendo com o que o material possa ter caráter global no combate aos riscos cibernéticos. O uso de padrões de segurança existentes viabiliza que o *framework* possa ser utilizado por países de economias emergentes ou mais desenvolvidas, fazendo com que seja possível atender às necessidades de cada nação ou mercado (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018).

Embora o Guia do NIST tenha sido desenvolvido para aperfeiçoar o gerenciamento do risco cibernético de infraestruturas críticas, ele pode ser utilizado em qualquer organização em diferentes setores da economia ou da sociedade. Seu objetivo é ser útil para órgãos governamentais, iniciativa privada e organizações sem fins lucrativos, independentemente de sua área de atuação ou tamanho. A taxonomia[38] comum de padrões, diretrizes e práticas fornecidas não são específicas a nenhum país, fazendo com que organizações fora dos Estados Unidos também possam usar o Guia para fortalecer seus próprios esforços de segurança cibernética. Com isso, a ideia do *framework* é contribuir para uma linguagem comum para cooperação internacional em segurança cibernética para infraestruturas críticas (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018)

A abordagem utilizada no Guia é composta por três componentes que reforçam a necessidade da conexão entre os indicadores de negócio/missão e as atividades de segurança cibernética. Esses componentes são: a Estrutura Básica, os Níveis de Implementação e as Avaliações da Estrutura. A Estrutura Básica apresenta padrões, diretrizes e práticas da indústria de maneira a permitir a comunicação das atividades e dos resultados da segurança cibernética em toda a organização, desde o nível executivo até o nível de implementação ou operacional. A Estrutura Básica consiste em um conjunto de cinco funções simultâneas e contínuas — identificar, proteger, detectar, responder e recuperar. Quando analisadas em conjunto, essas

[38] Refere-se a identificação e classificação de ameaças e vulnerabilidades do ciberespaço, bem como das contramedidas para mitigar ou eliminar esse risco.

funções fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento do risco de segurança cibernética de uma organização (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018)

Em seguida, os Níveis de Implementação da Estrutura apresentam um contexto sobre como uma organização lida com o risco de segurança cibernética e os processos envolvidos para gerenciar esse risco. Esses níveis classificam as práticas de uma organização de Parcial (nível 1) a Adaptável (nível 4), refletindo uma progressão de respostas informais e reativas a abordagens que são ágeis e baseadas no conhecimento dos riscos (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018). Por fim, a Avaliação da Estrutura representa os resultados com base nas necessidades de negócio que determinada organização escolheu a partir das categorias e subcategorias da Estrutura Básica. Assim sendo, as avaliações podem ser usadas para identificar oportunidades de aprimoramento da segurança cibernética, por meio da comparação do cenário atual com uma situação desejada (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018)

3.2.1 Análise do NIST Cybersecurity Framework

Submetido à leitura e análise através da Teoria Fundamentada, o *framework* do NIST não se encaixa nas ações securitizadas levantadas por essa pesquisa, como apresentado no quadro 5, abaixo. A solução é focada em ações que podem ser conduzidas dentro do espectro político normal, como o uso de padrões internacionais, governança, conscientização e cultura em cibersegurança, gestão de riscos, gestão de vulnerabilidades e a criação de arcabouço legal para tratamento do crime cibernético, entre outros. Com a ideia de utilizar padrões de segurança conhecidos do mercado, o *framework* do NIST pode tanto ser utilizado por países, como por organizações diversas (comerciais ou não-comerciais).

Desta forma, o quadro 5 apresenta o código “4.2 Ameaças de Ataque Cibernético”, que destaca o receio com ataques através do ciberespaço que possam inviabilizar a economia, infraestruturas críticas, segurança pública e saúde da nação (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018)No entanto, essa pesquisa inseriu todas as informações que se referem ao cibercrime (categoria 4: Combate ao Cibercrime), de forma que se possa visualizar os tipos de delitos digitais mais comuns em todos os documentos. No entanto, o framework do NIST faz referência a apenas ao item *Ameaças de ataque cibernético* codificado no trabalho.

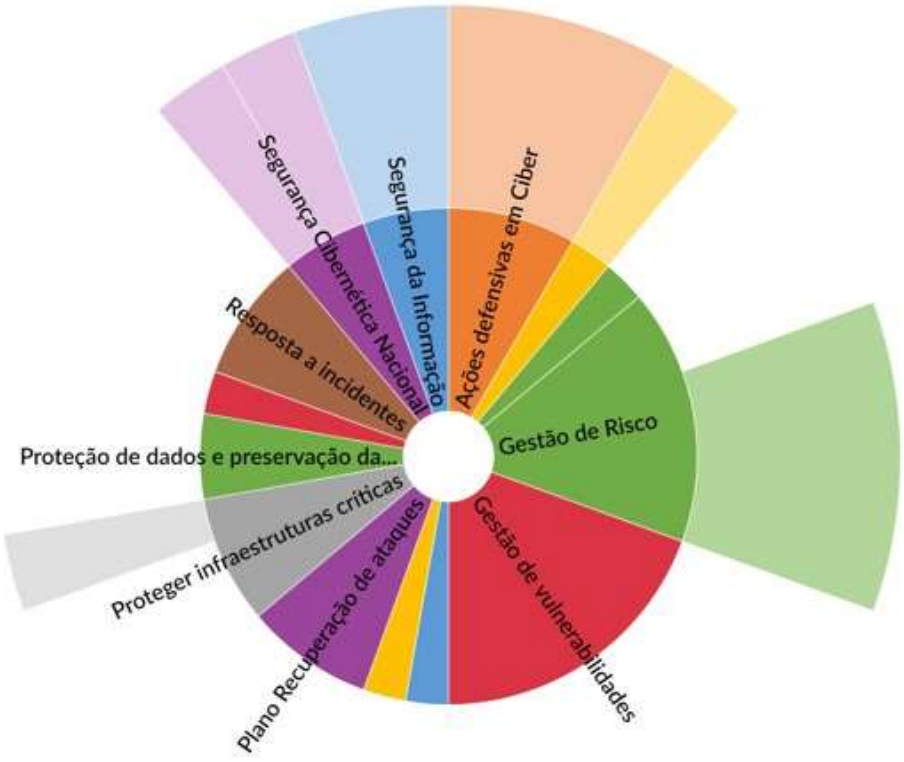
Quadro 5 - Codificações mais próximas da securitização do framework do NIST

AÇÕES SECURITIZADAS	NIST
4: Combate ao Cibercrime	0%
4.2: Ameaças de ataque cibernético	31%

Fonte: Elaborado pelo autor com dados da ferramenta Nvivo

Assim sendo, a natureza do *framework* do NIST pode explicar a inexistência de ações securitizadas para propor suas ações de proteção do ciberespaço, isso devido à possibilidade de ser utilizado tanto por nações como por organizações civis de diferentes tipos através de padronizações de segurança da informação elaboradas por organizações civis. Dessa forma, pode-se verificar nas figuras 4 e 5 que o NIST tem maior preocupação com a gestão de riscos, gestão de vulnerabilidades, resposta a incidentes, recuperação de ataques e, principalmente, proteção das infraestruturas críticas, ou seja, está mais voltado para ações de gestão. Mesmo assim, não esquece os países, inserindo itens que podem ser utilizados para que as nações possam elaborar projetos para melhorar sua segurança cibernética nacional.

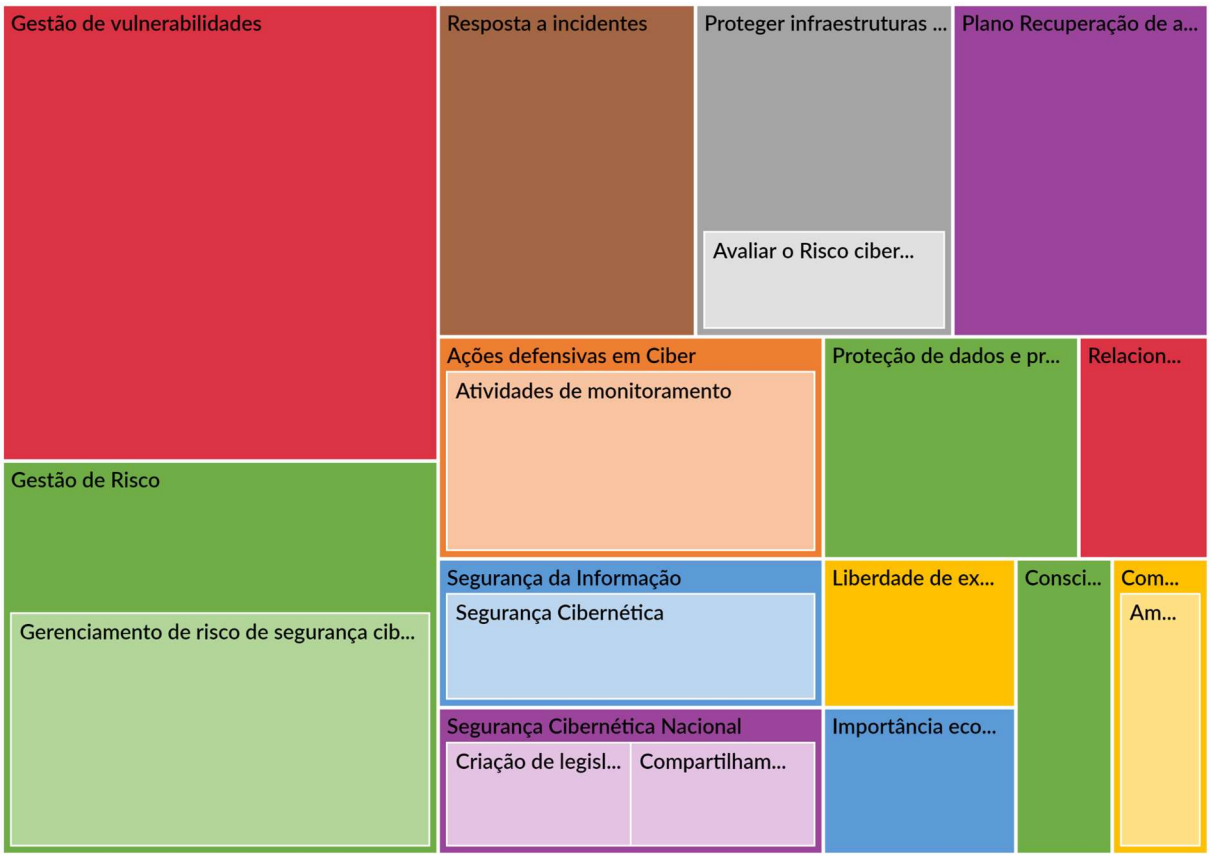
Figura 4 - Representação gráfica das ações de cibersegurança do *framework* do NIST



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Outra maneira de representar as ações de cibersegurança propostas pelo *framework* do NIST pode ser vista na Figura 5. No gráfico é possível visualizar alguns dos subcódigos contidos nas ações raiz, além de novos códigos como *Liberdade de Expressão, Direitos Humanos*, *Importância Econômica*, *Conscientização, Treinamento e Educação*, entre outros.

Figura 5 - Representação das ações do NIST em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

3.3 NATIONAL CYBER SECURITY STRATEGIES: AN IMPLEMENTATION GUIDE (ENISA)

A Agência da União Europeia para a Segurança da Rede e da Informação (ENISA) é um centro de conhecimento em rede e segurança da informação para a União Europeia, seus Estados-Membros, o setor privado e os cidadãos europeus. A ENISA trabalha com esses grupos para desenvolver recomendações sobre boas práticas em segurança da informação, auxiliando os Estados-Membros da UE na implementação de legislação relevante, bem como trabalha para melhorar a resiliência da infraestrutura e das redes de informação críticas da Europa. Desta forma, busca aprimorar a expertise em segurança cibernética existente nos Estados-Membros da UE, apoiando o desenvolvimento de comunidades transversais e fronteiriças comprometidas

em melhorar a segurança do espaço cibernético em toda a União Europeia (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2014).

Assim, tentando construir uma resposta às ameaças cibernéticas que eram apresentadas pelos Estados Unidos em sua estratégia cibernética de 2003, a ENISA elaborou, no início de 2012, um documento intitulado *An Evaluation Framework for NCSS*, com o objetivo de identificar os elementos de segurança cibernética mais comuns nas estratégias nacionais de segurança cibernética dos países da União Europeia. Em dezembro do mesmo ano, a Agência desenvolveu um guia chamado *National Cybersecurity Strategies: An Implementation Guide*, com a proposta de identificar os elementos e práticas mais comuns e recorrentes das estratégias de segurança cibernética de países do bloco europeu, bem como fora dele, a fim de determinar a relevância das medidas implementadas por essas nações (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2012).

Nesse contexto, o *National Cybersecurity Strategies* tem objetivo de apresentar em termos de estrutura e conteúdo as medidas mais relevantes para que os países possam elaborar (ou atualizar) suas estratégias nacionais de segurança cibernética. Sendo assim, o *framework* elaborado pela ENISA identifica um conjunto de ações concretas que, se implementadas, levarão a uma estratégia de segurança cibernética nacional coerente e holística (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2012). Diferente do *framework* do NIST, que é voltado para diferentes públicos, a ENISA desenvolveu esse guia voltado para os formuladores de políticas dos Estados-Membros interessados em gerenciar os processos de segurança cibernética em seus países (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2012).

O Guia é focado em ideias para a construção de uma estratégia nacional de segurança cibernética, acreditando que essa tarefa é um esforço desafiador que precisa de coordenação de diferentes atores nacionais, do setor público e privado. Embora existam muitas - e consideravelmente diferentes - definições de estratégia de segurança cibernética para países, o material constrói um conjunto de ações que têm por finalidade ajudar os governos a gerenciar os esforços em todas as partes envolvidas a fim de enfrentar os riscos cibernéticos em nível nacional. Desta forma, a ENISA destaca um conjunto de vinte ações concretas para os formuladores de políticas, que são: 1. definir a visão, o escopo e os objetivos; 2. seguir uma abordagem nacional de avaliação de risco; 3. avaliar as legislações existentes; 4. desenvolver um programa de governança cibernética; 5. identificar e engajar as partes interessadas; 6. estabelecer informações confiáveis e mecanismos para compartilhá-las; 7. desenvolver planos de contingência de segurança cibernética; 8. organizar exercícios de segurança cibernética; 9. estabelecer requisitos mínimos de segurança para organizações; 10. estabelecer mecanismos de

notificação de incidentes; 11. conscientizar os cidadãos; 12. fomentar P&D; 13. fortalecer programas de treinamento e educação; 14. estabelecer uma capacidade para resposta a incidentes; 15. abordar os crimes cibernéticos; 16. engajar-se na cooperação internacional em segurança cibernética; 17. estabelecer uma parceria público-privada; 18. equilibrar segurança com privacidade; 19. avaliar os planos constantemente; 20. ajustar a estratégia nacional de segurança cibernética (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2012).

No que tange os crimes cibernéticos, o Guia destaca que o combate depende da colaboração de muitos atores e comunidades para que uma resposta concertada e coordenada com as partes interessadas possa ser dada. Assim sendo, são sugeridas algumas tarefas que incluem:

> 1 Adaptar a legislação necessária e ratificar os tratados internacionais existentes; 2 Criar unidades nacionais especializadas em crimes cibernéticos (autoridades policiais e judiciais); 3 Garantir treinamento contínuo e especializado para os funcionários da polícia e da autoridade judiciária em forense digital; 4 Desenvolver conhecimento e experiência em ameaças e vulnerabilidades emergentes relacionadas ao crime cibernético, mas também em métodos de ataque por meio do compartilhamento de informações em nível nacional e internacional; 5 Criar um conjunto harmonizado de regras para a manutenção de registros policiais e ferramentas adequadas para análise estatística de crimes cibernéticos; 6 Estabelecer fóruns para promover a cooperação entre os vários atores (por exemplo, CERTs e comunidades de inteligência); 7 Incentivar a ação direta da indústria contra crimes relacionados a computadores; 8 Estabelecer cooperação com as principais instituições acadêmicas e de P&D em novas técnicas de forense digital; 9 Estabelecer cooperação entre as partes interessadas do setor público e privado para identificar e responder rapidamente às questões relacionadas ao crime cibernético (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2012, p. 25-26, tradução nossa).[39]

3.3.1 Análise do National Cyber Security Strategies: An Implementation Guide (ENISA)

No âmbito da perspectiva de securitização adotada por esta pesquisa, o estudo do *framework* encontrou as seguintes ações: combate ao cibercrime, execução de exercícios cibernéticos, o uso da dissuasão cibernética, o chamado para a garantia da soberania nacional e a preocupação com a possibilidade do terrorismo através do domínio cibernético. O quadro 6 exibe as ações securitizadas encontradas na pesquisa e que se encaixam com a documentação

[39] Em inglês: - Adapt the required legislation and ratify existing international treaties. - Create specialised national cyber crime units (law enforcement and judicial authorities). - Ensure continuous and specialised training for police and judicial authority staff (e.g. on digital forensics). - Develop knowledge and expertise on emerging cyber crime-related threats and vulnerabilities but also attack methods through information sharing at national and international level. - Create a harmonised set of rules for police and judicial record-keeping and appropriate tools for statistical analysis of computer crime. - Establish forums to foster cooperation between the various players (e.g. CERTs and intelligence communities). - Encourage direct action by industry against computer-related crime. - Establish cooperation with leading academic and R&D institutions on new digital forensic techniques. - Establish cooperation between public and private sector stakeholders to quickly identify and respond to cyber crime related issues.

sugerida pela ENISA para proteção do ciberespaço. No que se refere ao combate ao cibercrime, pode-se verificar uma maior preocupação com a criação de centros para tratamento de crimes digitais, o desenvolvimento de capacidades e da cooperação com polícias de outros países.

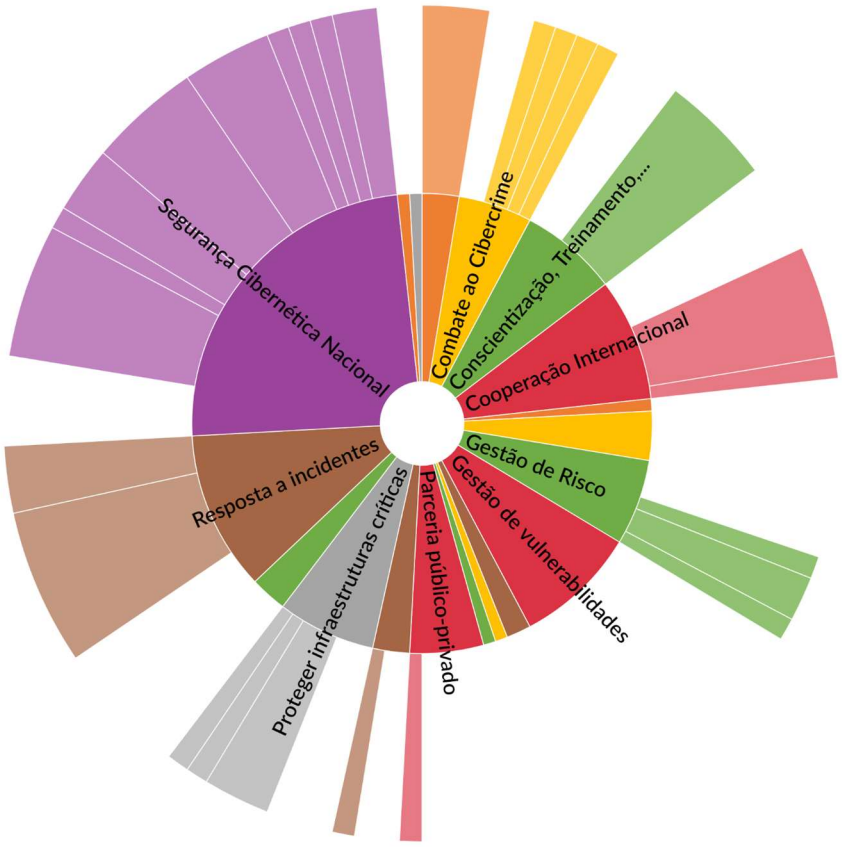
Quadro 6 - Codificação das ações securitizadas no *framework* da ENISA

CATEGORIAS E SUBCATEGORIAS	ENISA
4: **Combate ao Cibercrime**	12%
4.2: Ameaças de ataque cibernético	6%
4.7: Cooperação com polícias internacionais	6%
4.8: Criação de um centro de operações de Seg. cibernética	6%
4.10: Desenvolver conhecimento e experiência em cibercrimes	6%
10: Dissuasão cibernética	2%
12: Exercícios cibernéticos	24%
34: Garantia da soberania nacional	8%
35: Terrorismo cibernético	4%

Fonte: Elaborado pelo autor com dados da ferramenta Nvivo

A análise do *framework* da ENISA demonstra uma maior atenção dedicada a ações de proteção cibernética dentro do espectro político, como o fortalecimento da resiliência cibernética, o gerenciamento de riscos, a gestão de vulnerabilidades, a pesquisa e o desenvolvimento para o ciberespaço, a criação de marcos legais, a cooperação internacional e regional, o estabelecimento de um plano de contingência nacional, o desenvolvimento de conhecimento e experiência para combate ao cibercrime, além da proteção dos dados dos cidadãos e da preservação da privacidade, entre outros. A ENISA indica esse documento para os formuladores de políticas nacionais, ou seja, suas ações são voltadas para países. Dessa forma, pode-se notar uma maior quantidade de ações securitizadas em relação ao *framework* do NIST, que não possui itens como cooperação internacional e dissuasão cibernética, além de não dar nenhuma ênfase ao discurso da segurança nacional, necessário para a perspectiva da securitização. A figura 6 exibe a codificação resultante do estudo do documento proposto pela ENISA

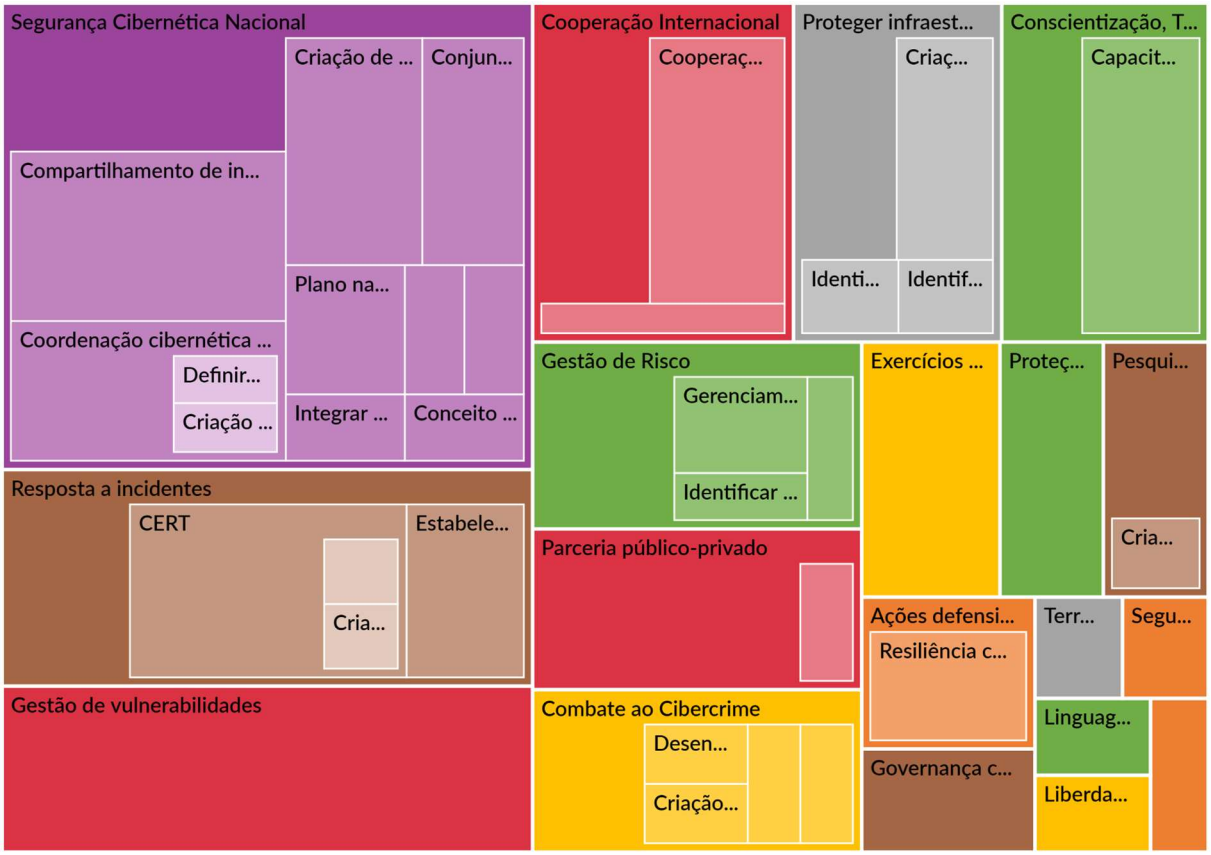
Figura 6 - Representação gráfica das ações de cibersegurança do *framework* da ENISA



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Outra forma de representar as ações de cibersegurança propostas pelo framework da ENISA pode ser vista na Figura 7. No gráfico, podem ser vistos mais códigos e subcódigos oriundos dessa pesquisa, com destaque para a *Linguagem Cibernética Comum* e a *Parceria público-privada*.

Figura 7 - Representação das ações da ENISA em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

3.4 OTAN - NATIONAL CYBER SECURITY FRAMEWORK MANUAL

O *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) foi estabelecido por iniciativa da Estônia juntamente com seis outras nações - Alemanha, Itália, Letônia, Lituânia, Eslováquia e Espanha - em maio de 2008 (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2008). A OTAN decidiu conceder *status* de organização militar ao Centro em outubro do mesmo ano, ainda que a Estônia houvesse proposto o conceito de Centro de Excelência em Defesa Cibernética à Organização em 2004, após aderir à aliança. Embora esse conceito de defesa cibernética estivesse na pauta da OTAN desde 2006, foram os ataques cibernéticos com motivação política contra a Estônia, em 2007, que serviram de alerta para outras nações e para a Aliança, alertando a todos sobre a crescente relevância de ameaças potenciais no domínio cibernético (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2008). Em 2009, o CCDCOE realizou sua primeira conferência de segurança cibernética, com foco em aspectos jurídicos, tecnológicos e sobre conflitos cibernéticos. Em 2010, o CCDCOE criou a Conferência Anual sobre Conflito Cibernético (CyCon), transformando o evento em uma referência para os profissionais de segurança cibernética, por

aderir aos mais altos padrões de pesquisa acadêmica (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2008).

Desde 2010, o Centro organiza anualmente o *Locked Shields*, que é considerado o maior e mais complexo exercício internacional de defesa cibernética do mundo, tendo a finalidade de simular toda a complexidade de um grande incidente cibernético, com o intuito de defender sistemas regulares de TI, militares e de infraestrutura crítica, fazendo com que os especialistas em segurança cibernética possam praticar a tomada de decisões estratégicas, técnicas, jurídicas e de comunicação com a mídia (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2008). Outra realização de pesquisa do CCDCOE reconhecida internacionalmente foi a elaboração do Manual de Tallinn, lançado em 2009, que envolveu especialistas do Centro, acadêmicos jurídicos de renome internacional de várias nações e consultores jurídicos de quase 50 Estados, versando sobre a aplicabilidade do Direito internacional na resolução de ciberconflitos (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2008).

Em 2017, foi lançado o Manual de Tallin 2.0 sobre o Direito Internacional Aplicável às Operações Cibernéticas, ampliando a primeira edição com uma análise jurídica dos incidentes cibernéticos mais comuns sofridos pelos Estados e que estão abaixo dos limiares do uso da força ou do conflito armado. Esse Manual é considerado a análise mais abrangente sobre como o direito internacional existente se aplica ao ciberespaço (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2017). A partir de 2018, o CCDCOE tornou-se responsável por identificar e coordenar as soluções de educação e treinamento em defesa cibernética para todos os órgãos da OTAN, devido à garantia de qualidade pela contribuição à educação e formação em segurança cibernética para a Aliança (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2008).

Uma das possíveis razões para essa confiança junto à OTAN pode ser a intensa publicação de artigos relativos à segurança cibernética realizada pelo CCDCOE. Além de pesquisar sobre as interações das inovações tecnológicas para a proteção do ciberespaço, fomenta o debate sobre a segurança e defesa cibernética dos países, através da publicação de avaliações sobre as estratégias nacionais de segurança cibernética de diferentes nações. Entre essas publicações está o *National Cyber Security Framework Manual*, que deixa claro que não se pretende definir o termo cibersegurança nacional, uma vez que ele é cada vez mais usado em discussões políticas, e sim fornecer estruturas teóricas com informações básicas e detalhadas para que sejam compreendidas as diferentes facetas da segurança cibernética nacional, de acordo com os diferentes níveis de formulação de políticas públicas, que são os níveis de

governo, político, estratégico, operacional e tático (KLIMBURG, 2012).

Nesse contexto, o Manual assume que a segurança cibernética deve desempenhar um papel relevante no que tange a formulação de políticas públicas de segurança. Considerando que desde o fim da Guerra Fria, uma série de novas ameaças e fatores de risco precisaram ser levadas em conta pelos formuladores de políticas, sendo a segurança cibernética apenas uma dessas novas questões a serem pensadas. No entanto, segundo Klimburg (2012), há uma mudança crescente no sentido de ver a segurança cibernética como um dos mais importantes desses novos desafios. Além disso, o Manual avalia os elementos-chave da segurança cibernética dentro da segurança nacional, descrevendo uma série de atividades ofensivas e defensivas no ciberespaço, bem como a variedade de atores envolvidos nessas atividades e as tensões existentes entre instituições sob a perspectiva de desenvolvimento de objetivos estratégicos para atender a um requisito específico de segurança nacional (KLIMBURG, 2012).

No contexto geral da discussão da segurança cibernética nacional, o Manual destaca que o tema pode ser abordado em diferentes áreas, que são divididas em cinco perspectivas distintas, em que cada uma poderia ser tratada por diferentes departamentos governamentais. Segundo o Manual, cada perspectiva possui sua própria ênfase e até mesmo seu próprio léxico, no entanto considera que todas elas são facetas diferentes do mesmo problema, sendo elas: *ciber* militar, atuação contra o crime cibernético, inteligência e contrainteligência, proteção da infraestrutura crítica e gestão de crise nacionais, diplomacia cibernética e governança da internet (KLIMBURG, 2012).

No que se refere ao tema desta pesquisa, o Manual cita que as atividades do cibercrime podem incluir uma ampla gama de atividades que afetam diretamente os indivíduos (como roubo de identidade) e corporações (por exemplo, roubo de propriedade intelectual) (KLIMBURG, 2012). No entanto, o mais significativo e preocupante para a segurança nacional seria a capacidade dos atacantes conseguirem executar ataques de qualquer lugar do planeta. É nesse contexto que o cibercrime interage com as atividades cibernéticas militares, como no caso da proteção das redes de dados. Outra interação importante da perspectiva do cibercrime envolveria a proteção das infraestruturas críticas, devido aos riscos cibernéticos intrínsecos aos provedores de serviços públicos, de finanças ou de telecomunicações (KLIMBURG, 2012).

Abordando ações mais diretas, para o Manual o combate ao crime cibernético compreende um amplo conjunto de organizações, sendo que, nos níveis político e estratégico, um Ministério da Justiça deveria estar envolvido no desenvolvimento e manutenção da legislação sobre segurança cibernética nacional, e até mesmo internacional (KLIMBURG, 2012). Nessa mesma linha, também sugere a existência de um Ministério do Interior, que ficaria

responsável pela administração dos policiais. No entanto, de acordo com o Manual algumas dessas capacidades poderiam ser delegadas em um nível de governo local (provincial) e não ser apenas de responsabilidade do governo federal. Além disso, a prevenção do crime cibernético é vista como uma questão multifacetada, do ponto de vista econômico, sendo sugerida a criação de um ministério de assuntos econômicos responsável por gerar a conscientização sobre segurança cibernética no nível operacional, assim como programas de desenvolvimento contra o crime cibernético (KLIMBURG, 2012).

Analisando a perspectiva da atuação do Governo, para o Manual, a segurança do Estado e a prevenção do crime cibernético são questões organizacionais em todos os departamentos e agências governamentais (KLIMBURG, 2012). Sugere que as nações atribuam a um gestor essa responsabilidade estratégica de desenvolver, manter e monitorar as políticas estatais de informação e segurança cibernética. Do ponto de vista do fornecimento seguro de serviços ao público em geral, as organizações de serviços não governamentais, como provedores de Internet (ISP), deveriam atuar ativamente contra a disseminação de *malware* e outras atividades maliciosas no ciberespaço (KLIMBURG, 2012). Para isso ocorrer, poderiam ser construídos arranjos público-privados, como o Código de Prática de ISP e a identificação de sistemas que foram comprometidos, que são iniciativas existentes, por exemplo, na Austrália (AUSTRALIAN GOVERNMENT, 1992).

No nível operacional/tático, o Manual sugere a criação de uma função policial específica para investigar, prender e processar os cibercriminosos. Essa função se estenderia aos elementos de preparação (treinamento e exercícios), resposta e recuperação (KLIMBURG, 2012). Com base nisso, o combate ao cibercrime precisaria de uma área de conhecimento especial na polícia federal/nacional e nas forças policiais locais, necessitando ainda de uma de rede de troca de informações com forças policiais estrangeiras, seja com base na colaboração bilateral, seja através das unidades de cibercriminalidade de alta tecnologia de organizações policiais internacionais, como a Europol e a Interpol (KLIMBURG, 2012). Além disso, para ser mais eficaz, as organizações policiais poderiam se vincular aos CERTs nacionais.

3.4.1 Análise do National Cyber Security Framework Manual (OTAN)

O documento da OTAN possui praticamente todas as ações securitizadas sugeridas nesta pesquisa, sendo o *framework* elaborado pela Organização um dos mais completos guias para a elaboração de estratégias de segurança cibernética nacionais. Isso se dá porque ele dispõe de uma série de sugestões para a implementação de uma estratégia nacional de segurança

cibernética, sem a necessidade de que sejam seguidas todas as ações sugeridas, ou seja, os países podem utilizar aquilo que está ao alcance de seus recursos. Por ser elaborado e validado por uma organização militar, o *framework* caminha para uma maior quantidade de ações militarizadas, também possuindo, todavia, instruções sobre gestão de riscos, governança, criação de um marco legal para o cibercrime e proteção da economia, entre outros.

No que tange os objetivos dessa pesquisa, o *framework* da OTAN é o que apresenta a maior quantidade de sugestões fora do espectro político para a implantação de uma segurança cibernética nacional. Assim como o documento da ENISA, existe a preocupação com a questão do terrorismo cibernético. Ademais, a importância de uma capacidade cibernética militar, bem como de habilidades de inteligência e dissuasão, é relevante nesse modelo. A proteção das infraestruturas críticas também recebe grande atenção, inclusive com a sugestão de que possa ser realizada pelos militares. Dessa forma, se trata de um documento direcionado para países, principalmente pela importância dada às questões do discurso de soberania nacional - tema relevante para a temática da securitização - além de citar a possibilidade de retaliação convencional para ataques cibernéticos. O quadro 7 exibe as ações securitizadas encontradas na pesquisa, sendo possível notar uma maior quantidade de codificações relativas ao combate ao cibercrime.

Quadro 7 - Codificação das ações securitizadas no *framework* da OTAN

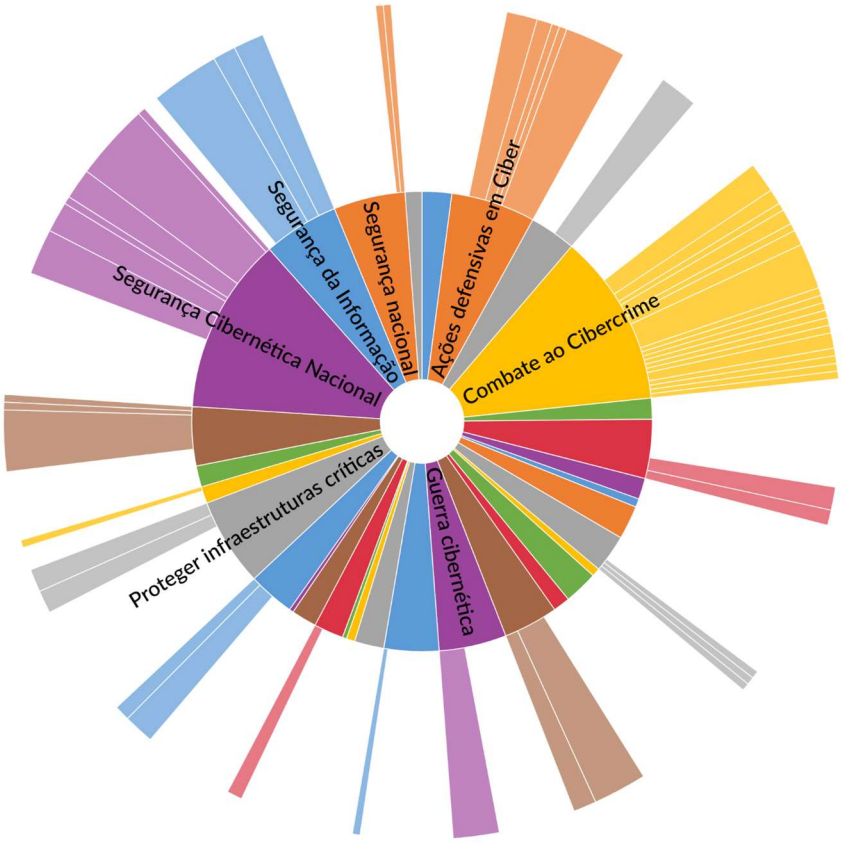
CATEGORIAS E SUBCATEGORIAS	OTAN
2: Ações ofensivas no ciberespaço	3%
2.2: Ataque Cibernético	3%
3: Ataque cinético através de um ataque cibernético	8%
4: Combate ao Cibercrime	9%
4.1: Acesso ilegal às informações em computadores, sistemas e redes	2%
4.2: Ameaças de ataque cibernético	2%
4.5: Atribuição de ataques	2%
4.7: Cooperação com polícias internacionais	1%
4.11: Disseminação de malware	1%
4.12: Espionagem industrial	4%
4.22: Proteção do ISP	1%
4.28: Vulnerabilidades do Dia Zero	1%

10: Dissuasão cibernética	9%
11: Espionagem cibernética	4%
12: Exercícios cibernéticos	1%
16: Guerra cibernética	6%
16.1: Capacidade militar cibernética	7%
19: Inteligência e Contrainteligência	4%
25: Poder nacional	2%
25.1: Poder cibernético nacional	3%
28: Proteger infraestruturas críticas	7%
28.10: Uso militar para proteção de IC	2%
34: Garantia da soberania nacional	12%
34.1: Proteção das infraestruturas críticas	2%
35: Terrorismo cibernético	3%

Fonte: Elaborado pelo autor com dados extraídos da ferramenta Nvivo.

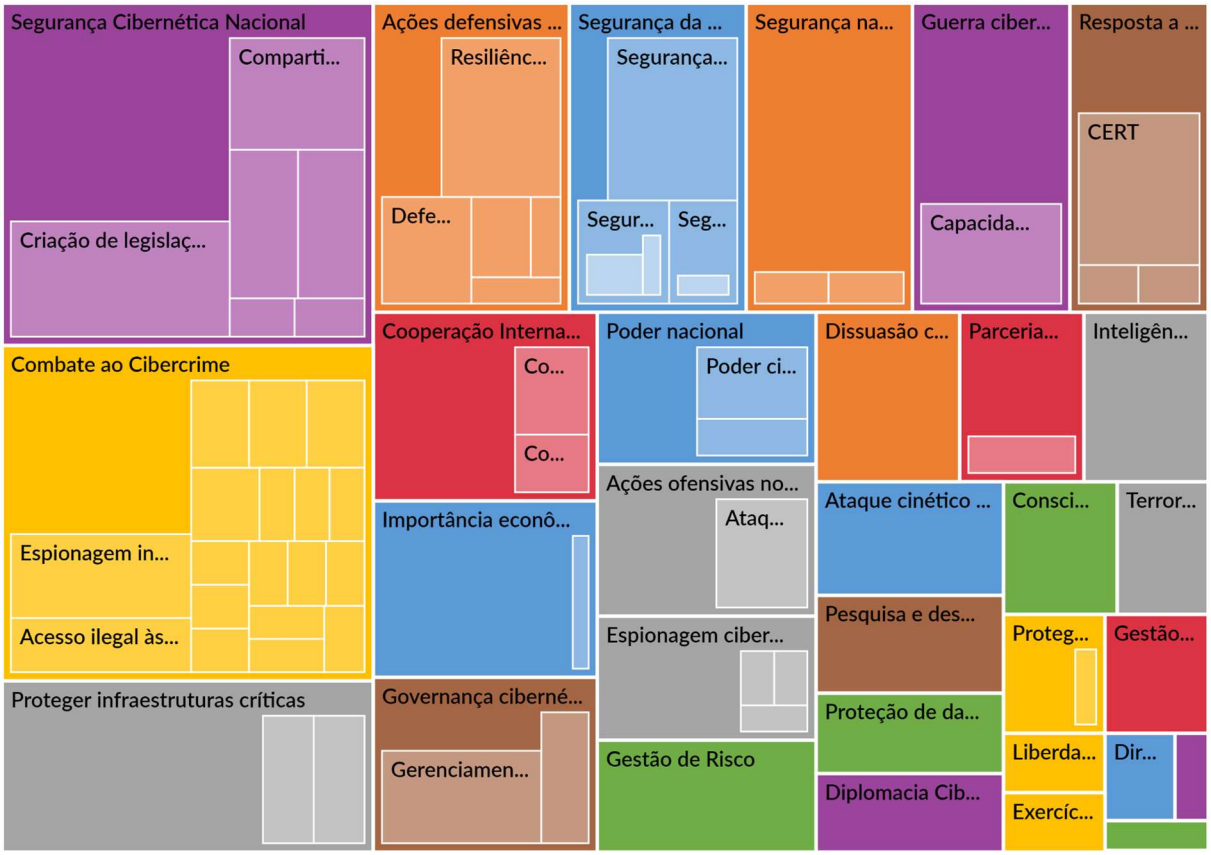
Apesar de entender a importância da gestão de riscos e da governança como ferramentas de proteção do ciberespaço, esses ocupam um lugar menor no *framework* da OTAN, como pode ser visto na Figura 8. Além disso, pela primeira vez no trabalho encontramos a preocupação com o embate entre países, que nesta pesquisa está contido no código *Guerra Cibernética*, bem como uma relevância para assuntos do campo da *Segurança da Informação*, que envolvem a segurança cibernética, de redes e da internet. Na Figura 9 temos uma representação expandida das codificações do *framework* da OTAN, sendo possível observar códigos que ainda não haviam sido apresentados na pesquisa, como a *Diplomacia Cibernética* e a *Espionagem Cibernética*.

Figura 8 - Representação gráfica das ações de cibersegurança do *framework* da OTAN



Fonte: Elaborado pelo autor por meio da ferramenta Nvivo

Figura 9 - Representação das ações da OTAN em formato de Mapa de Árvore



Fonte: Elaborado pelo autor por meio da ferramenta Nvivo

3.5 GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY: STRATEGIC ENGAGEMENT IN CYBERSECURITY (ITU)

A *International Telecommunication Union* (ITU) foi fundada em 1865 para facilitar a conectividade internacional em redes de comunicação, trabalhando para estabelecer padrões técnicos e regular as ondas de rádio e telecomunicações internacionais, garantindo os arranjos de interconexão de redes e tecnologias entre todos os países, permitindo, por exemplo, ligações de telefone internacionais (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Atualmente, é uma das agências especializadas das Organizações das Nações Unidas (ONU), e também trabalha para melhorar o acesso à tecnologia da informação para comunidades em todo o mundo. A ITU é composta por todos os 193 países membros da ONU e por mais de 700 entidades do setor privado e acadêmico (INTERNATIONAL TELECOMMUNICATION UNION, 2019).

Os padrões internacionais produzidos pela ITU são denominados como Recomendações (com R maiúsculo para diferenciar do significado comum da palavra recomendação). Em sua

organização, a ITU é composta por três setores, radiocomunicações, desenvolvimento e normatização (INTERNATIONAL TELECOMMUNICATION UNION, 2019) cada um possuindo um grupo consultivo e uma comissão de estudos, que gerencia um aspecto diferente dos assuntos tratados pelo ITU. Entre as responsabilidades desses setores estão a gestão do espectro de radiofrequência internacional e dos recursos de órbita de satélite, mediante a elaboração de normas para o uso eficaz das radiofrequências (INTERNATIONAL TELECOMMUNICATION UNION, 2019). Além disso, tem a responsabilidade de ajudar a difundir o acesso equitativo, sustentável e barato à infraestrutura e aos serviços de tecnologia de informação e comunicação, com a missão de tentar garantir o direito à comunicação a todos os habitantes do planeta (INTERNATIONAL TELECOMMUNICATION UNION, 2019). A partir do diálogo com o setor industrial, também é responsável pela elaboração de normas consensuais sobre tecnologia que garantam o funcionamento, a interoperabilidade e a integração dos sistemas de comunicação em todo mundo com a finalidade de facilitar o acesso das indústrias aos diferentes mercados de cada país (INTERNATIONAL TELECOMMUNICATION UNION, 2019).

Nesse contexto, em 2018, o ITU elaborou o *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity,* com o objetivo de fornecer um conjunto agregado e harmonizado de princípios e boas práticas sobre o desenvolvimento, estabelecimento e implementação de estratégias nacionais de segurança cibernética (ITU, 2018). O Guia foi elaborado em colaboração com doze instituições, como o Banco Mundial, o CCDCOE, o *Geneva Centre for Security Policy* (GCSP), a *Global Cyber Security Capacity Center* (GCSCC) da Universidade de Oxford, entre outros parceiros do setor privado, bem como da academia e da sociedade civil (INTERNATIONAL TELECOMMUNICATION UNION, 2018). O material tem por objetivo ser uma ferramenta útil para todas as partes interessadas, incluindo formuladores de políticas nacionais, legisladores e reguladores, com responsabilidades de segurança cibernética. Além disso, foi criado para ter aplicabilidade ampla para que os conceitos introduzidos possam ser aplicados nos níveis regional e municipal, bem como ser adaptados para a indústria (INTERNATIONAL TELECOMMUNICATION UNION, 2018)

Segundo o Guia, nas últimas duas décadas, bilhões de pessoas em todo o mundo se beneficiaram do crescimento exponencial e da rápida adoção de tecnologias da informação e comunicação, e das oportunidades econômicas e sociais associadas, sendo a cibersegurança um fator fundamental para alcançar o desenvolvimento socioeconômico (INTERNATIONAL TELECOMMUNICATION UNION, 2018)Atualmente, cento e vinte e sete países em todo o

mundo possuem estratégias nacionais de segurança cibernética publicadas (ITU, 2021), o que demonstra que o esforço das instituições internacionais, como o ITU, tem apresentado resultado, pois em 2018 eram apenas setenta e seis nações com ferramentas deste tipo (INTERNATIONAL TELECOMMUNICATION UNION, 2018)).

No que tange às ações para combate ao cibercrime, o Guia foca em legislação, regulação e na cooperação internacional. Na legislação e regulação, a recomendação abrange o desenvolvimento de um marco legal e regulatório para proteger a sociedade contra crimes cibernéticos e, consequentemente, promover um ambiente cibernético seguro e confiável (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Assim sendo, o Guia argumenta que a estratégia cibernética nacional deve promover o desenvolvimento de um marco legal interno que defina claramente o que constitui atividade cibernética proibida, e que tenha como propósito reduzir a cibercriminalidade, seja através da promulgação de novas leis específicas ou da alteração das já existentes (INTERNATIONAL TELECOMMUNICATION UNION, 2018)). Como exemplo de legislações desse tipo que podem ser alteradas temos o código penal e as leis das telecomunicações. O Guia fortalece, em diversas passagens, a preocupação com a salvaguarda de direitos e liberdade individuais, destacando o caso de investigações criminais, bem como os direitos de proteção de dados, incluindo a proteção da privacidade de dados pessoais (INTERNATIONAL TELECOMMUNICATION UNION, 2018)

Semelhante ao *framework* do CCDCOE (OTAN), o Guia do ITU incentiva que o desenvolvimento da aplicação da lei cibernética deve incluir treinamento e educação para as partes interessadas envolvidas no combate ao crime cibernético, como juízes, promotores, advogados, policiais, especialista forenses, entre outros (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Além disso, sugere que devem ser reconhecidas as autoridades responsáveis pela proteção das infraestruturas críticas, bem como os responsáveis por garantir que todos os requisitos internacionais de crimes cibernéticos estejam sendo cumpridos (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Também coloca a necessidade da criação de instituições envolvidas em cibersegurança, como Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERTs),[40] Grupo de Resposta a Incidentes de Segurança (*Computer Security Incident Response Team,* CSIRTs)[41]

[40] Seu objetivo é auxiliar o Administrador de redes na gerência e implementação de soluções de segurança.

[41] O *Computer Security Incident Response Team* (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança, é uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores

ou CSIRTs nacionais, seja para responder a incidentes cibernéticos ou como uma autoridade responsável para coordenar a política cibernética em um país (ITU, 2018). Em se tratando de cooperação internacional para combate ao cibercrime, o Guia destaca que a segurança cibernética "desempenha cada vez mais um papel em muitas áreas diferentes das Relações Internacionais, incluindo Direitos Humanos, desenvolvimento econômico, comércio, controle de armas, segurança, estabilidade, paz e resolução de conflitos" (INTERNATIONAL TELECOMMUNICATION UNION, 2018), p. 48, tradução nossa).

Dessa forma, para o Guia deve-se reconhecer a natureza sem fronteiras da segurança cibernética, destacando a necessidade de cooperar não apenas com as partes interessadas nacionais, mas também internacionais (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Assim sendo, ao elaborar sua estratégia, a nação precisa expressar um compromisso com a cooperação internacional sobre cibersegurança e, também, reconhecer as questões cibernéticas como um componente integral da política externa do país (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Para isso, é importante incentivar o desenvolvimento e uso de competências e habilidades focadas em questões cibernéticas, como diplomacia cibernética, para complementar os métodos e processos tradicionais da diplomacia. Neste sentido, o guia traz exemplos notáveis de esforços internacionais, como o Grupo Governamental de Especialistas em Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional (UN GGE), a Organização de Segurança e Cooperação na Europa (OSCE), o trabalho do subgrupo de Crimes de Alta Tecnologia do G7, a Convenção de Budapeste sobre Crimes Cibernéticos do Conselho da Europa, a Convenção sobre Cibersegurança da União Europeia e a Convenção Árabe sobre o Combate aos Crimes de Tecnologia da Informação, entre outros (INTERNATIONAL TELECOMMUNICATION UNION, 2018).

3.5.1 Análise do Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity (ITU)

O *framework* do ITU tem apenas duas ações inseridas no espectro de securitização sugerido por essa pesquisa: a *prática de exercícios cibernéticos* e o *discurso da soberania nacional*, conforme mostra o quadro 8, abaixo. No entanto, o instituto tem como pretensão que a maior parte dos países possuam estratégias de segurança cibernética próprias para enfrentar os desafios do cibercrime (INTERNATIONAL TELECOMMUNICATION UNION, 2018). Desta maneira, as ações sugeridas pelo ITU vão no sentido de proteger as liberdades

individuais, de garantir a privacidade e de criar um ambiente de confiança no ciberespaço. Além disso, o *framework* traz orientações para a implantação da gestão de riscos, para a proteção das infraestruturas críticas e para a capacitação técnica nas universidades, além da sugestão de uma coordenação cibernética nacional e do cuidado com a resiliência cibernética, conforme demonstra a figura 10, que apresenta as diferentes intensidades de cada categoria.

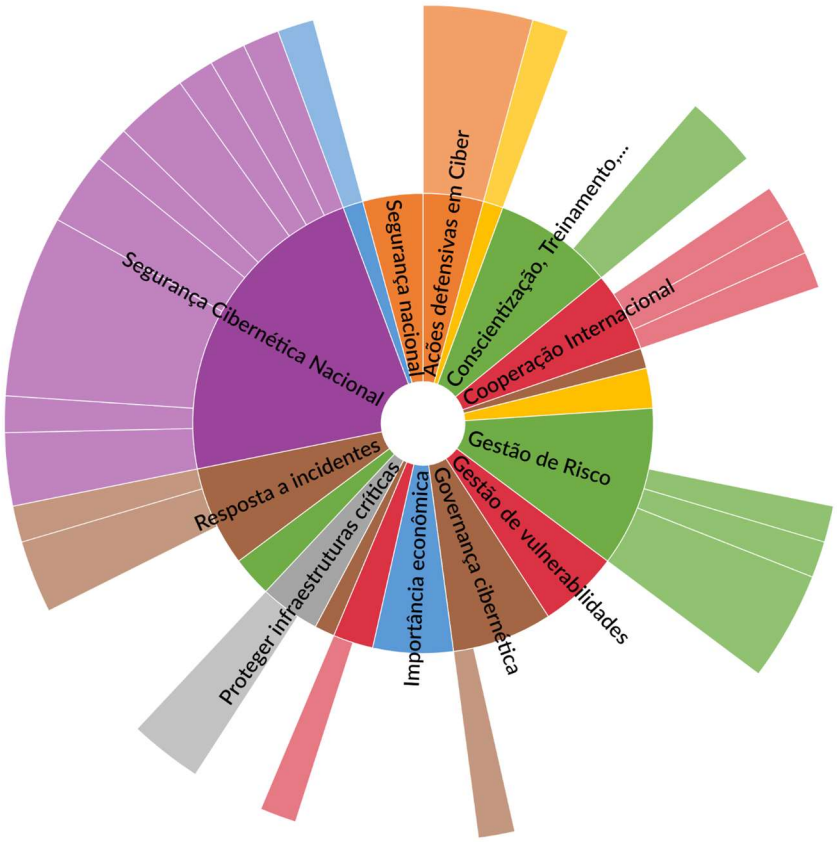
Quadro 8 - Codificações de securitização do framework do ITU

CATEGORIAS E SUBCATEGORIAS	ITU
4.2: Ameaças de ataque cibernético	9%
12: Exercícios cibernéticos	26%
34: Garantia da soberania nacional	35%

Fonte: Elaborado pelo autor com dados extraídos da ferramenta Nvivo

O *framework* do ITU tem um foco em ações de governança cibernética, que envolvem gestão de riscos e de vulnerabilidades. Ademais, a partir da Figura 10, pode-se verificar a relevância dada para as ações de *Gestão de Risco, Conscientização, Treinamento e Cooperação Internacional.*

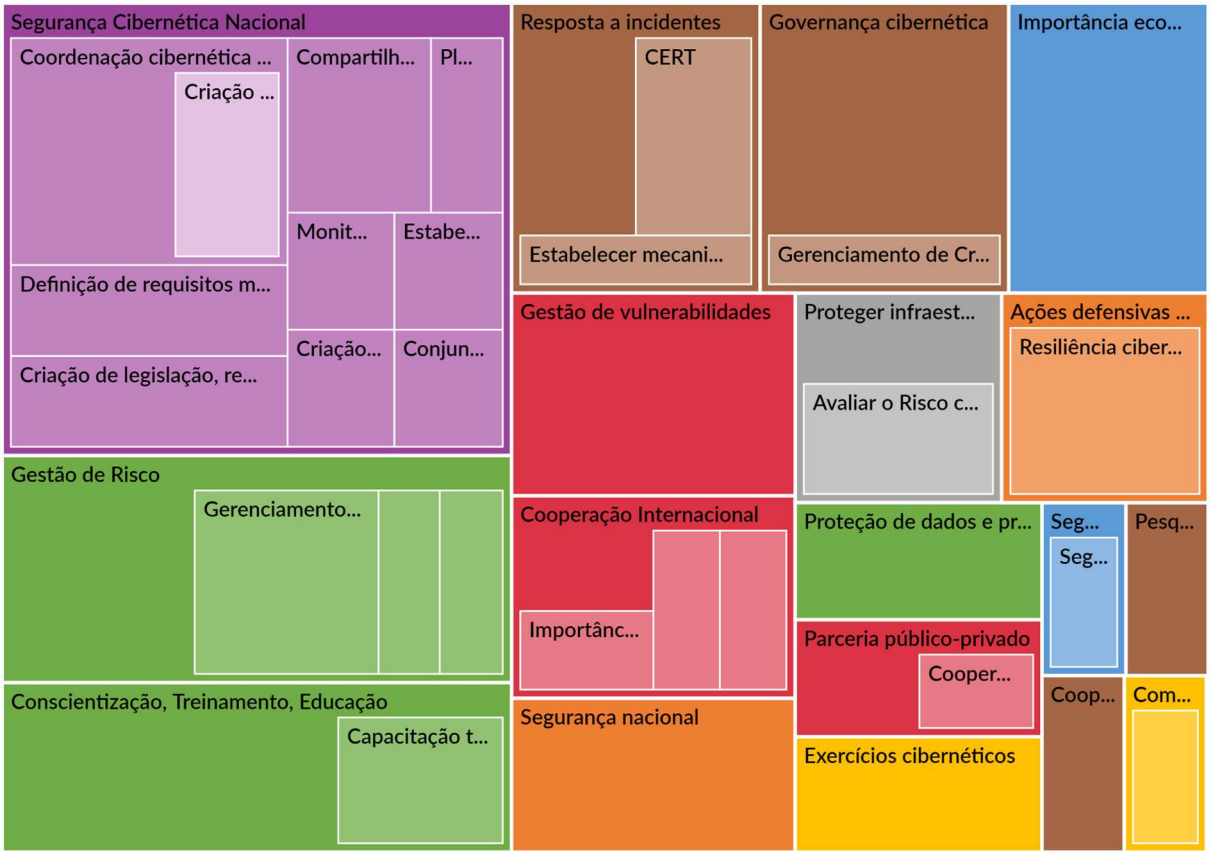
Figura 10 - Representação gráfica das ações de cibersegurança do framework da ITU



Fonte: Elaborado pelo autor através da ferramenta Nvivo

A Figura 11 exibe de outra maneira as categorias e subcategorias encontradas na análise do documento do ITU. Percebe-se que a categoria *Segurança Cibernética Nacional* é a mais relevante. Nela são definidos os responsáveis pela coordenação nacional, bem como a criação de um conselho nacional para tratar da cibersegurança, além da definição de requisitos mínimos de proteção, monitoramento da estratégia, entre outros. Por fim, a conscientização da população e a capacitação de profissionais nas universidades recebem destaque nesse modelo.

Figura 11 - Representação das ações do ITU em formato de Mapa de Árvore



Fonte: Elaborado pelo autor por meio da ferramenta Nvivo

3.6 CYBERSECURITY: RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN (OEA)

A Organização dos Estados Americanos (OEA) é a organização regional mais antiga do mundo, tendo sua origem na Primeira Conferência Internacional Americana, que ocorreu de outubro de 1889 a abril de 1890, nos Estados Unidos (ORGANIZATION OF AMERICAN STATES, 2009a). Segundo a OEA (2009), o resultado dessa reunião foi a criação da União Internacional das Repúblicas Americanas, que deu início ao mais antigo sistema institucional internacional, através do estabelecimento de uma série de disposições e instituições. Em 1948, a OEA foi fundada com a assinatura da Carta da OEA, em Bogotá, na Colômbia. Segundo o Artigo 1º da Carta, o propósito da organização é levar aos Estados membros uma ordem de paz e de justiça, para promover a solidariedade, intensificar sua colaboração e defender sua soberania, sua integridade territorial e sua independência (OEA, 2014). Atualmente, a OEA reúne 35 países das Américas, e tem como pilares a democracia, os direitos humanos, a segurança e o desenvolvimento (ORGANIZATION OF AMERICAN STATES, 2009a).

A ampla utilização da internet nas Américas na última década fez com que a OEA decidisse apoiar os Estados membros na luta contra o cibercrime. Desta forma, através do Comitê Interamericano contra o Terrorismo (CICTE) e do Programa de Segurança Cibernética, estabeleceu uma agenda para discutir a segurança cibernética na região (ORGANIZATION OF AMERICAN STATES, 2009b). Assim, por meio de instituições nacionais e regionais, dos setores público e privado, a OEA tenta fortalecer as capacidades de proteção cibernética dos Estados membros por meio de assistência técnica e treinamento, além de fóruns sobre política e intercâmbio das melhores práticas para uso de tecnologia e da segurança da informação (ORGANIZATION OF AMERICAN STATES, 2009b).

Em 2016, com o objetivo de diagnosticar o nível de maturidade em cibersegurança dos países da América Latina, o Banco Interamericano de Desenvolvimento (BID) e a OEA elaboraram o relatório *Cybersecurity: Risks, Progress, and the Way Forward in Latin America and Caribbean*. A avaliação foi realizada com base no *Capability Maturity Model* (CMM) para nações, um modelo criado em 2013 pelo *Global Cyber Security Capacity Centre*, que pertence à Universidade de Oxford. A abordagem avaliou a capacidade dos países em cinco dimensões: Política e Estratégia de Segurança; Cibercultura e Sociedade; Educação, Treinamento e Habilidades em Segurança Cibernética; Marcos Legais e Regulatórios; e Padrões, Organizações e Tecnologias (ORGANIZATION OF AMERICAN STATES, 2020).

Essas dimensões foram subdivididas em um conjunto de fatores que descrevem e definem o que significa a capacidade de segurança cibernética naquela dimensão. Assim, mesmo não sendo um guia para implantação, acaba por construir uma estrutura que se assemelha aos *frameworks* que são avaliados nessa pesquisa. Desta forma, elenca uma série de ações que fazem parte de uma estratégia nacional de segurança cibernética, entre elas a proteção das infraestruturas críticas, o gerenciamento de crises, o estabelecimento da ciberdefesa, a criação de cultura cibernética, a conscientização da população em cibersegurança, o treinamento de profissionais, a criação de leis e o processamento dos crimes cibernéticos, entre outros. Assim sendo, essa pesquisa submeteu esse relatório à Teoria fundamentada, pois ele consegue elaborar um modelo que pode ser seguido para estabelecer ações na segurança cibernética de países. O estudo utiliza a versão 2020 do relatório, uma vez que, com a atualização do modelo CMM em 2017, a OEA e o BID submeteram os países a uma nova avaliação.

3.6.1 Análise do Cybersecurity: Risks, Progress, and the Way Forward in Latin America and Caribbean (OEA)

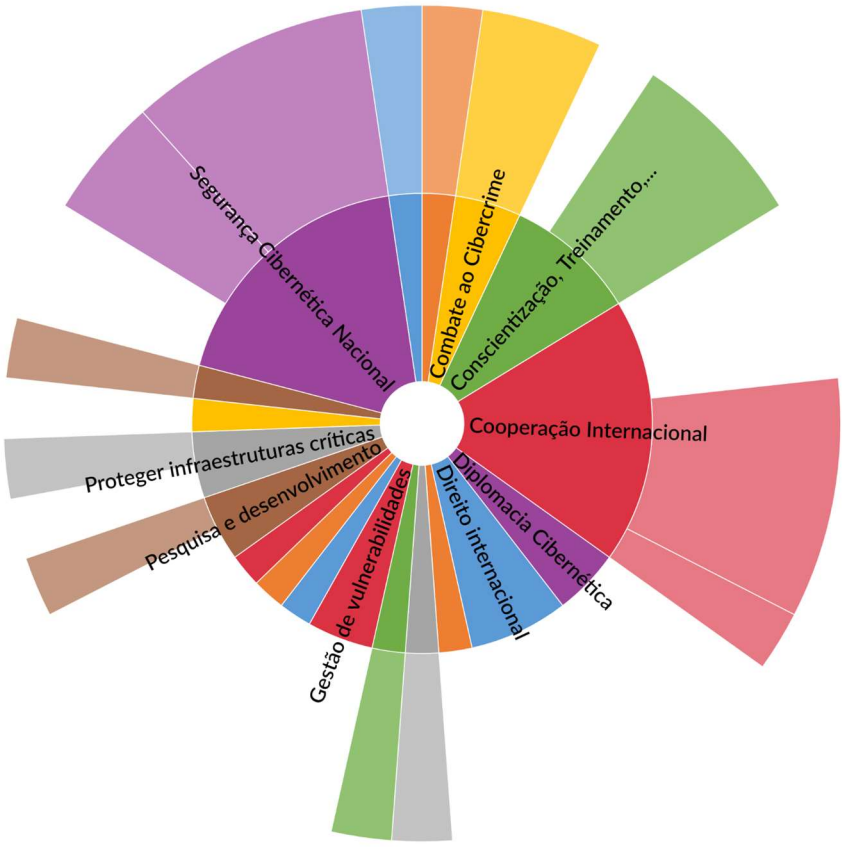
Em relação ao combate ao cibercrime, o documento da OEA apenas faz referência ao *Roubo de Propriedade Intelectual*, que também surge novamente na categoria de *Espionagem Cibernética,* conforme o Quadro 9. No que tange ao objetivo dessa pesquisa, o único item dentro do espectro da securitização encontrado foi a *Dissuasão Cibernética*. A maioria das ações sugeridas pelo *framework* da OEA situam-se dentro do espectro político, conforme apresenta a Figura 12, destacando-se a *Segurança Cibernética Nacional* e a *Cooperação Internacional*, além das iniciativas para a *Conscientização, Treinamento e Cultura*. A Figura 13 exibe de uma forma mais abrangente as categorias encontradas no *framework* da OEA, sendo possível visualizar a *Diplomacia Cibernética*, *Gestão de Vulnerabilidades* e o *Direito Internacional*.

Quadro 9 - Codificações mais próximas da securitização do *framework* do OEA

CATEGORIAS E SUBCATEGORIAS	OEA
4: Combate ao cibercrime	0%
4.24: Roubo de propriedade intelectual	47%
10: Dissuasão cibernética	21%
11: Espionagem cibernética	0%
11.3: Roubo de propriedade intelectual comercial	23%

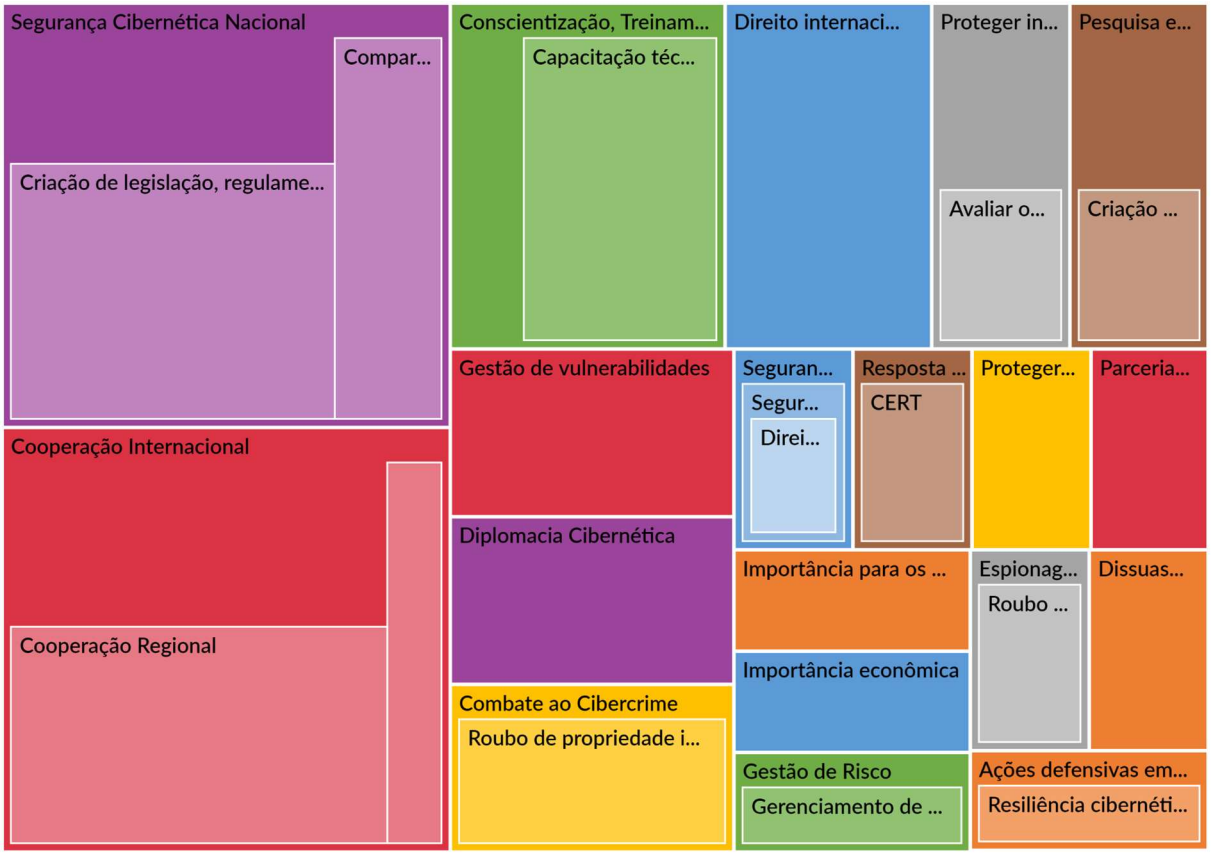
Fonte: Elaborado pelo autor com dados da ferramenta Nvivo

Figura 12 - Representação gráfica das ações de cibersegurança sugeridas pela OEA



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Figura 13 - Representação das ações da OEA em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

3.7 SÍNTESE DO CAPÍTULO

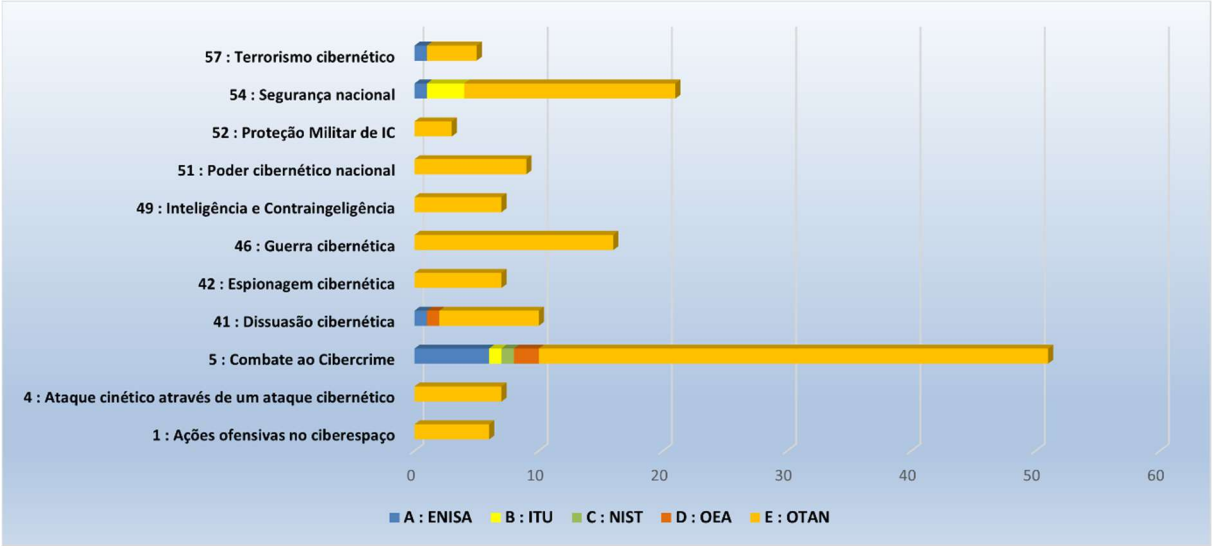
O Capítulo 3 apresenta o resultado da aplicação da Teoria Fundamentada à qual os documentos de OTAN, OEA, NIST, ITU e ENISA foram submetidos. A codificação dos *frameworks* serviu para mostrar todas as práticas sugeridas por essas organizações para que os países desenvolvam suas próprias estratégias/políticas de segurança cibernética. A partir da análise, é possível identificar uma série de ações de cibersegurança situadas dentro do espectro político, como gestão de riscos e de vulnerabilidades, governança cibernética, entre outras. Além disso, tendo como base os conceitos elencados no item *2.4.2 Securitização cibernética*, a pesquisa focou na identificação de ações inseridas no espectro da securitização para proteção do domínio cibernético.

A identificação de códigos nos *frameworks* foi fundamental para a busca dos demais objetivos desta pesquisa, isso porque o processo de codificação da Teoria Fundamentada só foi concluído com a realização deste processo nas estratégias ou políticas dos países, fazendo com que a busca por dados ficasse ainda mais robusta, principalmente pela inserção dos delitos

penais mais combatidos entre as nações pesquisadas. Em síntese, o resultado encontrado na codificação dos *frameworks* mostra que, em sua maioria, as práticas sugeridas pelos documentos situam-se dentro do espectro político, com destaque para as ações de gestão cibernética, criação de uma coordenação nacional, bem como o gerenciamento de riscos e de vulnerabilidades. No que tange às ações securitizadas, o *framework* da OTAN é o que mais se situa no campo da securitização, o que pode ser explicado pela natureza militar dessa organização. Entretanto, como já foi dito, o documento da OTAN pode ser aplicado conforme a capacidade e necessidade de cada país, ou seja, embora aborde a linguagem da securitização, pode ser usado como um guia para a implementação de ações na área de gestão da segurança cibernética.

Como forma de apresentar as securitizadas em cada *framework* estudado, a figura 14 contabiliza o total de securitização em cada categoria. Pode-se notar que o documento da OTAN é o mais representativo em relação aos objetivos dessa pesquisa, como o maior número de ações securitizadas. Dessa forma, é possível estabelecer um ranking de securitização dos *frameworks* estudados, visualizando a quantidade de ações, bem como a representatividade delas em cada documento codificado.

Figura 14 - Resumo das ações securitizadas nos *frameworks*



Fonte: Elaborado pelo autor com dados extraídos por meio da ferramenta Nvivo

No capítulo seguinte, ampliamos a codificação da Teoria Fundamentada, aplicando-a aos países que possuem estratégia ou política cibernética, viabilizando, dessa forma, que se identifiquem correlações entre as ações desenvolvidas pelos países e os *frameworks* estudados na pesquisa. Dessa forma é possível, por exemplo, identificar a que *framework* um país está

mais alinhado, bem como gerar visualizações que tornem mais prático o entendimento dos objetivos e ações destes países para desenvolvimento de sua segurança cibernética nacional.

4 ANÁLISE DOS PAÍSES DA AMÉRICA DO SUL

Além de apresentar os resultados da pesquisa sobre a securitização cibernética no continente, esse capítulo apresenta de forma abrangente as ações técnicas, legislativas e de cooperação que os países da América do Sul adotam para promover sua proteção no ciberespaço. Na primeira parte, são apresentados os países que possuem estratégia cibernética nacional ou política publicada (Argentina, Brasil, Chile, Colômbia, Equador e Paraguai), e que serão avaliados segundo a perspectiva da securitização dessas estratégias, a partir da avaliação dos *frameworks* no capítulo anterior. Em seguida, serão discutidas as iniciativas dos outros países do continente, os quais ainda não possuem uma estratégia elaborada, mas que apresentam - muitos deles - uma série de ações para estabelecer sua segurança e defesa cibernéticas.

Os países que possuem estratégia/política cibernética também foram submetidos às etapas de codificação da Teoria Fundamentada. Com isso, além de se obter novas codificações para enriquecer a pesquisa, permite que os dados, de países e *frameworks*, possam ser cruzados, dando origem a gráficos e tabelas que explicam a relação comum existente entre eles. Ademais, foi possível encontrar dados mais específicos sobre esses países, os quais revelaram, por exemplo alguns dos tipos de cibercrimes de maior destaque nesses lugares - exemplo disso é o Paraguai, que dedica relevante atenção ao combate à pornografia infantil.

Na etapa seguinte à codificação foi realizada a comparação das codificações obtidas nas estratégias dos países estudados com o resultado encontrado na codificação seletiva - que reúne as ações consideradas securitizadas. Assim, além de compreender se esses países adotam ações securitizadas para sua proteção cibernética, também foi possível verificar a qual *framework* cada estratégia se adequa melhor. Com isso, é possível saber, de maneira mais assertiva, se um país adota ações voltadas à governança e gestão, ou se prefere (ou opta por) atingir seus objetivos por meio de uma perspectiva que vai além da política. A seguir, será apresentado o estudo realizado com esses países da América do Sul.

4.1 APLICAÇÃO DA TEORIA FUNDAMENTADA NAS ESTRATÉGIAS

Assim como os frameworks, as estratégias dos países (Argentina, Brasil, Chile, Colômbia, Equador e Paraguai) foram submetidos a Teoria Fundamentada. Embora a codificação dos documentos desses países tenha gerado códigos referentes a práticas de gestão, o quadro 10 apresenta apenas a codificação relativa à securitização cibernética, objeto desta pesquisa. A porcentagem exibida representa o valor que essa categoria representa em todo o

universo de categorias consideradas securitizadas codificadas entre esses países. Um outro detalhe importante na tabela é a informação dos tipos de delitos digitais, que agora possuem informações que revelam mais especificidades sobre o cibercrime na região. Nos próximos itens desse capítulo são detalhadas as estratégias ou políticas dos países pesquisados, com foco na securitização cibernética de suas ações.

Quadro 10 - Resultado da codificação de securitização cibernética dos países

Categorias e subcategorias	Argentina	Brasil	Chile	Colômbia	Equador	Paraguai
1: Ações ofensivas no ciberespaço	-	6%	-	-	3%	-
1.1: Agressão entre Estados	14%	-	-	-	3%	-
1.2: Ataque Cibernético	-	-	4%	4%	5%	-
3: Ataque cinético através de um ataque cibernético	-	-	-	-	-	-
4: Combate ao Cibercrime	7%	-	11%	-	13%	9%
4.1: Acesso ilegal às informações em computadores, sistemas e redes	-	-	-	-		2%
4.2: Ameaças de ataque cibernético	-	-	3%	-	3%	-
4.3: Análise conjunta de desafios do cibercrime	-	5%	-	-		-
4.4: Ataque DDoS	-	8%	1%	-	3%	2%
4.5: Atribuição de ataques	-	-	15%	-	2%	-
4.6: Ciberbullying	-	-	-	-	2%	3%
4.7: Cooperação com polícias internacionais	-	-	-	-	-	-
4.8: Criação de um centro de operações de Seg. cibernética	-	-	-	3%	-	-
4.9: Defacement	-	-	-	-	-	2%
4.10: Desenvolver conhecimento e experiência em cibercrimes	-	4%	5%	9%	4%	5%
4.11: Disseminação de malware	-	-	-	-	2%	-
4.12: Espionagem industrial	-	-	2%	-	-	-
4.13: Exploração de crianças na Internet	-	-	-	-	-	4%
4.14: Falsificação	-	-	-	-	-	-
4.15: Fraude	-	-	2%	-	4%	4%
4.16: Função policial	-	-	-	6%	1%	18%
4.17: Interrupção de serviços	-	6%	2%	-	-	-
4.18: Pharming	-	-	-	-	-	-

4.19: Phishing	-	12%	-	-	-	-
4.20: Pirataria	-	3%	-	-	1%	-
4.21: Pornografia infantil	-	-	-	5%	2%	20%
4.22: Proteção do ISP	-	-	-	-	-	-
4.23: Ransomware	-	-	1%	-	-	-
4.24: Roubo de propriedade intelectual	-	-	1%	-	-	-
4.25: Sabotagem de sistemas	-	-	-	-	4%	-
4.26: Spam	-	-	-	-	1%	-
4.27: Vazamento de dados	-	6%	-	-	1%	3%
4.28: Vulnerabilidades do Dia Zero	-	-	-	-	-	-
4.29: Botnet	-	-	-	-	1%	-
4.30: Discurso de ódio	-	-	-	-	1%	-
4.31: Exposição de conteúdo impróprio	-	-	-	-	1%	-
4.32: Extorsão	-	-	-	-	2%	-
4.33: Mineração de bitcoins	-	-	-	-	1%	-
4.34: Ataques baseados na web	-	-	-	-	2%	
10: Dissuasão cibernética	-	-	8%	-	-	-
11: Espionagem cibernética	-	6%	18%	-	6%	6%
11.1: Perda do crescimento econômico	-	-	-	-	-	-
11.2: Minar economia nacional	-	-	-	-	-	-
11.3: Roubo de propriedade intelectual comercial	-	-	-	-	-	-
12: Exercícios cibernéticos	5%	11%	-	2%	-	-
16: Guerra cibernética	-	-	-	-	-	-
16.1: Capacidade militar cibernética	-	-	-	6%	-	-
16.2: Criação de um comando cibernético	-	-	-	1%	-	-
19: Inteligência e Contrainteligência	-	-	-	3%	2%	-
25: Poder nacional	-	-	-	-	-	-
25.1: Poder cibernético nacional	-	-	-	1%	-	-
28: Proteger infraestruturas críticas	27%	12%	4%	14%	12%	22%
28.10: Uso militar para proteção	-	-	-	10%	-	-
34: Garantia da soberania nacional	23%	17%	23%	21%	10%	-
34.1: Ameaça à Prosperidade	-	4%	-	2%	-	-

34.2: Proteção das infraestruturas críticas	17%	-	-	-	3%	-
35: Terrorismo cibernético	7%	-	-	13%	5%	-

Fonte: Elaborado pelo autor com dados extraídos do *software* Nvivo

4.2 ARGENTINA

Em 2019, o país publicou uma atualização da *Estrategia Nacional de Ciberseguridad de la República Argentina*, que foi elaborada de forma multidisciplinar e multisetorial pelo poder executivo, estabelecendo os princípios básicos e os objetivos fundamentais que buscam permitir ao país estabelecer suas ações de proteção do ciberespaço (REPÚBLICA ARGENTINA, 2019). A iniciativa faz parte de várias medidas legislativas tomadas pelo país nos últimos anos para implementar políticas administrativas e regulatórias para os setores de telecomunicações, tecnologia e internet. Em 2017, foi promulgado o Decreto 577/2017, que criou o Comitê de Cibersegurança, que inclui representantes do Ministério da Defesa e do Ministério da Segurança, com o objetivo de continuar o trabalho de desenvolvimento de uma estratégia nacional de cibersegurança (REPÚBLICA ARGENTINA, 2017).

Por meio de empréstimos aprovados pelo Banco Interamericano de Desenvolvimento (BID), o governo argentino se capacitou financeiramente para desenvolver políticas relacionadas à infraestrutura crítica nacional, à segurança de dados pessoais e implementação de boas práticas no uso da tecnologia da informação, como ações específicas para fortalecer suas capacidades de cibersegurança nacional (BANCO INTERAMERICANO DE DESARROLLO, 2020). Além disso, em 2017, o país fez uma parceria técnica com os Estados Unidos para estabelecer um grupo de trabalho que auxilie o país no fortalecimento das capacidades nacionais de segurança cibernética (U.S. EMBASSY IN ARGENTINA, 2017). O país também estabeleceu acordos com países como Espanha e Chile (OEA, 2020).

Em 2011, a Argentina instituiu um Programa Nacional de Infraestruturas Críticas para a Informação e Segurança Cibernética (ICIC), com a finalidade de criar e adotar um marco regulatório para definir e proteger a infraestrutura crítica dos setores público e privado nacionais (REPÚBLICA ARGENTINA, 2011). O programa levou à criação do CSIRT Nacional da Argentina, o ICIC-CERT, que é a equipe nacional de resposta a incidentes de segurança cibernética. Mesmo com o trabalho desenvolvido pelo ICIC com o setor privado, um relatório apresentado pela consultoria *Price Waterhouse Cooper* em 2018 informa que 53% das empresas argentinas pesquisadas não possuem uma estratégia de segurança cibernética, e 61% não têm um plano de contingência sobre como responder a um incidente cibernético

(PRICEWATERHOUSECOOPERS, 2018).

No que tange o marco regulatório sobre segurança cibernética, a Argentina foi um dos primeiros países das Américas a possuir uma legislação para a proteção dos dados pessoais, a Lei 25.326/2000 (REPÚBLICA ARGENTINA, 2000). Além disso, em 2008 o país sancionou a Lei 26.388, que alterou o código penal para incluir o crime cibernético (REPÚBLICA ARGENTINA, 2008), e possui um projeto de lei que prevê a tipificação de crimes contra danos à infraestrutura crítica (OEA, 2020). Por fim, em busca de cooperação internacional para o combate ao cibercrime, a Argentina teve sua adesão à Convenção de Budapeste sobre Crimes Cibernéticos do Conselho da Europa ratificada em 2018 (COUNCIL OF EUROPE, 2018).

4.2.1 Análise da Estratégia Nacional de Segurança Cibernética Argentina

Apesar da estratégia cibernética da Argentina citar algumas vezes a possibilidade de agressão entre países por meio do domínio cibernético, em geral, a maioria de suas ações se encontra inserida no espectro político. Embora o combate ao cibercrime tenha importância, não houve uma descrição sobre a ocorrência de algum delito digital em específico, conforme pode ser visto no Quadro 11. Além disso, o discurso da necessidade de proteção para garantir a soberania recebe a maior relevância em sua estratégia. Por fim, um destaque importante na codificação do documento é relativo à preocupação com a possibilidade do terrorismo cibernético. O cuidado pode ser devido ao histórico da Argentina com ataques terroristas, como o executado contra o prédio da Associação Mutual Israelita (AMIA), em 1994, e o outro contra a embaixada de Israel em 1992, ambos em Buenos Aires (G1, 2019), bem como pelos alertas de atentados, como um emitido em 1998, contra um alvo judaico (GERCHMANN, 1998), e outro da possibilidade da *Al Qaeda* atacar um *shopping center* em 2015, ambos também na capital (CLARÍN, 2015).

Quadro 11 - Codificações de securitização encontradas na estratégia da Argentina

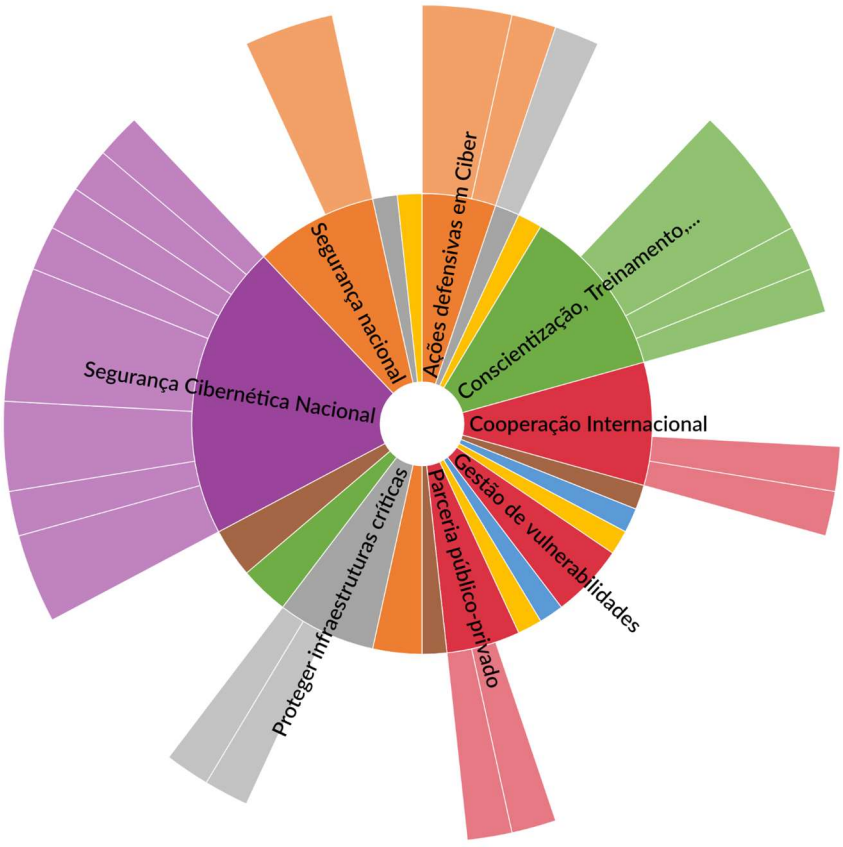
CATEGORIA E SUBCATEGORIAS	ARGENTINA
2: Ações ofensivas no ciberespaço	-
2.1: Agressão entre Estados	14%
4: Combate ao Cibercrime	7%
12: Exercícios cibernéticos	5%
34: Garantia da soberania nacional	23%

35: Terrorismo cibernético	7%

Fonte: Elaborado com dados extraídos através da ferramenta Nvivo

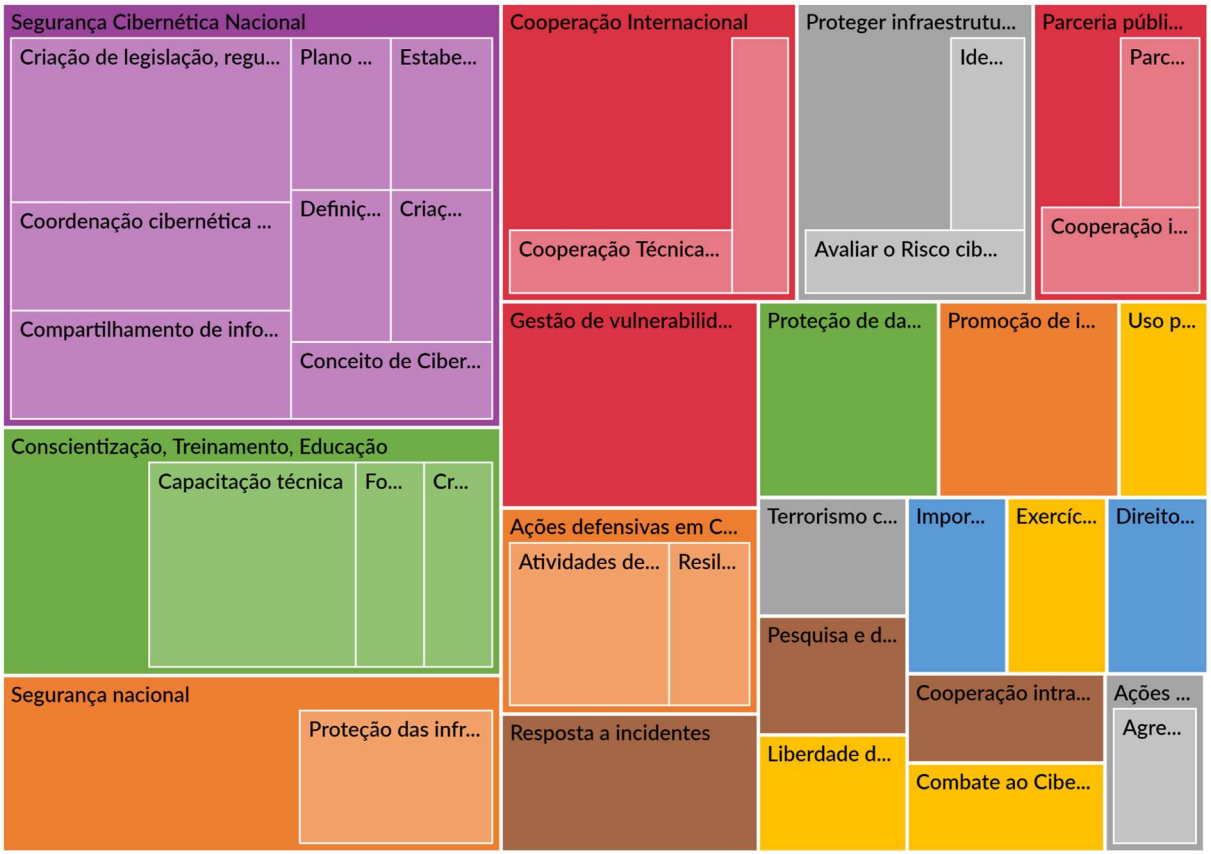
As ações de proteção do domínio cibernético da Argentina estão, em sua maioria, inseridas no espectro político. Desta forma, as codificações que mais se destacam são referentes à criação de um ambiente estatal para gerir a cibersegurança nacional, bem como a criação de legislação, o estabelecimento de um conselho de segurança, entre outros, conforme mostra a Figura 15. Além disso, o país valoriza a conscientização, a cooperação internacional, a proteção das infraestruturas críticas e as parcerias público-privadas. Ademais, a Figura 16 apresenta outras categorias presentes na estratégia da Argentina, como o *uso pacífico do ciberespaço*, o *cuidado com a proteção dos dados e da privacidade*, a *vontade de estabelecer uma indústria cibernética nacional*, o *respeito pelo direito internacional* e a relevância *da liberdade de expressão e dos direitos humanos*.

Figura 15 - Representação gráfica das ações de cibersegurança da Argentina



Fonte: Elaborado pelo autor por meio da ferramenta Nvivo

Figura 16 - Representação das ações da Argentina em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Em uma última análise sobre a estratégia cibernética nacional da Argentina, o ANEXO A mostra que o *framework* da ENISA é aquele com o qual as ações de proteção do domínio cibernético do país mais se assemelham. Essa análise é realizada através da ferramenta de comparação de arquivos do *software* Nvivo, que verifica que códigos são idênticos entre dois documentos diferentes. Dessa forma, a pesquisa retornou que existem 23 pontos de convergência entre a estratégia da Argentina com o *framework* do ITU, 22 com a OTAN, 11 com o NIST, 14 com o da OEA e 25 códigos convergentes com o modelo da ENISA.

4.3 BRASIL

Em 2020, o país publicou sua Estratégia Nacional de Segurança Cibernética, com o intuito de orientar a abordagem de segurança cibernética do Estado e, também, incluir ações para aumentar a resiliência contra ameaças cibernéticas e fortalecer seu desempenho internacional no tema (BRASIL, 2020a). A estratégia brasileira estabelece um modelo centralizado de governança em nível nacional para promover a coordenação entre diferentes

atores relacionados com a segurança cibernética, criando um Conselho Nacional de Cibersegurança com a finalidade de incentivar ações de conformidade, bem como de proteção cibernética em entidades públicas e privadas (BRASIL, 2020a).

No que tange o arcabouço legal para cibersegurança, desde 2012, o país possui uma lei que tipifica os delitos cibernéticos, especificando crimes como a invasão de dispositivo informático e falsificação de cartão magnético (BRASIL, 2012). Em 2014, o Brasil aprovou o Marco Civil da Internet, Lei 12.965/2014, com o objetivo de regulamentar o uso da internet no país por meio do estabelecimento de princípios, garantias, direitos e deveres para os usuários da internet e para os prestadores de serviços de conexão (BRASIL, 2014a). Em 2018, foi publicada a Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018, com a finalidade de estabelecer ações sobre o tratamento de dados pessoais, por pessoa física ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais e de privacidade (BRASIL, 2018).

O Brasil possui um centro para tratar de incidentes de segurança cibernética que afetem órgãos públicos (chamado de CSIRT.gov), além de vários CSIRT's, do setor privado e de instituições públicas. No entanto, o CERT.br continua sendo a maior referência em tratamento de incidentes e emissão de boletins de ocorrência de sobre segurança cibernética em nível nacional para diferentes setores da sociedade brasileira, bem como uma fonte de dados estatísticos sobre o cenário de ataques cibernéticos no país. Além disso, o centro possui um programa nacional de conscientização sobre cibersegurança que vai desde cartilhas para uso da internet até cursos avançados de tratamento de incidentes e diversas publicações sobre segurança cibernética (CERT, 2022).

Em 2018, o Brasil aprovou a Política Nacional de Infraestruturas Críticas, com a finalidade de orientar ações para a segurança das infraestruturas suportadas pelo poder público (BRASIL, 2018a). A política define que compete ao Gabinete de Segurança Institucional da Presidência da República a responsabilidade pelos assuntos pertinentes às infraestruturas críticas nacionais no âmbito da administração pública federal com foco em ações de governança e gestão de riscos (BRASIL, 2018a). No entanto, o documento não especifica quem acompanha a proteção das infraestruturas administradas pelo setor privado, nem mesmo descreve quais são as indústrias consideradas estratégicas para o país.

A indefinição quanto à descrição das infraestruturas nacionais continua explícita na Estratégia Nacional de Infraestruturas Críticas, publicada em 2020 (Decreto 10.569/2020), que considera as infraestruturas de comunicação, energia, transportes, finanças e de águas como de dimensão estratégica, porém sem maiores especificações (BRASIL, 2020b). A estratégia

estabelece a necessidade de identificação e classificação das infraestruturas críticas do país e as suas possíveis ameaças e vulnerabilidades, bem como de proposição de medidas de controle para redução dos riscos às infraestruturas consideradas prioritárias (BRASIL, 2020b). No entanto, a estratégia do Brasil para infraestruturas críticas faz apenas uma referência à segurança cibernética no quadro de eixos estruturantes, destacando a importância da adoção de procedimentos de cibersegurança no setor, porém sem a apresentação de maiores detalhes (BRASIL, 2020b).

4.3.1 Análise da securitização da Estratégia Nacional de Segurança Cibernética brasileira

Em relação ao combate ao cibercrime, o documento brasileiro faz referência a uma série de tipos de crimes digitais, entre eles o *phishing,*[42] a pirataria, o vazamento de dados, a interrupção de serviços e o ataque DDoS,[43] como exposto no quadro 13. Sobre o espectro da securitização, o documento brasileiro não cita que o Brasil possui um comando cibernético militar - Comando de Defesa Cibernética (ComDCiber) - sendo que o setor cibernético recebe a atribuição de estratégico na Estratégia Nacional de Defesa, juntamente com os setores nuclear e espacial (BRASIL, 2008). Em sua definição no site do Ministério da Defesa, o ComDCiber tem o desafio de conduzir ações de proteção, exploração e ataques cibernéticos em proveito da defesa nacional (BRASIL, 2022). Apesar da existência desse comando, a estratégia brasileira coloca o Gabinete de Segurança da Presidência da República (GSI) como o órgão responsável pela coordenação das ações de proteção do domínio cibernético.

No que se refere ao objetivo desta pesquisa, não existem muitos itens de codificação relativos à perspectiva da securitização no documento brasileiro, tendo a questão do discurso da soberania nacional no ciberespaço o maior destaque. Além disso, conforme o Quadro 12, o país tem preocupações com a espionagem cibernética, ações ofensivas disparadas por outros Estados e a prática de exercícios cibernéticos militares, que é uma forma de treinar ações de ataque e defesa com armas cibernéticas. Uma característica que essa pesquisa destaca sobre a realidade da proteção cibernética do Brasil é a falta de uma coordenação unificada para o tema, ficando as iniciativas de segurança cibernética (governança, gestão de riscos e vulnerabilidades, ações políticas) a cargo do GSI, e as ações de defesa cibernética (ações ofensivas e defensivas

[42] É o crime de enganar as pessoas na tentativa de que compartilhem informações confidenciais como senhas e número de cartões de crédito, através de diversas técnicas como páginas falsas, por exemplo.

[43] Também chamado de ataque de negação de serviço distribuído, o DDoS aproveita que os servidores possuem uma limitação para receber requisições de acesso, assim o ataque se baseia "bombardear" um servidor com um número de requisições que ele não consegue processar, tornando o serviço indisponível ou lento.

no ciberespaço) sob a responsabilidade das Forças Armadas.

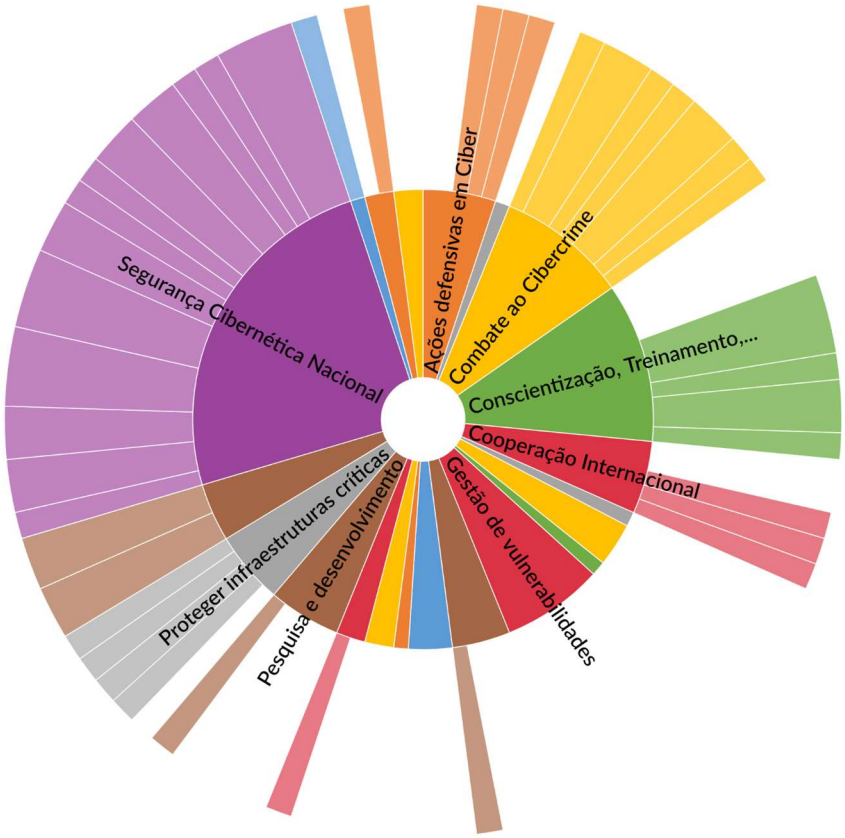
Quadro 12 - Codificações de securitização encontradas na estratégia do Brasil

CATEGORIAS E SUBCATEGORIAS	BRASIL
2: Ações ofensivas no ciberespaço	6%
4: Combate ao cibercrime	-
4.3: Análise conjunta de desafios do cibercrime	5%
4.4: Ataque DDoS	8%
4.10: Desenvolver conhecimento e experiência em cibercrimes	4%
4.17: Interrupção de serviços	6%
4.19: Phishing	12%
4.20: Pirataria	3%
4.27: Vazamento de dados	6%
11: Espionagem cibernética	6%
12: Exercícios cibernéticos	11%
34: Garantia da soberania nacional	17%
34.1: Ameaça à Prosperidade	4%

Fonte: Elaborado com dados extraídos através da ferramenta Nvivo

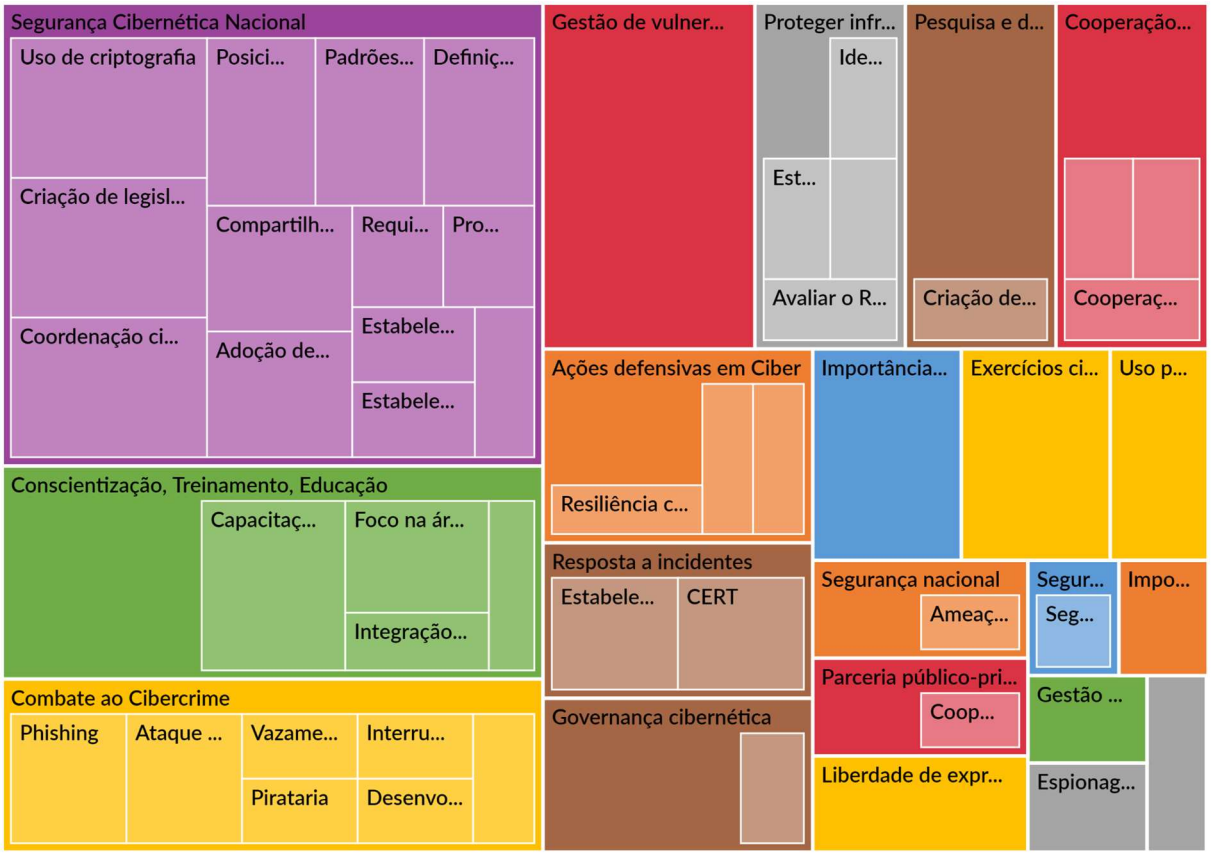
A Figura 17 mostra o resultado obtido com a codificação da estratégia cibernética brasileira, que apresenta maior quantidade de ações na categoria Segurança Cibernética Nacional, que engloba as iniciativas de elaboração de legislações, definição de políticas, compartilhamento de informações entre atores, produção de requisitos mínimos de segurança da informação e, também, para o 5G, além de ter a intenção de ser um líder sobre o tema no mundo. Ademais, existe a atenção com as infraestruturas críticas, conscientização da população e formação de profissionais capacitados em segurança cibernética. A representação mostrada na Figura 18 amplia a visualização da codificação da estratégia cibernética do Brasil.

Figura 17 - Representação gráfica das ações de cibersegurança do Brasil



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Figura 18 - Representação das ações do Brasil em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Em uma última análise sobre a estratégia cibernética nacional do Brasil, o ANEXO B mostra que o *framework* da OTAN é aquele com o qual as ações de proteção do domínio cibernético do país mais se assemelham. Dessa forma, a pesquisa retornou que existem 25 pontos de convergência entre a estratégia do Brasil com o *framework* da ENISA, 24 com o do ITU, 10 com o NIST, 16 com o da OEA e 27 códigos convergentes com o modelo da OTAN.

4.4 CHILE

Em 2017, o Chile publicou sua *Política Nacional de Ciberseguridad*, com a intenção de atingir metas de proteção cibernética até o ano de 2022. Entre os objetivos propostos estão ter uma infraestrutura de informações robusta e resiliente; o Estado ser o garantidor dos direitos das pessoas no ciberespaço; desenvolver estratégias de educação, boas práticas e relações de cooperação em segurança cibernética com diversos atores; e, desenvolver uma indústria de cibersegurança nacional para atender aos seus objetivos estratégicos (REPÚBLICA DE CHILE, 2017). Além disso, em 2018, conforme determina a política chilena, o presidente nomeou um

conselheiro presidencial que o informa diretamente sobre questões de segurança cibernética, bem como a criação de uma Coordenação de Cibersegurança (REPÚBLICA DE CHILE, 2017).

Em 2018, a Coordenação determinou a execução de uma série de ações relacionadas aos objetivos estratégicos da política nacional, como o fortalecimento do CSIRT do governo, que está ligado ao Ministério do Interior e da Segurança Pública (REPÚBLICA DE CHILE, 2022). Além disso, o país possui um acordo de cooperação com o BID, que fornece assessoria técnica para melhoria do nível de resposta de incidentes de segurança cibernética, de forma a fortalecer a gestão estratégica da segurança pública visando garantir um ciberespaço aberto, seguro e resiliente (ORGANIZATION OF AMERICAN STATES, 2020). O CSIRT do governo chileno é membro do CSIRT Américas, um programa de compartilhamento de informações sobre *malwares* e ameaças, que inclui a troca dinâmica de informações entre os CSIRT's membros (REPÚBLICA DE CHILE, 2022a).

No que se refere à proteção das infraestruturas críticas, o Chile define que os setores considerados críticos são energia, telecomunicações, serviços de saneamento, saúde, serviços financeiros, segurança pública, transporte, administração pública, proteção civil e defesa (REPÚBLICA DE CHILE, 2017). Segundo a estratégia, o governo precisaria estabelecer um grupo de trabalho cuja responsabilidade seria criar um marco regulatório para a proteção da infraestrutura crítica do país, bem como avaliar a construção de um CSIRT específico para tratamento dos incidentes que envolvam suas infraestruturas críticas (REPÚBLICA DE CHILE, 2017).

Ainda na década de 1990, o Chile desenvolveu legislações voltadas ao ambiente cibernético. Em 1993, foi criada a lei que penaliza atividades ilícitas em sistemas de informação, a Lei 19.223 (BIBLIOTECA DEL CONGRESO, 1993), anos depois, em 1999, foi sancionada a Lei 19.628 que protege e orienta o tratamento dos dados pessoais (BIBLIOTECA DEL CONGRESO, 1999). Em 2018, o Chile aprovou uma reforma constitucional para que seja reconhecido o direito à honra e à vida privada em sua Constituição, e inseriu um artigo que modifica as normas sobre proteção de dados pessoais (REPÚBLICA DE CHILE, 2018). Por fim, em 2017, o país adaptou suas regulamentações à Convenção de Budapeste sobre Crimes Cibernéticos (BIBLIOTECA DEL CONGRESO, 2017), além de adotar outras iniciativas legais em questões financeiras e gestão de continuidade de negócios (ORGANIZATION OF AMERICAN STATES, 2020).

Em 2020, o Chile foi considerado pelas Nações Unidas como o segundo país mais desenvolvido em termos de governo eletrônico entre os países da América Latina e do Caribe (ONU, 2020), sendo um possível resultado do investimento do país em se desenvolver nessa

área (BIBLIOTECA DEL CONGRESO, 2019). O país também possui ações de segurança cibernética relacionadas com a educação nos níveis de graduação, pós-graduação e especialização disponíveis em suas universidades. Ademais, o Ministério da Educação chileno criou um programa chamado “Internet Segura”, que tem o objetivo de informar aos adultos sobre o uso da internet e suas ameaças para que possam acompanhar crianças e jovens no domínio cibernético, além de oferecer orientação às escolas primárias e secundárias através de uma perspectiva mais pedagógica, para que possam educar os cidadãos digitais do futuro (REPÚBLICA DE CHILE, 2022b).

4.4.1 Análise da securitização da Estratégia Nacional de Segurança Cibernética chilena

Na codificação da política cibernética do Chile, surgem preocupações com tipos de delitos bem diferentes das apresentadas pelo Brasil. Conforme o quadro 13, existe uma preocupação com a correta atribuição dos ataques, que é importante para saber se um ataque é realizado por um indivíduo ou uma nação, bem como a importância dada à espionagem industrial, *ransomware*, interrupção de serviço, roubo de propriedade intelectual e fraude, sem esquecer da possibilidade de desenvolver mais conhecimento e experiência em crimes digitais. No que se refere à perspectiva da securitização, a política cita a possibilidade das ameaças cibernéticas disparadas por outros Estados, sendo esse talvez o motivo para verificar-se uma elevada codificação sobre dissuasão e espionagem cibernéticas no documento. Além disso, o país faz uso do discurso de que a soberania nacional precisa ser garantida, também, por meio do ciberespaço.

Quadro 13 - Codificações de securitização encontradas na estratégia do Chile

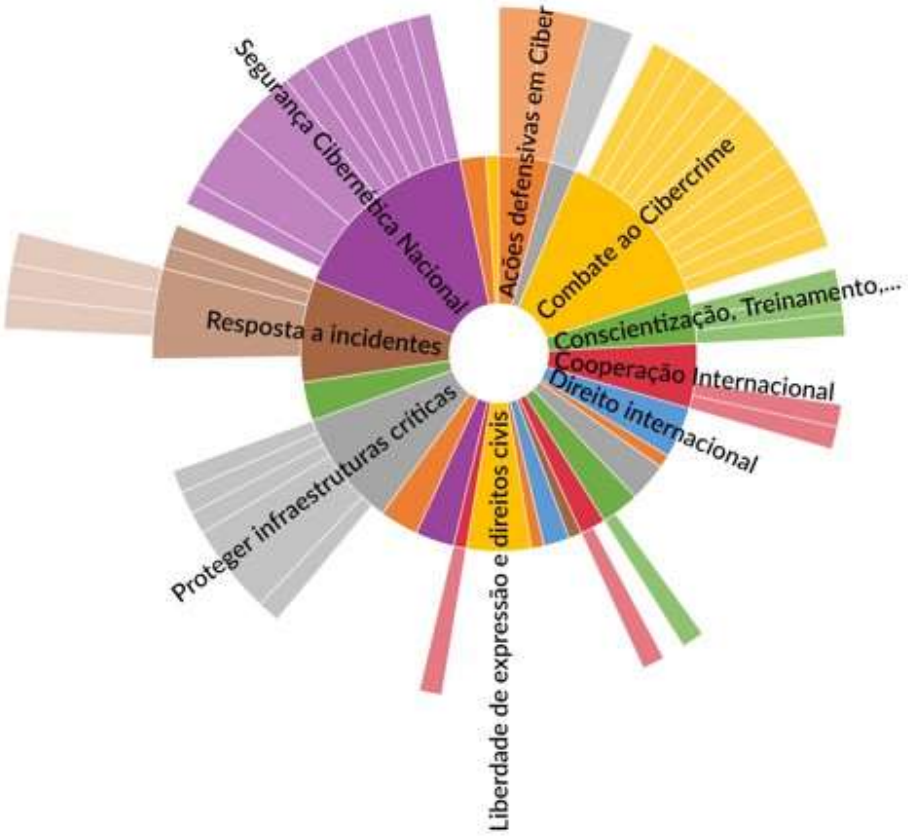
CATEGORIAS E SUBCATEGORIAS	CHILE
2: Ações ofensivas no ciberespaço	-
2.2: Ameaças de ataque cibernético	4%
4: Combate ao Cibercrime	11%
4.2: Ameaças cibernéticas	3%
4.4: Ataque DDoS	1%
4.5: Atribuição de ataques	15%
4.10: Desenvolver conhecimento e experiência em cibercrimes	5%
4.12: Espionagem industrial	2%

4.15: Fraude	2%
4.17: Interrupção de serviços	2%
4.23: Ransomware	1%
4.24: Roubo de propriedade intelectual	1%
10: Dissuasão cibernética	8%
11: Espionagem cibernética	18%
34: Garantia da soberania nacional	23%

Fonte: Elaborado com dados extraídos através da ferramenta Nvivo

Em relação a todas as codificações realizadas na estratégia cibernética do Chile, a Figura 19 mostra uma grande relevância para a liberdade de expressão e os direitos civis. No entanto, suas ações também estão na segurança cibernética nacional, proteção das infraestruturas críticas, resposta a incidentes, combate ao cibercrime e cooperação internacional.

Figura 19 - Representação gráfica das ações de cibersegurança do Chile

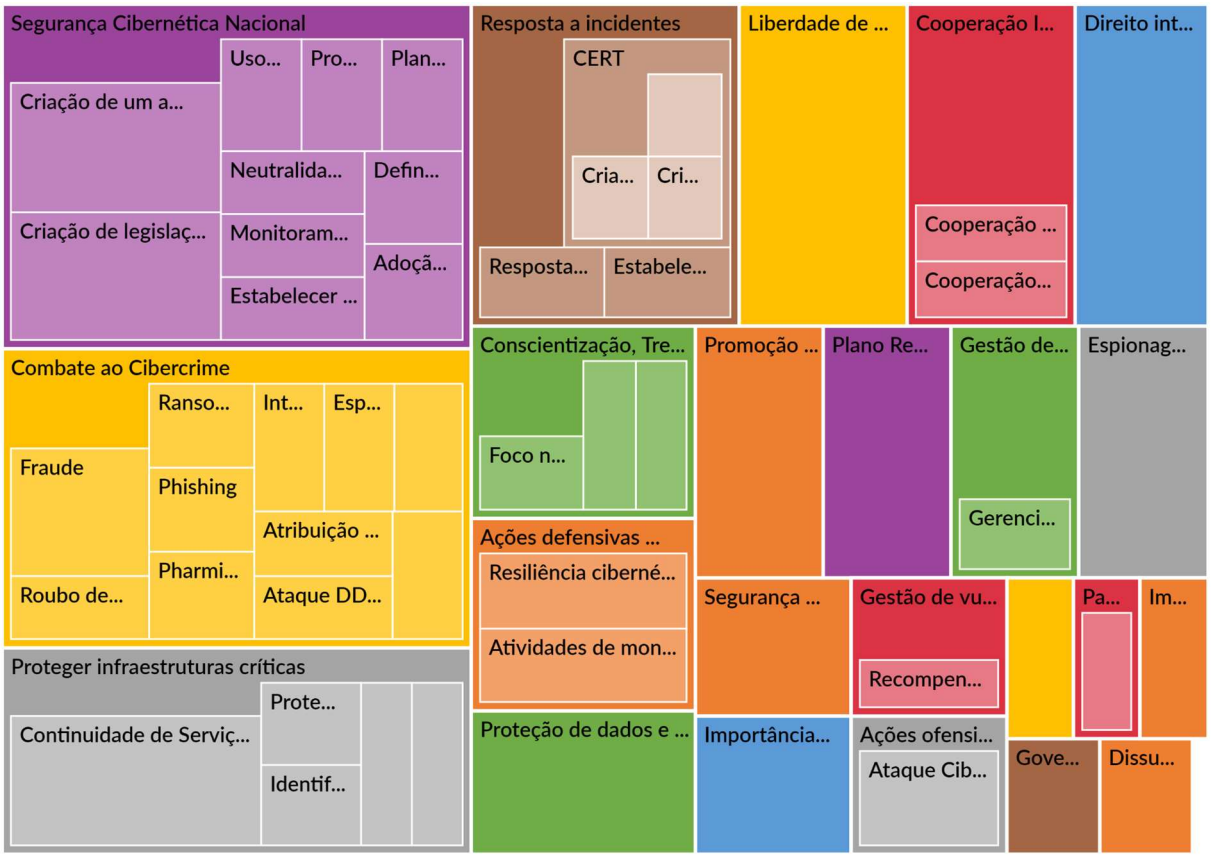


Fonte: Elaborado pelo autor através da ferramenta Nvivo

Na representação das ações apresentada na Figura 20, pode-se destacar o objetivo do país de criar um centro de tratamento de incidentes específico para infraestruturas críticas, de

pensar em um plano de continuidade de serviços críticos nacionais, bem como um plano de recuperação em casos de ataques. Além disso, o Chile tem planos para a promoção de uma indústria de cibersegurança no país e, para isso, tem objetivos para melhorar a capacitação universitária em segurança cibernética.

Figura 20 - Representação das ações do Chile em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Em uma última análise sobre a estratégia cibernética nacional do Chile, o ANEXO C mostra que *framework* da OTAN é aquele com o qual as ações de proteção do domínio cibernético do país mais se assemelham. Dessa forma, a pesquisa retornou que existem 27 pontos de convergência entre a estratégia do Chile com o *framework* da ENISA, 24 com o do ITU, 17 com o NIST, 17 com o da OEA e 28 códigos convergentes com o modelo da OTAN.

4.5 COLÔMBIA

Em 2011, a Colômbia lançou sua primeira política nacional de cibersegurança intitulada *Lineamientos de Política para Ciberseguridad y Ciberdefensa*, com a finalidade de propor os objetivos para o fortalecimento da capacidade do Estado para responder às ameaças de

segurança e defesa cibernéticas no país (REPÚBLICA DE COLOMBIA, 2011). Em 2016, o país publicou sua nova política de segurança cibernética, a *Política Nacional de Seguridad Digital*, visando fortalecer ainda mais as capacidades de todas as áreas interessadas para identificar, gerenciar, tratar e mitigar riscos de cibersegurança (REPÚBLICA DE COLOMBIA, 2016). Essa política criou o papel do Coordenador Nacional de Segurança Digital, que trabalha junto ao Presidente da República, bem como montou o Comitê de Cibersegurança, que é responsável por tratar das questões intersetoriais do tema, sendo comandado pelo Coordenador Nacional (REPÚBLICA DE COLOMBIA, 2016).

Além disso, o governo inclui a política de cibersegurança como parte integrante de suas políticas de gestão e desempenho, fazendo com que a temática da segurança cibernética participe da operação estratégica de entidades públicas e privadas (REPÚBLICA DE COLOMBIA, 2016). Através do Ministério da Tecnologia e Comunicações, a Colômbia implantou um programa de privacidade de informações em nível nacional para apoiar ações de gestão de risco e boas práticas para proteção de ativos críticos de informações (OEA, 2020). O país também criou uma equipe nacional de resposta a incidentes de computadores, colCERT, sob o comando do Ministério da Defesa Nacional, que também atua na proteção da infraestrutura crítica cibernética nacional (REPÚBLICA DE COLOMBIA, 2016).

A função de proteção do domínio cibernético é desempenhada de forma colaborativa entre o Comando Cibernético Conjunto (CCOC), das Forças Armadas, o Centro Cibernético Policial (CCP), da Política Nacional, e também o CSIRT do governo, além da Procuradoria-Geral da República com a participação do setor privado e da cooperação de equipes de resposta de outros países (REPÚBLICA DE COLOMBIA, 2011). Caso seja detectado um incidente que possa levar a uma crise nacional, o colCERT comunica o Coordenador Nacional de Cibersegurança, que ativa o Comitê de Cibersegurança para gerenciar a crise (OEA, 2020).

Em relação ao marco regulatório do setor, o crime cibernético está coberto pela Lei 1273/2009, que modificou o código penal para incluir os delitos digitais (REPÚBLICA DE COLOMBIA, 2009). No que tange a proteção dos dados pessoais e da privacidade, a Colômbia promulgou a Lei 1581/2012, além de criar um escritório específico para tratar assuntos sobre dados pessoais (REPÚBLICA DE COLOMBIA, 2022). Outro ponto que deve ser destacado são as oportunidades de estudos em cibersegurança nos níveis de graduação e pós-graduação oferecidas pelo Ministério da Tecnologia da Informação e das Comunicações da Colômbia, que também concede bolsas de estudo para servidores públicos que trabalham com tecnologia da informação (OEA, 2020).

Por fim, em 2018, o Banco Interamericano de Desenvolvimento aprovou um projeto de

melhoria da conectividade e digitalização da economia, por meio de um empréstimo de US$ 350 milhões destinado à implementação de políticas para a proteção do domínio cibernético (BID, 2018). Sobre outras formas de cooperação, o país é membro da Interpol e da Europol (INTERPOL, 2022), além disso, em 2018, revisou sua legislação para se adequar à Convenção de Budapeste sobre Crimes Cibernéticos e teve sua adesão ao grupo efetivada em março de 2020 (CONSEIL DE L'EUROPE, 2020).

4.5.1 Análise da securitização da Estratégia Nacional de Segurança Cibernética colombiana

A codificação da estratégia cibernética da Colômbia traz uma forte preocupação com o crime cibernético. No quadro 14 são apresentadas ações como a criação de um centro de operação para combate ao crime cibernético e o estabelecimento de uma função policial para investigação de cibercrimes, estrutura que já existe no país. Entre os tipos de delitos destacados no documento a pornografia infantil é o que recebe maior destaque, seguido pelo *defacement*[44] e o *phishing*. No que tange ao objeto desta pesquisa, entre os países estudados, a Colômbia é o que apresenta mais itens inseridos no espectro da securitização cibernética, destacando-se a relevância dada à capacidade militar, uma vez que são as Forças Armadas que, também, realizam a proteção das infraestruturas críticas do país.

Além disso, são consideradas as ações de inteligência e contrainteligência e uma grande preocupação com o terrorismo cibernético, que, assim como no caso da Argentina, pode ser explicado pelo histórico de ações consideradas terroristas dentro de seu território, seja proveniente do narcotráfico ou através de ações de grupos revolucionários (EBC, 2021). Por fim, a Colômbia dá ênfase destacada ao discurso da garantia da soberania nacional por meio do ciberespaço, e traz para essa pesquisa a ideia do exercício de poder nesta dimensão, seja como líder do tema no continente ou pela demonstração de uma capacidade militar cibernética que possa desestimular possíveis ataques de seus adversários aos seus ativos críticos.

[44] Também conhecido como *deface*, consiste na realização de modificações na estética ou conteúdo de um site. Normalmente, o invasor não costuma acessar o banco de dados do site, nem mesmo derrubar o servidor, simplesmente deixa uma mensagem para os usuários e responsáveis, que se sobrepõe à estrutura original da página.

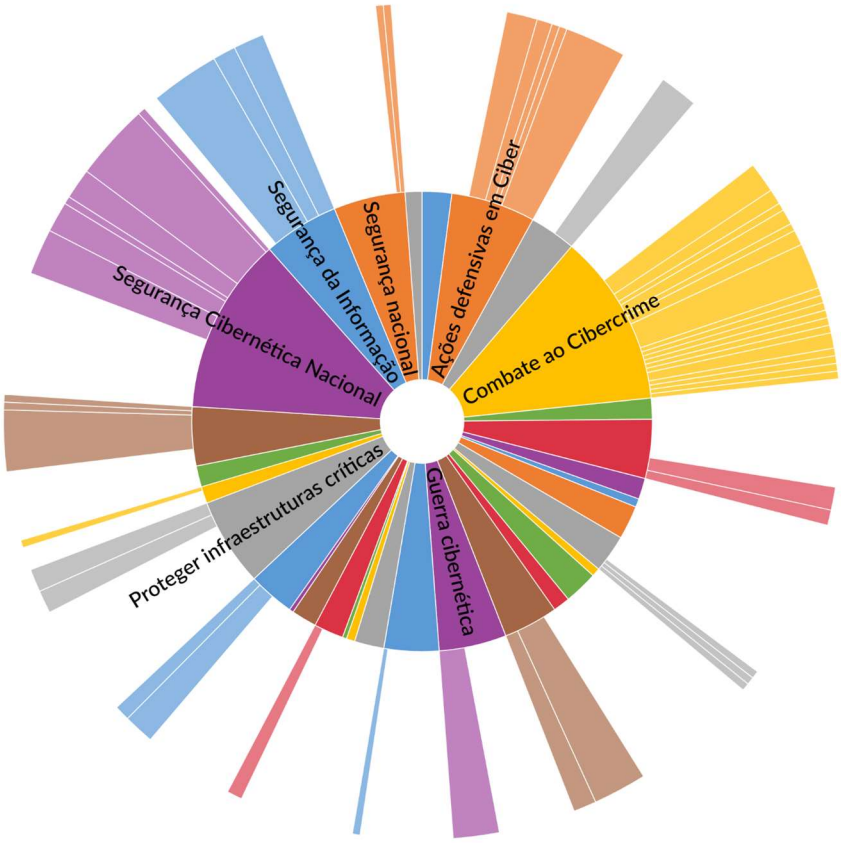
Quadro 14 - Codificações de securitização encontradas na estratégia da Colômbia

CATEGORIAS E SUBCATEGORIAS	COLÔMBIA
2: Ações ofensivas no ciberespaço	-
2.2: Ameaças de ataque cibernético	2%
4: Combate ao cibercrime	1%
4.8: Criação de um centro de operações de Seg. cibernética	3%
4.9: Defacement	1%
4.10: Desenvolver conhecimento e experiência em cibercrimes	9%
4.16: Função policial	6%
4.19: Phishing	1%
4.21: Pornografia infantil	5%
11: Espionagem cibernética	1%
12: Exercícios cibernéticos	2%
16: Guerra cibernética	-
16.1: Capacidade militar cibernética	6%
16.2: Criação de um comando cibernético	1%
19: Inteligência e Contrainteligência	3%
25: Poder nacional	-
25.1: Poder cibernético nacional	1%
28: Proteger infraestruturas críticas	14%
28.10: Uso militar para proteção de IC	10%
34: Garantia da soberania nacional	21%
34.1: Ameaça à Prosperidade	2%
35: Terrorismo cibernético	13%

Fonte: Elaborado com dados extraídos através da ferramenta Nvivo

Em relação à avaliação de toda a codificação da estratégia nacional da Colômbia, a Figura 21 apresenta, pela primeira vez entre os países estudados, a categoria da Guerra Cibernética, que envolve a capacidade cibernética militar e a criação de um comando militar para o ciberespaço (algo que o país já possui). Ainda, verifica-se a preocupação com as infraestruturas críticas, com combate ao cibercrime e com o cuidado com as áreas da segurança da informação, muito necessárias para a implantação de medidas técnicas e de gestão de projetos de segurança cibernética.

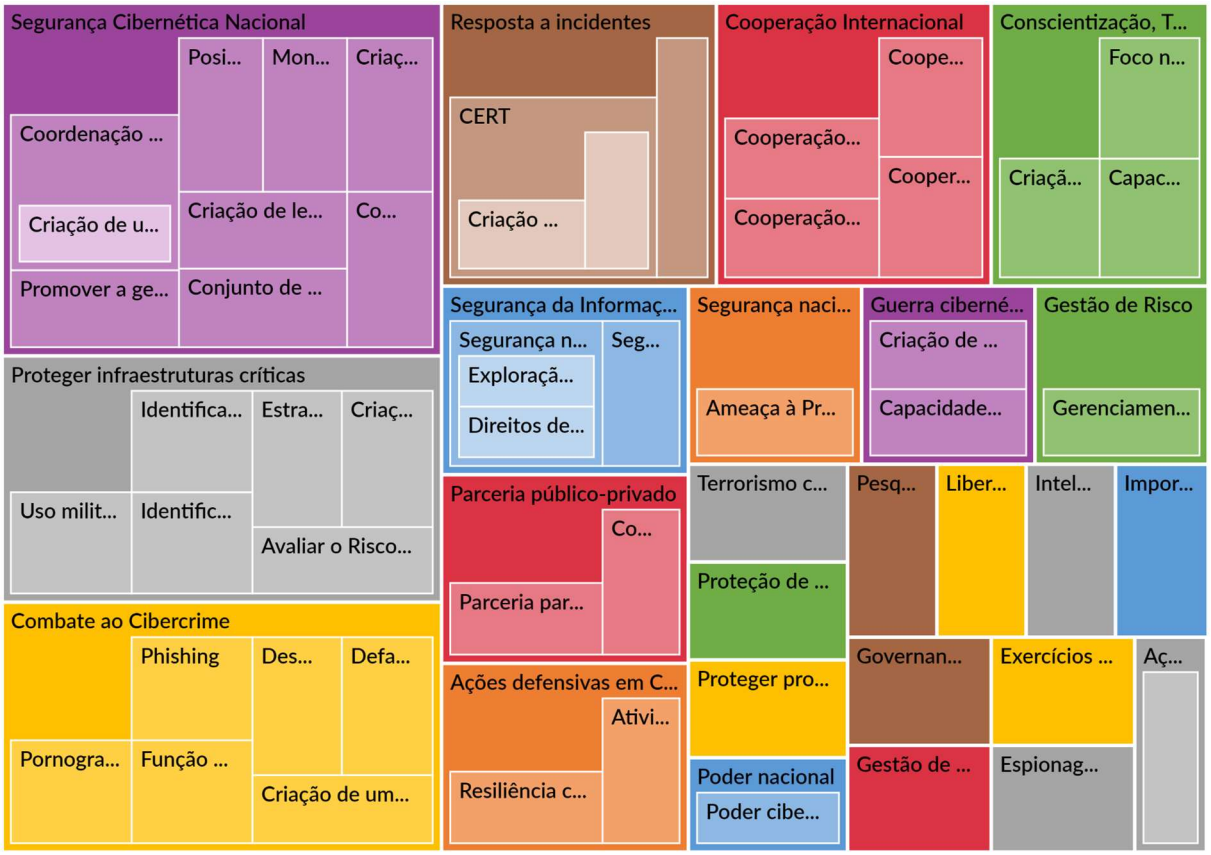
Figura 21 - Representação gráfica das ações de cibersegurança da Colômbia



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Na representação mais ampliada, Figura 22, nota-se um conjunto maior de ações para combate ao cibercrime, assim como uma tipificação maior de delitos digitais. Em seus objetivos de proteção do ciberespaço, a Colômbia tem em seus objetivos futuros - ou já utiliza - ações securitizadas, como a espionagem cibernética, inteligência e contrainteligência, entre outras, tendo sempre as Forças Armadas ocupando um papel de relevância nos projetos. Além disso, o país busca reforçar a cooperação internacional, tanto na sua região ou com países da Europa para aprofundar o combate aos crimes digitais.

Figura 22 - Representação das ações da Colômbia em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Em uma última análise sobre a estratégia cibernética nacional da Colômbia, o ANEXO D mostra que *framework* da OTAN é aquele com o qual as ações de proteção do domínio cibernético do país mais se assemelham. Dessa forma, a pesquisa retornou que existem 32 pontos de convergência entre a estratégia da Colômbia com o *framework* da ENISA, 29 com o do ITU, 14 com o NIST, 18 com o da OEA e 40 códigos são convergentes com o modelo da OTAN.

4.6 EQUADOR

Ainda sem possuir uma estratégia de segurança cibernética, desde 2016, o país fez avanços interessantes visando a melhoria de suas capacidades no ciberespaço. Uma delas foi, em 2021, a criação da *Política de Ciberseguridad*, com o objetivo de construir e fortalecer as capacidades nacionais que permitam garantir os direitos humanos e liberdades fundamentais da população no ciberespaço. Além disso, deve contribuir para aumentar a confiança, a resiliência e a responsabilidade compartilhada no desenvolvimento da proteção do domínio cibernético, fazendo dele um ambiente livre, aberto e seguro (REPÚBLICA DEL ECUADOR, 2021). A

Política tem como seus pilares a governança cibernética, a gestão de incidentes, a proteção das infraestruturas críticas e dos serviços essenciais à garantia da soberania e da defesa do ciberespaço, a diplomacia cibernética e a cooperação internacional, e o desenvolvimento de cultura e educação cibernéticas (REPÚBLICA DEL ECUADOR, 2021).

A prevenção, tratamento e resposta de incidentes cibernéticos do país é realizada pelo EcuCERT, o CSIRT nacional, que está sob o comando da Agência nacional de Regulação e Controle de Telecomunicações (*Agencia de Regulación y Control de las Telecomunicaciones*, ARCOTEL) (REPÚBLICA DEL ECUADOR, 2022). O EcuCERT participa do CSIRT Américas, beneficiando-se do intercâmbio de informações entre outros CSIRTs nacionais, policiais e de defesa que também são membros do projeto (CSIRT AMÉRICAS, 2022). Em relação à legislação nacional sobre crimes digitais, o Código Penal do Equador tem nos artigos 229 a 234 a tipificação e a forma de judicialização de delitos cibernéticos (REPÚBLICA DEL ECUADOR, 2015). Neste sentido, também há a lei que regula o comércio eletrônico e assinatura digitais (REPÚBLICA DEL ECUADOR, 2002), ainda não existindo, no entanto, um regulamento específico sobre a proteção dos dados pessoais e da privacidade.

4.6.1 Análise da securitização da Política Nacional de Segurança Cibernética do Equador

Entre todas as estratégias estudadas nessa pesquisa, a política equatoriana é a que apresenta no texto o maior número de tipificações de delitos digitais, conforme é mostrado no Quadro 15. Com destaque para a extorsão, o discurso de ódio, a mineração de *bitcoins* e o combate às *botnets*[45], crimes cibernéticos que não haviam sido reportados por nenhum outro país neste estudo. Entre os tipos de delitos mais comuns combatidos estão a pornografia infantil, a sabotagem de sistemas e fraudes, entre outros. Além disso, o país é um dos poucos dessa pesquisa que demonstra preocupação com o *ciberbullying.* Desta forma, o Equador dá foco ao combate ao cibercrime, possuindo, em sua política, projetos para desenvolver conhecimento e experiência para combater os delitos digitais, bem como estabelecer na força policial uma maior capacidade de investigar e processar esse tipo de delito.

No que se refere à securitização, objeto dessa dissertação, o Equador cita as ameaças de ataques cibernéticos entre países, por isso reforça o discurso da proteção cibernética como necessária para garantir a soberania nacional com crimes cibernéticos contra infraestruturas

[45] *Botnets* são uma série de dispositivos conectados à Internet sob controle de um invasor, formando uma rede que pode ser utilizada para executar crimes como ataques de negação de serviço, roubar dados, enviar spam, entre outros.

críticas e roubo da propriedade intelectual desenvolvida no país. No entanto, não existe, no texto da política nenhuma referência sobre preparar o Equador para realizar ataques cibernéticos ou responder em caso de agressão pelo ciberespaço. A política faz parte de uma série de ações do país para melhorar sua segurança cibernética, assim sendo, entre elas, projeta estabelecer uma área de inteligência e contrainteligência para apoiar a segurança cibernética, bem como combater a espionagem cibernética. Por fim, assim como Argentina e Colômbia, o Equador também demonstra preocupação com o terrorismo cibernético.

Quadro 15 - Codificações de securitização encontradas na estratégia do Equador

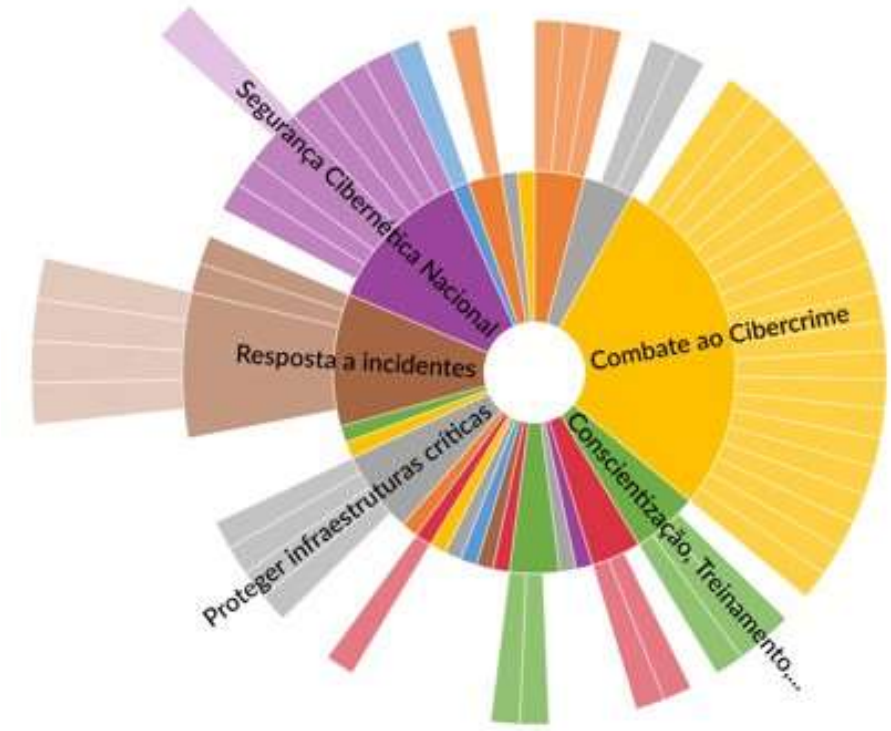
CATEGORIAS E SUBCATEGORIAS	EQUADOR
1: Ações ofensivas no ciberespaço	3%
1.1: Agressão entre Estados	3%
1.2: Ameaças de Ataque Cibernético	5%
4: Combate ao Cibercrime	13%
4.2: Ameaças de ataque cibernético	3%
4.4: Ataque DDoS	3%
4.5: Atribuição de ataques	2%
4.6: Ciberbullying	2%
4.10: Desenvolver conhecimento e experiência em cibercrimes	4%
4.11: Disseminação de malware	2%
4.15: Fraude	4%
4.16: Função policial	1%
4.20: Pirataria	1%
4.21: Pornografia infantil	2%
4.25: Sabotagem de sistemas	4%
4.26: Spam	1%
4.27: Vazamento de dados	1%
4.29: Botnet	1%
4.30: Discurso de ódio	1%
4.31: Exposição de conteúdo impróprio	1%
4.32: Extorsão	2%
4.33: Mineração de bitcoins	1%
4.34: Ataques baseados na web	2%
11: Espionagem cibernética	6%

19: Inteligência e Contrainteligência	2%
34: Garantia da soberania nacional	10%
35: Terrorismo cibernético	5%

Fonte: Elaborado com dados extraídos através da ferramenta Nvivo

Em relação à avaliação de toda a codificação da política nacional de cibersegurança do Equador, a Figura 23, que exibe as categorias em diferentes graus de intensidade, mostra que o combate ao cibercrime tem a maior relevância para o país, seguido pelas iniciativas para o estabelecimento de uma estrutura nacional de segurança cibernética (*Segurança Cibernética Nacional*), bem como de ações para responder a incidentes cibernéticos.

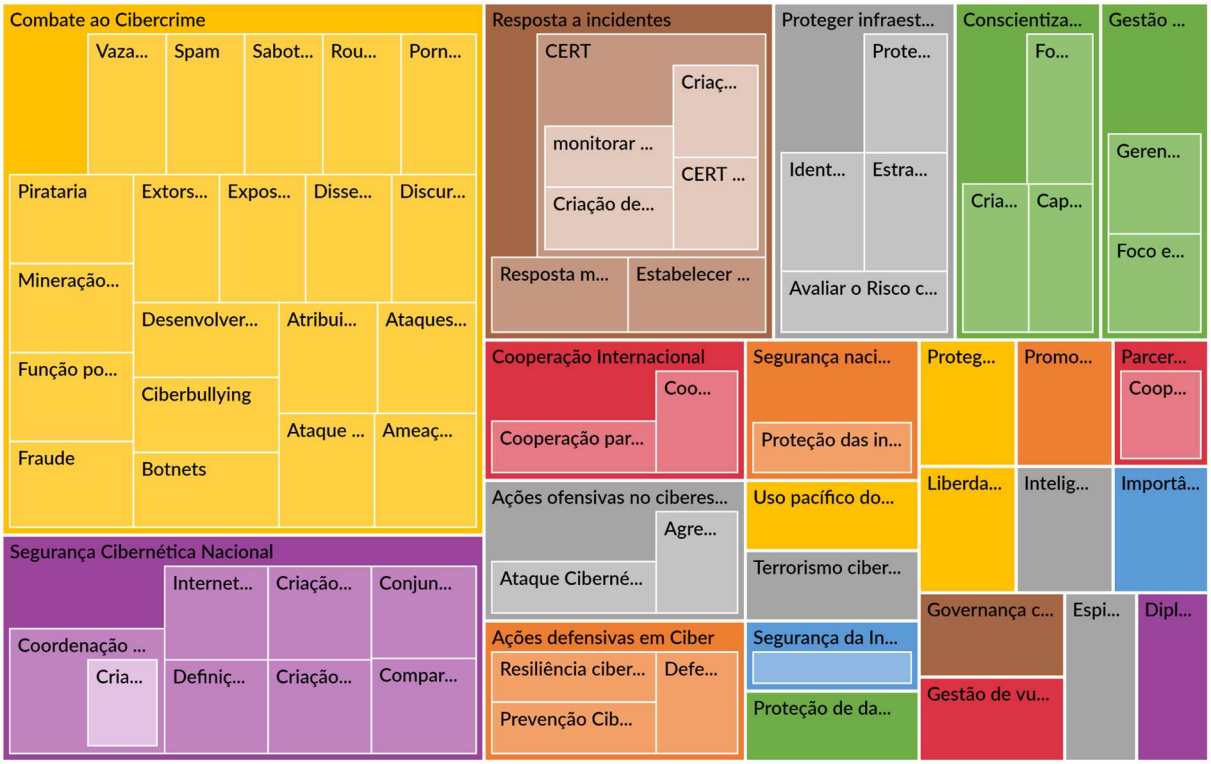
Figura 23 - Representação gráfica das ações de cibersegurança do Equador



Fonte: Elaborado pelo autor através da ferramenta Nvivo

O foco no combate ao cibercrime fica mais visível na Figura 24, em que são descritos os tipos de crimes digitais encontrados no processo de codificação da política do Equador. Mesmo se tratando de uma política que descreve ações futuras para estabelecer a segurança nacional cibernética, o documento já possui objetivos de atuação em diferentes categorias, como proteção de infraestruturas críticas, cooperação internacional, conscientização da população, estabelecimento de ações defensivas, diplomacia cibernética, entre outras.

Figura 24 - Representação das ações do Equador em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Em uma última análise sobre a estratégia cibernética nacional do Equador, o ANEXO E mostra que o *framework* da OTAN é aquele com o qual as ações de proteção do domínio cibernético do país mais se assemelham. Dessa forma, a pesquisa retornou que existem 31 pontos de convergência entre a estratégia do Equador com o *framework* da ENISA, 28 com o do ITU, 14 com o NIST, 16 com o da OEA e 40 códigos são convergentes com o modelo da OTAN.

4.7 PARAGUAI

O Paraguai aprovou seu *Plan Nacional de Ciberseguridad* em 2017, com o objetivo de adotar medidas de segurança cibernética para garantir e promover o uso seguro e confiável da tecnologia da informação, bem como incentivar o progresso e a inovação no país. Além disso, o plano também criou uma Comissão Nacional de Cibersegurança para coordenar esses esforços no país (REPÚBLICA DEL PARAGUAY, 2017). O Plano de Cibersegurança define sete objetivos a serem alcançados, que são: consciência e cultura cibernética; pesquisa, desenvolvimento e inovação; proteção da infraestrutura crítica; capacidade de responder a incidentes cibernéticos; capacidade de investigar e processar o cibercrime; modernização e

proteção da administração pública; e, estabelecer um sistema nacional de cibersegurança (REPÚBLICA DEL PARAGUAY, 2017).

O plano também define a necessidade da proteção das infraestruturas críticas, descrevendo-as como sistemas ativos, físicos ou virtuais, essenciais para a manutenção de funções sociais vitais - como saúde, integridade física, segurança, bem-estar social e econômico da população - cuja interrupção ou destruição provocaria um impacto debilitante na segurança nacional (REPÚBLICA DEL PARAGUAY, 2017). Para atingir esses objetivos de proteção no domínio cibernético, em 2018, o país criou o Ministério de Tecnologia da Informação e Comunicações (MITIC), no qual a segurança cibernética foi estabelecida como um eixo estratégico. Entre as funções do MITIC estão a construção de um ecossistema digital seguro, confiável e resiliente; o estabelecimento de políticas de proteção de informações pessoais e de governo; a criação de planos e estratégias de cibersegurança em nível nacional; a definição de uma autoridade em cibersegurança e controle de incidentes no país; e, a proteção da infraestrutura crítica tecnológica (REPÚBLICA DEL PARAGUAY, 2018).

Em relação ao arcabouço legal para cibersegurança, em 2011, através da Lei 4.439/2011, o país modificou o Código Penal, inserindo condutas ilegais de cibercrime realizadas através do uso da tecnologia da informação (REPÚBLICA DEL PARAGUAY, 2011). No que tange a proteção dos dados pessoais e da privacidade, o Paraguai possui a Lei 1.682/2001, que trata de regulamentar a coleta, o armazenamento, o processamento e a publicação de dados ou características pessoais (REPÚBLICA DEL PARAGUAY, 2011a). Ademais, em 2017, através da Lei 5.994/2017, o país aderiu à Convenção de Budapeste sobre Crimes Cibernéticos, bem como ao seu protocolo adicional, que tem como objetivo principal buscar desenvolver uma política criminal comum que proteja a sociedade contra o crime cibernético, por meio de uma legislação adequada e da promoção da cooperação internacional (CONSEIL DE L'EUROPE, 2001).

Como parte integrante desta convenção, o Paraguai é beneficiário do programa *GLACY+*, uma ação global sobre crimes cibernéticos, realizada pelo Conselho da Europa em conjunto com a União Europeia, com a finalidade de apoiar os países membros na implementação da convenção à legislação nacional, através da capacitação de oficiais de justiça e de cooperação jurídica internacional para combate ao cibercrime (OEA, 2020). Além disso, como outras medidas de combate, o Paraguai possui uma unidade especializada em crimes cibernéticos em seu Ministério Público, bem como unidades penais especializadas em crimes eletrônicos (REPÚBLICA DEL PARAGUAY, 2022). Por sua vez, a Polícia Nacional do país também possui uma dvisão especializada que atua em conjunto com o Ministério Público

(REPÚBLICA DEL PARAGUAY, 2020).

4.7.1 Análise da securitização da Estratégia Nacional de Segurança Cibernética do Paraguai

No que se refere ao objeto de estudo dessa pesquisa, o Paraguai apresenta apenas a categoria Espionagem Cibernética dentro do espectro da securitização, conforme quadro 16. Entretanto, os dados apontam grande relevância para o aspecto do combate ao cibercrime, que é realizado dentro do espectro político pela força policial. Assim sendo, a codificação do documento encontrou um elevado número de tipos de delitos que preocupam as autoridades - dos mais comuns, como fraude, *phishing*, *defacement*, sabotagem de sistemas, entre outros, até crimes considerados mais graves no país, como a pornografia infantil (que recebe muito destaque) e a exploração de crianças na internet. Além disso, assim como o Equador, é um dos países estudados que cita em sua estratégia a necessidade do combate ao *cyberbullying*, utilizando-se de campanhas de conscientização para isso.

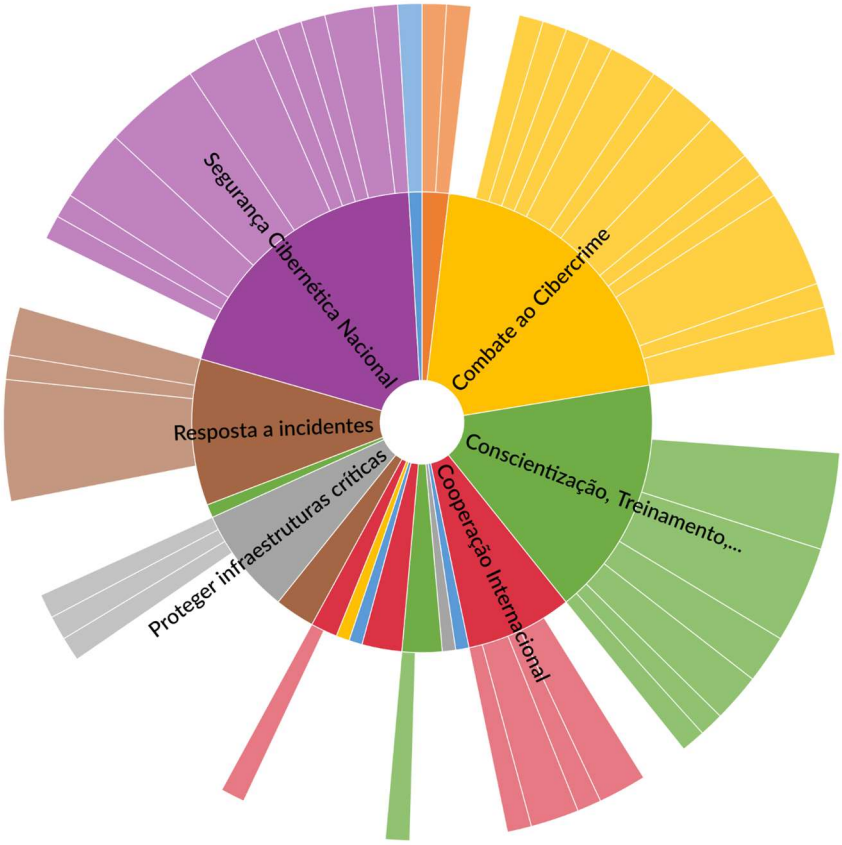
Quadro 16 - Codificações de securitização encontradas na estratégia do Paraguai

CATEGORIAS E SUBCATEGORIAS	PARAGUAI
4: Combate ao Cibercrime	9%
4.1: Acesso ilegal às informações em computadores, sistemas e redes	2%
4.4: Ataque DDoS	2%
4.6: Ciberbullying	3%
4.9: Defacement	2%
4.10: Desenvolver conhecimento e experiência em cibercrimes	5%
4.13: Exploração de crianças na Internet	4%
4.15: Fraude	4%
4.16: Função policial	15%
4.17: Interrupção de serviços	1%
4.19: Phishing	1%
4.21: Pornografia infantil	20%
4.25: Sabotagem de sistemas	1%
4.27: Vazamento de dados	3%
11: Espionagem cibernética	6%

Fonte: Elaborado com dados extraídos através da ferramenta Nvivo

Em relação à análise de toda a codificação da estratégia cibernética nacional do Paraguai, a Figura 25 apresenta um país muito preocupado com a questão dos crimes cibernéticos, bem como dá muita importância para a conscientização e educação da população. Além disso, considera importante a cooperação internacional para combate ao cibercrime, na qual já possui parcerias de colaboração e troca de informações com países europeus.

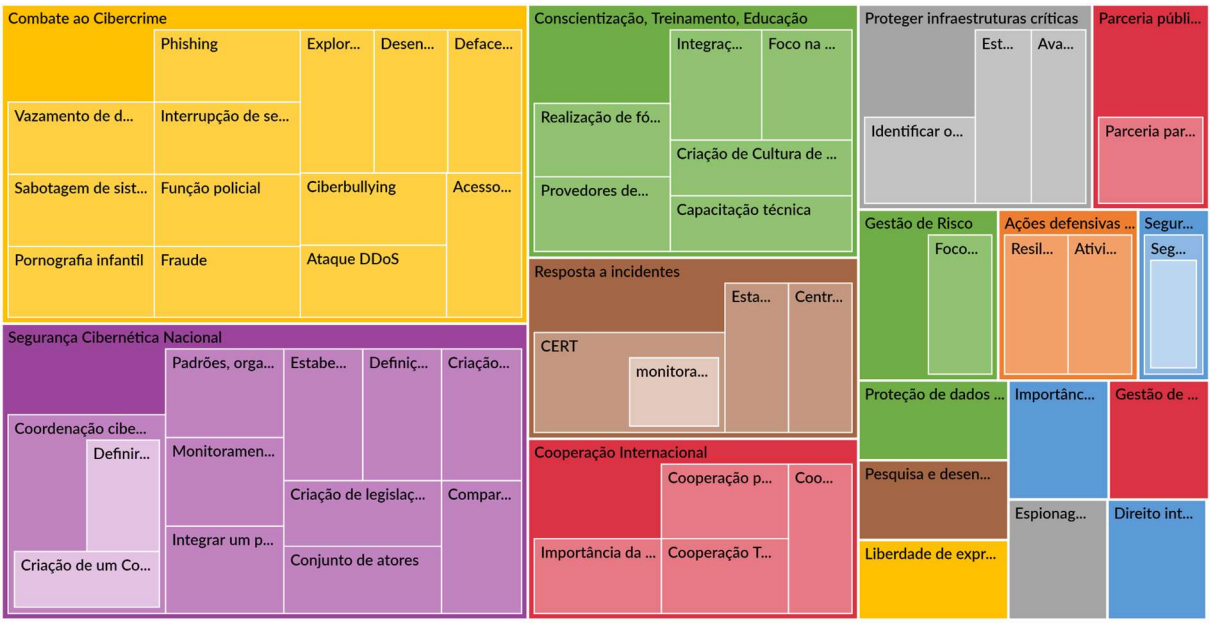
Figura 25 - Representação gráfica das ações de cibersegurança do Paraguai



Fonte: Elaborado pelo autor através da ferramenta Nvivo

A Figura 26, que oferece uma representação mais abrangente, mostra que as ações/preocupações com o crime cibernético são relevantes, ficando à frente de outras iniciativas como a Segurança Cibernética Nacional. Além disso, apresenta categorias interessantes como o Direito Internacional e a Liberdade de Expressão e Direitos Humanos, bem como uma série de itens relativos à conscientização dos usuários, como a necessidade dos provedores de acesso trabalharem cultura cibernética com os clientes, foco na capacitação de universitários e na educação fundamental para segurança cibernética.

Figura 26 - Representação das ações do Paraguai em formato de Mapa de Árvore



Fonte: Elaborado pelo autor através da ferramenta Nvivo

Em uma última análise sobre a estratégia cibernética nacional do Paraguai, o ANEXO F mostra que os *frameworks* da ENISA e da OTAN apresentam o mesmo número de codificações entre suas ações de proteção com o documento paraguaio. Dessa forma, a pesquisa retornou que existem 32 pontos de convergência entre a estratégia do Chile com o *framework* da ENISA, 27 com o do ITU, 12 com o NIST, 17 com o da OEA e 32 códigos são convergentes com o modelo da OTAN.

4.8 ANÁLISE DAS POLÍTICAS DOS PAÍSES

A partir daqui são elencadas as ações dos países que ainda não possuem uma estratégia ou política nacional de segurança cibernética. Pelo fato de não terem sido submetidas à análise da Teoria Fundamentada, não é possível fazer a correlação com os *frameworks* que outras informações como gráficos, por exemplo.

4.8.1 Bolívia

Em 2017, o país aprovou uma lei que declara como uma prioridade o desenvolvimento de uma estratégia nacional de segurança cibernética (BOLÍVIA, 2017). Ademais, em 2015, a Bolívia criou a Agência Nacional de Tecnologias da Informação e Comunicação (AGETIC), com a finalidade de desenvolver ações para a transformação da gestão pública para o governo

eletrônico, bem como promover a soberania tecnológica e científica do Estado (BOLÍVIA, 2015). Através do Decreto 2514/2015, foi criado o Centro de Gestão de Assuntos Cibernéticos (CGII), cuja missão é proteger as informações críticas do Estado e promover campanhas de conscientização sobre cibersegurança, bem como responder a incidentes de segurança cibernética (BOLÍVIA, 2015a). O CGII também faz parte do CSIRT Américas (CSIRT AMÉRICAS, 2022). No que se refere à legislação para crimes cibernéticos, a Bolívia não possui uma legislação própria para o tema, nem mesmo para a proteção de dados pessoais.

4.8.2 Guiana

Em 2019, sob orientação da Organização dos Estados Americanos, o país criou um grupo de trabalho para elaborar uma estratégia nacional de segurança cibernética (OEA, 2020). No entanto, a Guiana possui iniciativas como a criação de um CSIRT nacional (CIRT.GY), com a missão de responder aos incidentes cibernéticos disparados contra o país, através de medidas proativas de segurança e do compartilhamento de informações sobre ameaças, além de oferecer serviços aos setores público e privado do país (GUIANA, 2022). O CIRT.GY é um membro integrante do CSIRT Américas e, também, possui acordos de cooperação com CSIRTs de outros países como Colômbia, Estônia e Holanda (OEA, 2020).

Em relação ao crime cibernético, em 2016, a Força Policial da Guiana abriu um centro de cibersegurança com a finalidade de treinar a polícia, bem como o setor privado e o público sobre como responder ao cibercrime (GUIANA, 2019). Em 2019, a Força Policial do país estabeleceu de maneira formal uma unidade para investigar e processar crimes cibernéticos, bem como promulgou uma legislação abrangente sobre uma série de cibercrimes e seus métodos de execução. A despeito disso, a Guiana ainda não possui uma lei para proteção dos dados pessoais e da privacidade (GUIANA, 2016). Por fim, o país possui acordos de capacitação na área cibernética com o Reino Unido, bem como um acordo bilateral com o Governo da Índia, que provê um curso de pós-graduação em Segurança de Rede voltado para o setor público do país sul-americano (ORGANIZATION OF AMERICAN STATES, 2020).

4.8.3 Peru

Desde maio de 2021, está em desenvolvimento no país a *Estrategia Nacional de Seguridad y Confianza Digital*, que terá como missão desenvolver os eixos estratégicos e os objetivos nacionais para a proteção do domínio cibernético peruano (REPÚBLICA DEL PERU,

2021). No entanto, no site do Congresso peruano é encontrada uma *Política Nacional de Ciberseguridad*, que destaca a necessidade da criação de um comitê nacional de cibersegurança, bem como ações para investigação e judicialização dos crimes cibernéticos, além do desenvolvimento de planos de conscientização em segurança cibernética e de acordos de cooperação, entre outras ações, no entanto ainda não foi sancionado e, tampouco, existe alguma informação sobre os próximos passos do documento (REPÚBLICA DEL PERU, 2020).

Por meio da Lei 30.618/2017, o país definiu a segurança cibernética como prioridade para que se garanta um ambiente de confiança no meio digital, diante de ameaças que possam afetar as capacidades nacionais (REPÚBLICA DEL PERU, 2017). Assim sendo, define igualmente a necessidade da aplicação de medidas de gestão de riscos, bem como de capacidades de defesa cibernética para a proteção dos objetivos estatais no ciberespaço. Além disso, também fica estabelecida uma modificação no setor de inteligência do país, para que a Direção Nacional de Inteligência (DINI) seja o órgão responsável pela realização de atividades que visem alcançar a segurança cibernética peruana (REPÚBLICA DEL PERU, 2017).

Em 2019, foi sancionada a Lei 30.999/2019, que tem por objetivo estabelecer um marco normativo em matéria de defesa cibernética do Estado, regulando as operações militares no ciberespaço (REPÚBLICA DEL PERU, 2019). Também fica definido que é tarefa das Forças Armadas a proteção das infraestruturas críticas peruanas, bem como a defesa da soberania nacional mediante ataques por meio do domínio cibernético, quando a capacidade de proteção dos operadores dessas infraestruturas e da DINI forem ultrapassadas (REPÚBLICA DEL PERU, 2019). A lei também cita que devem ser desenvolvidos currículos de educação em matéria de ciberdefesa no nível superior, ensino tecnológico e pós-graduação.

Por fim, o PeCERT, que é membro do CSIRT Américas, é o CSIRT nacional do país, com a missão de coordenar a prevenção, o tratamento e a resposta a incidentes de segurança cibernética de instituições públicas, além de desenvolver ferramentas e estratégias para atender às necessidades de segurança da informação do governo peruano (REPÚBLICA DEL PERU, 2021b). Tal ação é considerada de grande relevância, uma vez que o Peru tem a intenção de promover um marco de governança em governo eletrônico, com destaque para áreas como a identidade digital e a prestação de serviços digitais pela administração pública, bem como para incentivar a inovação e a economia digital com foco no país (REPÚBLICA DEL PERU, 2018).

4.8.4 Suriname

O país ainda não possui estratégia nacional de segurança cibernética, estando,

entretanto, em processo de articular uma desde 2014, em colaboração com a Organização dos Estados Americanos (ORGANIZATION OF AMERICAN STATES, 2014a). Outro projeto em andamento é a criação de um CSIRT, pois o Suriname também não possui uma organização para resposta a incidentes em nível nacional (ORGANIZATION OF AMERICAN STATES, 2020). Segundo o relatório *Cybersecurity, Risk, Progress, and the Way Forward in Latin America and the Caribbean*, da Organização dos Estados Americanos (2020), devido ao aumento de ataques cibernéticos e do cibercrime, desde 2019, o Governo do Suriname criou o Comitê Nacional de Cibersegurança para que seja estabelecido um plano estratégico de segurança cibernética, bem como para que seja criado um CSIRT Nacional.

4.8.5 Uruguai

Embora ainda não possua uma estratégia nacional de segurança cibernética, o Uruguai tem uma estrutura de cibersegurança que está organizada em um documento chamado *Marco de Ciberseguridad*, que possui referências às normas internacionais que são aplicadas para o aprimoramento da proteção do domínio cibernético, como também das infraestruturas críticas (REPÚBLICA ORIENTAL DEL URUGUAY, 2019). O Uruguai foi o primeiro país da América do Sul a receber apoio técnico e financeiro do BID, por meio de um empréstimo, para projetos de fortalecimento da segurança cibernética nacional (BANCO INTERAMERICANO DE DESARROLLO, 2019).

Por meio da Agência para Desenvolvimento do Governo de Gestão Eletrônica e da Sociedade da Informação e do Conhecimento *Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento*, AGESIC), o país recebeu conselhos técnicos do BID para a implantação de um Centro Nacional de Treinamento em Segurança Cibernética (OEA, 2020). Por sua vez, a AGESIC coordena o CERTuy, que é o CSIRT nacional, que também faz parte da iniciativa colaborativa CSIRT Américas (REPÚBLICA ORIENTAL DEL URUGUAY, 2022). No que tange a proteção das infraestruturas críticas, essa missão recai sobre o D-CSIRT, que se trata de um CSIRT do Ministério da Defesa, focado em desenvolver capacidades de prevenção e detecção de incidentes de segurança cibernética nos ativos críticos mais importantes do país, em colaboração com o CERTuy (REPÚBLICA ORIENTAL DEL URUGUAY, 2015).

No que se refere ao arcabouço legal sobre cibersegurança, o Uruguai possui, desde 2008, uma legislação para proteção de dados pessoais e privacidade, a Lei 18.331/2008 (REPÚBLICA ORIENTAL DEL URUGUAY, 2008). No entanto, o país possui apenas projetos de lei para a

tipificação e judicialização dos crimes cibernéticos (TAQUE, 2021) (REPÚBLICA ORIENTAL DEL URUGUAY, 2021). Por fim, o Uruguai possui um projeto de governo eletrônico chamado de “Agenda Digital 2020”, que tem como objetivo levar inovação na prestação dos serviços públicos uruguaios (REPÚBLICA ORIENTAL DEL URUGUAY, 2020).

4.8.6 Venezuela

Apesar de não possuir uma estratégia nacional de segurança cibernética, o país mantém um Sistema Nacional de Segurança da Informação, que é gerenciado pela Superintendência de Serviços de Certificação Eletrônica (*Superintendencia de Servicios de Certificación Electrónica*, SUSCERTE), que presta serviços de fornecimento de certificados e assinaturas digitais. Além disso, tem a responsabilidade de proteger autenticidade, integridade, inviolabilidade e confiabilidade dos dados, informações e documentos eletrônicos obtidos e gerados pelo poder público, bem como ser a referência em termos de segurança cibernética nos ativos críticos da Venezuela (REPÚBLICA BOLIVARIANA DE VENEZUELA, 2022).

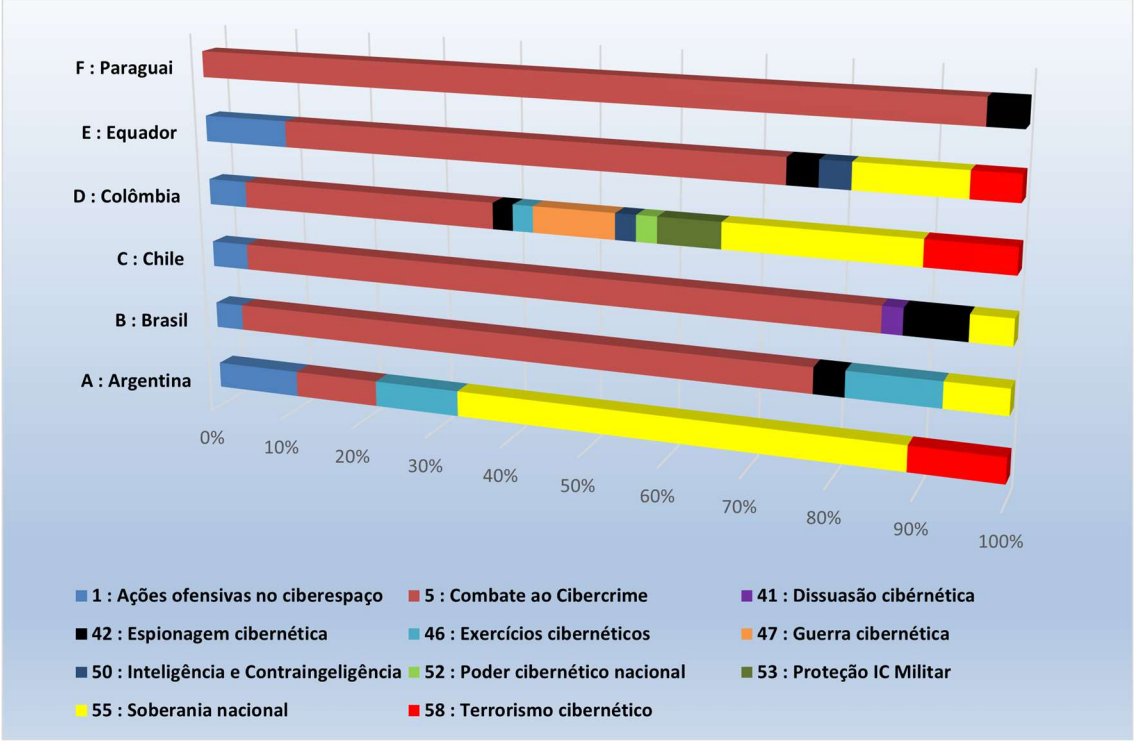
Sob a liderança do SUSCERTE está o CSIRT nacional, o VenCERT, com a finalidade de gerenciar o Sistema Nacional de Gestão de Incidentes Telemáticos, com as ações de prevenir, detectar e gerenciar os incidentes de segurança da informação do Estado, além daqueles que possam atacar a infraestrutura crítica do país (REPÚBLICA BOLIVARIANA DE VENEZUELA, 2015). Em relação ao marco regulatório sobre crimes cibernéticos, em 2001, a Venezuela aprovou a Lei Especial Contra os Crimes Informáticos, com a intenção de promover a proteção de sistemas de tecnologia da informação, tipificando os delitos cibernéticos, bem como as punições para os crimes (REPÚBLICA BOLIVARIANA DE VENEZUELA, 2014). O país, contudo, ainda não conta com uma legislação sobre proteção de dados e da privacidade.

4.9 SÍNTESE DO CAPÍTULO

Este capítulo tratou de apresentar o resultado das codificações que as estratégias dos países foram submetidas, além disso elenca as ações que vêm sendo desenvolvidas por aqueles que ainda não possuem ou que estão elaborando suas estratégias. Entre os países que possuem estratégia cibernética nacional, a maioria tem no combate ao cibercrime o maior desafio, conforme exibido na figura 27. Entre os países com mais ações securitizadas apontadas nesse trabalho, a Colômbia é a que mais se destaca, uma das causas prováveis para isso pode ser a

aliança com os Estados Unidos para o combate ao narcotráfico. No entanto, mesmo com a adoção de algumas práticas securitizadas por alguns países, não foi possível identificar um movimento de securitização e dessecuritização cibernética na região, consequentemente, também não foi identificado um Complexo Regional de Segurança por meio do viés da segurança cibernética.

Figura 27 - Resumo das ações securitizadas por país



Fonte: Elaborado pelo autor com dados extraídos por meio da ferramenta Nvivo

5 CONCLUSÃO

Este trabalho buscou analisar se os países da América do Sul passam por um processo de securitização em suas ações para combater o cibercrime. Esses países foram escolhidos pela proximidade geográfica e por suas características semelhantes (aspectos sociais, históricos, políticos e econômicos). Assim sendo, além de analisá-los sob a perspectiva da Teoria da Securitização, a pesquisa também procurou entender se teoria dos Complexos Regionais de Segurança (de Buzan e Waever) pode ser verificada na região através do viés das ações nacionais de segurança cibernética adotadas por esses países. Para isso, a dissertação partiu da hipótese de que apesar de compartilharem diversas características semelhantes, nem todos os países da região implementam ações securitizadas para promover sua defesa contra o crime cibernético, não sendo, portanto, possível verificar um mesmo padrão de securitização na região - ou seja, não sendo a questão do cibercrime um elemento que contribua para a formação de um CRS na região.

A cada vez maior sofisticação das ameaças cibernéticas, combinada com a informatização crescente dos sistemas de governos, bem como das infraestruturas críticas, despertou nos países a necessidade de proteção de seus ativos mais importantes no ciberespaço, a fim de proteger sua soberania. A descoberta do vírus *Stuxnet*, em 2010, que, pela complexidade, foi provavelmente desenvolvido por alguma nação, confirmou a suspeita de que as ameaças digitais poderiam ser capazes de causar enormes danos à segurança, economia e soberania dos Estados.

A busca pela proteção no domínio cibernético faz com os países criem estratégias de segurança cibernética semelhantes às suas estratégias nacionais de defesa, para que estabeleçam seus objetivos no ciberespaço e definam as ameaças de punição em caso de ataques contra sua soberania. Entretanto, não existe uma forma única de se construir uma estratégia cibernética nacional, sendo os países, conforme sua capacidade e estrutura, que determinam como implantam suas ações e quais instituições serão utilizadas para isso. Sendo assim, como forma de apoiar as nações nessa construção, algumas organizações internacionais criaram *frameworks* (ou guias) com sugestões de como estruturar uma coordenação cibernética nacional, capaz de enfrentar as ameaças cibernéticas, buscar a cooperação internacional e, com isso, optar entre abordagens militarizadas ou voltadas à gestão.

Para entender se esses guias se apoiam em uma perspectiva securitizada, essa dissertação escolheu os documentos de instituições da Europa, dos Estados Unidos, de uma agência da ONU e da OEA, ou seja, organizações dotadas de diferentes funções e objetivos,

bem como de regiões de atuação distintas. Assim, a pesquisa submeteu cinco desses documentos a um estudo através da Teoria Fundamentada, que se trata de uma pesquisa qualitativa que busca gerar novas teorias através de elementos básicos como: conceitos, categorias e propriedades. Dessa forma, essa pesquisa codificou os documentos na busca de conceituar as ações cibernéticas que vão ao encontro da perspectiva securitizada.

Para isso, a pesquisa partiu da discussão da academia sobre a existência de uma securitização cibernética para identificar ações e conceitos securitizados nesses documentos. Assim sendo, entre essas práticas securitizadas encontradas em artigos e livros, temos como exemplos: o discurso da ameaça cibernética iminente contra ativos críticos, a capacitação de unidades cibernéticas militares, a proteção de infraestruturas críticas pelas forças armadas, o receio de roubo de propriedade intelectual nacional, a espionagem cibernética, combate ao terrorismo cibernético, estabelecer uma dissuasão no ciberespaço, a ameaça de agressão entre Estados, entre outras.

Entre os *frameworks* estudados, o *Cooperative Cyber Defence Centre of Excellence* da OTAN, que possui status militar, é aquele que apresenta a maior quantidade de categorias que se enquadram na perspectiva de securitização. Em seguida, também da Europa, vem o documento da ENISA, o qual tem um número menor de ações securitizadas. Nos outros *frameworks* foram identificados poucos elementos que se encaixam como securitizados. A natureza dessas organizações pode explicar a opção por sugestão de ações securitizadas ou que caminham em direção à governança. O NIST é uma agência estadunidense que trabalha em prol da padronização e constrói um guia para avaliar e melhorar a segurança cibernética, capaz de ser usado tanto por países quanto por organizações da sociedade civil. O ITU é uma agência da ONU que trabalha para estabelecer padrões tecnológicos convergentes entre os países, desenvolvendo um documento com a proposta de criar uma linguagem de cibersegurança comum entre as nações. A OEA pensa na evolução do nível de proteção cibernética entre os países da América, tendo ações como diplomacia e cooperação como principais destaques.

Entre os mais securitizados, a ENISA foi criada para desenvolver conhecimento em segurança de rede e da informação para os países da Europa. Possivelmente, pelo caráter regional das suas ameaças, seu *framework* inclui a preocupação com o terrorismo cibernético, assim como com a dissuasão e a prática de exercícios ofensivos e defensivos no ciberespaço. Mesmo assim, o documento possui a maior parte das ações dentro do campo político, focado nas ações de governança cibernética, que compreendem ações voltadas ao gerenciamento de riscos, vulnerabilidades e na gestão de incidentes. Por outro lado, a natureza militar do CCDCOE pode explicar por que o *framework* da OTAN é o que estabelece o maior número de

ações securitizadas. Cabe lembrar que o centro fica situado na Estônia, país alvo de um dos maiores ataques cibernéticos já ocorridos entre Estados. Assim, embora traga muitas ações que convergem com as categorias securitizadas sugeridas por essa pesquisa, o documento informa que sua utilização deve ser feita de maneira livre pelos países, ou seja, as ações devem ser escolhidas conforme seus objetivos, aliados com sua capacidade de implantação.

Após a análise dos *frameworks*, o próximo objetivo da pesquisa foi, por meio das categorias securitizadas encontradas, comparar se as ações de combate ao cibercrime dos países da América do Sul se posicionam dentro do espectro da securitização dos *frameworks* estudados. De forma a proporcionar uma avaliação sistemática e metodológica, bem como conhecer a natureza dos objetivos da proteção cibernética desses países, esse trabalho optou por estudar apenas aqueles que possuem estratégia ou política nacional de cibersegurança, submetendo-as também à Teoria Fundamentada. No entanto, a dissertação não deixa de comentar as principais atividades desenvolvidas pelos países que ainda não construíram suas estratégias/políticas cibernéticas.

Isto posto, a pesquisa encontrou que, desde a última década, os países da América do Sul têm se mostrado preocupados com o combate ao crime cibernético. Como o trabalho mostra, os países do continente têm elaborado leis específicas para delitos digitais, bem como legislações para proteção de dados e da privacidade dos usuários. A pesquisa também mostra que, conforme sua sociedade/modo de vida, cada país possui tipificação penal diferente, no Paraguai, por exemplo, a pornografia infantil é relatada em sua estratégia com um problema nacional a ser enfrentado. No Brasil, o *phishing* e a pirataria; no Equador, o cuidado com os crimes de ódio e *cyberbullying*. Em suma, o trabalho identificou que cada país tem sua tipificação penal digital própria, sem que exista um desafio comum a ser enfrentado por essas nações. Apesar disso, existe no continente um esforço por uma linguagem e ações comuns para deter os crimes digitais, através de alianças com organizações internacionais de combate ao cibercrime. É o caso de Argentina, Colômbia, Chile, Paraguai e Peru, que alteraram suas legislações para serem signatários da Convenção de Budapeste de Combate ao Cibercrime. Em 2021, o Brasil iniciou os trâmites para sua adesão ao grupo, assim como outros países da região.

A pesquisa constatou que todas as ações de combate ao cibercrime dos países pesquisados estão dentro do espectro político, ou seja, não se verifica um processo de securitização das ações de repressão. Existe, sim, um movimento na direção da construção de forças policiais e de justiça capacitadas para investigar, bem como judicializar esses crimes. Um exemplo disso é a Colômbia que criou um centro policial que, integrado com outras forças, trabalha em prol da proteção cibernética. Porém, cabe destacar que praticamente todos os países

pesquisados estabelecem em suas estratégias/políticas o uso pacífico do ciberespaço, assim como o compromisso com o respeito aos direitos humanos e à privacidade. Desta forma, parece-nos possível afirmar que esse seja um fator importante para que essa perspectiva política seja mantida na região.

A preocupação com o terrorismo cibernético no continente foi encontrada nos casos de Argentina, Colômbia e Equador. Assim, parece-nos provável que fatores históricos podem explicar o temor que esses países possuem em relação a esse tipo de ameaça, uma vez que Argentina e Colômbia já enfrentaram esse desafio em seu próprio território. No Equador esse receio pode ser justificado pelos conflitos entre Venezuela e Colômbia, que acabaram por se estender até a fronteira do país. Nesse sentido, no entanto, a pesquisa não encontrou nas estratégias/políticas ações de enfrentamento do terrorismo cibernético dentro do espectro da securitização, ou seja, não existem, nos documentos, citações sobre a possibilidade de violação da privacidade dos cidadãos em prol da segurança nacional, assim como ocorreu com o *USA Patriotic Act* assinado pelo presidente George W. Bush em 2001, que permitiu a interceptação de ligações telefônicas e e-mails de pessoas supostamente envolvidas com terrorismo por órgãos de inteligência, sem a necessidade de qualquer autorização da Justiça (THE UNITED STATES, 2018).

A despeito de ter encontrado algumas ações securitizadas por países como a Colômbia, por exemplo, essa pesquisa não identificou na América do Sul um movimento desses países em direção a uma securitização do domínio cibernético no século XXI. Ao contrário disso, os países têm se esforçado para integrar organizações internacionais de combate ao cibercrime, bem como ampliar a cooperação com países e organizações que possam auxiliar na identificação e tratamento de ameaças cibernéticas, principalmente com a Europa e os Estados Unidos. Além disso, a pesquisa considera que a história e as características sociais são fatores fundamentais para moldar as estratégias e políticas nacionais de cibersegurança desses Estados. Por exemplo, a experiência com a ditadura contribuiu para seja dedicada especial ênfase às questões de direitos humanos e privacidade, como descreve o texto chileno. Outro caso é a influência militar estadunidense no fortalecimento das Forças Armadas colombianas no combate ao narcotráfico, que pode ter influenciado o país sul-americano a propor ações mais securitizadas que outros países da região. Desta forma, a hipótese do trabalho, de que apesar de compartilharem diversas características semelhantes (como aspectos sociais, históricos, políticos e econômicos) e de sua proximidade geográfica, nem todos os países da América do Sul implementam ações securitizadas para promover sua defesa contra o cibercrime, sendo possível verificar níveis diferentes de securitização nos casos em que ela ocorre, se confirma. Entretanto, deve ser

acrescentado que o fator histórico tem muita relevância na construção de uma estratégia cibernética nacional.

Ademais, considerando a segurança cibernética nacional como parâmetro de avaliação, essa pesquisa não encontrou, na região, elementos que indiquem, nessa temática, a configuração de um Complexo Regional de Segurança, como proposto por Buzan e Waever (2003). Segundo os autores da teoria dos CRS, um elemento importante para compreender sua aplicação à América do Sul, seria o papel desempenhado pelos Estados Unidos na região, que é considerado uma potência extrarregional que apesar de se projetar na região, não a molda, nem mesmo a regula. No entanto, no contexto da cibersegurança, a pesquisa encontrou uma maior aproximação dos países sul-americanos em direção às organizações europeias, bem como a formação de parcerias com bancos de fomento, como o BID, que fornecem empréstimos para o desenvolvimento da segurança cibernética nesses países.

Isto posto, parece-nos que as possibilidades de estudo do ciberespaço e seus fenômenos são inúmeras. Dessa forma, cientes do desafio, buscou-se nesse trabalho unir conceitos de Segurança da Informação e das Relações Internacionais para responder à questão de pesquisa proposta. Desta forma, a pesquisa consegue trazer informações sobre as práticas mais comuns para a elaboração de estratégias de segurança cibernéticas nacionais, sejam elas voltadas à gestão ou para as ações securitizadas, além de mostrar alguns dados dos crimes cibernéticos mais comuns na região. Ademais, apresenta um estudo sobre os *frameworks* que orientam os países nessa tarefa, deixando seus objetivos claros, bem como enumerando as principais práticas sugeridas nos documentos. Embora o risco da ameaça cibernética seja um problema global, o estudo também colabora para demonstrar que os países estabelecem suas estratégias baseados em fatores históricos e na própria avaliação de risco cibernético, o que poderia explicar porque as ações de combate têm porcentagens tão diferentes entre eles. O trabalho mostra que a natureza do ciberespaço (anárquica e sem fronteiras), demonstra que são necessários novos estudos das Relações Internacionais sobre esse domínio, além de exigir nova atenção da Segurança da Informação sobre fatores políticos, econômicos e de segurança internacional nos estudos da segurança cibernética nacional.

REFERÊNCIAS

ACHARYA, Amitav; BUZAN, Barry. **The Making of global international relations:** origins and evolution of IR at its centenary. Cambridge: Cambridge University Press, 2019.

AGÊNCIA BRASIL. **Venezuela oferece "asilo humanitário" a Edward Snowden**. [*S. l.*], 2013. Disponível em: https://memoria.ebc.com.br/noticias/internacional/2013/07/venezuela-oferece-asilo-humanitario-a-edward-snowden. Acesso em: 11 Nov. 2020.

AGÊNCIAS, El País. **Ciberataque paralisa 16 hospitais do Reino Unido**. [*S. l.*], 2017. Disponível em: https://brasil.elpais.com/brasil/2017/05/12/internacional/1494602389_458942.html. Acesso em: 23 Sep. 2020.

ASSANGE, Julian Paul *et al.* **Cypherpunks**: Liberdade e o futuro da internet. São Paulo: Boitempo Editorial, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27032. Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética**. [*S. l.*]: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015.

AUSTRALIAN GOVERNMENT. **Cyber Security Strategy 2020**. [*S. l.: s. n.*], 2020. Disponível em: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf. Acesso em: 19 Jun. 2021.

AUSTRALIAN GOVERNMENT. **Internet Regulation in Australia | Australian Human Rights Commission**. [*S. l.*], 1992. Disponível em: https://humanrights.gov.au/our-work/publications/internet-regulation-australia. Acesso em: 30 Dec. 2021.

BAKER, Stewart; WATERMAN, Shaun; IVANOV, George. **Critical Infrastructure Protection In the Crossfire Critical Infrastructure in the Age of Cyber War A global report on the threats facing key industries**. [*S. l.: s. n.*], 2010. Disponível em: https://www.govexec.com/pdfs/012810j1.pdf. Acesso em: 23 Sep. 2020.

BANCO INTERAMERICANO DE DESAROLLO. **Project Details | IADB**. [*S. l.*], 2018. Disponível em: https://www.iadb.org/en/project/CO-L1233. Acesso em: 18 Jan. 2022.

BANCO INTERAMERICANO DE DESARROLLO. **Project Details | IADB**. [*S. l.*], 2019a. Disponível em: https://www.iadb.org/en/project/AR-L1304. Acesso em: 14 Jan. 2022.

BANCO INTERAMERICANO DE DESARROLLO. **Project Details | IADB**. [*S. l.*], 2019b. Disponível em: https://www.iadb.org/en/project/UR-L1152. Acesso em: 19 Jan. 2022.

BANCO INTERAMERICANO DE DESARROLLO. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. [*s. l.*], 2020. Disponível em: https://doi.org/10.18235/0002513. Acesso em: 15 Oct. 2020.

BBC MUNDO. Ciber-ataque en Chile. **news.bbc.co.uk**, [*s. l.*], 11 May 2008. Disponível em: http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7395000/7395288.stm. Acesso em: 23 Sep. 2020.

BENDRATH, Ralf. **The American Cyber-Angst and the Real World—Any Link? Publicado em Bombs and Badwidth: The emerging relationship between information technology and security**. [*S. l.*]: The New Presss, 2003.

BIBLIOTECA DEL CONGRESO. **Biblioteca del Congreso Nacional | Ley Chile**. [*S. l.*], 1999. Disponível em: http://bcn.cl/2f7cg. Acesso em: 17 Jan. 2022.

BIBLIOTECA DEL CONGRESO. **Biblioteca del Congreso Nacional | Ley Chile**. [*S. l.*], 1993. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=30590. Acesso em: 17 Jan. 2022.

BIBLIOTECA DEL CONGRESO. **Biblioteca del Congreso Nacional | Ley Chile**. [*S. l.*], 2017. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1106936. Acesso em: 17 Jan. 2022.

BIBLIOTECA DEL CONGRESO. **Biblioteca del Congreso Nacional | Ley Chile**. [*S. l.*], 2019. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1138479. Acesso em: 17 Jan. 2022.

BOLÍVIA. **Aprueban PL que declara prioridad nacional la elaboración e implementación de la Estrategia Nacional de Ciberseguridad de Estado**. [*S. l.*], 2017. Disponível em: https://web.senado.gob.bo/prensa/noticias/aprueban-pl-que-declara-prioridad-nacional-la-elaboraci%C3%B3n-e-implementaci%C3%B3n-de-la. Acesso em: 19 Jan. 2022.

BOLÍVIA. **Decreto Supremo nº 2514 Evo Morales Ayma Presidente Constitucional del Estado Plurinacional de Bolívia Considerando**. [*S. l.: s. n.*], 2015a. Disponível em: https://www.probolivia.gob.bo/wp-content/uploads/2021/05/norma-22-DS2514.pdf. Acesso em: 19 Jan. 2022.

BOLÍVIA. **Normativa | Centro de Gestión de Incidentes Informáticos**. [*S. l.*], 2015b. Disponível em: https://www.cgii.gob.bo/es/normativa. Acesso em: 19 Jan. 2022.

BORGHELLO, Cristian; TEMPERINI, Marcelo. **Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública**. [*S. l.: s. n.*], 2013. Disponível em: http://sedici.unlp.edu.ar/bitstream/handle/10915/94081/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y. Acesso em: 23 Sep. 2020.

BRASIL. **D10222**. [*S. l.*], 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm#:~:text=DECRETO%20N%C2%BA%2010.222%2C%20DE%205. Acesso em: 17 Jan. 2022.

BRASIL. **D10566**. [*S. l.*], 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 7 Dec. 2021.

BRASIL. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** [*S. l.*], 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 Jan. 2022.

BRASIL. **Estratégia Nacional de Defesa**. [*S. l.: s. n.*], 2008. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/end.pdf. Acesso em: 22 Jan. 2022.

BRASIL. **Lei Carolina Dickmann**. [*S. l.*], 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 Jan. 2022.

BRASIL. **Sistema Militar de Defesa Cibernética entra em vigor nesta terça-feira**. [*S. l.*], 2022. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/sistema-militar-de-defesa-cibernetica-entra-em-vigor-nesta-terca-feira. Acesso em: 22 Jan. 2022.

BRASIL. **D9573**. [*S. l.*], 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm. Acesso em: 17 Jan. 2022.

BRASIL. **L13709**. [*S. l.*], 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 17 Jan. 2022.

BRASIL. **MD31-M-07 Doutrina Militar de Defesa Cibernética**. [*S. l.*]: Ministério da Defesa, 2014b. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 27 Oct. 2020.

BUZAN, Barry; WAEVER, Ole; DE WILDE, Jaap. **Security a new framework for analysis**. [*S. l.*]: Boulder, Colo. Lynne Rienner, 1998.

CENTRAL INTELLIGENCE AGENCY - CIA. **The World Factbook — Central Intelligence Agency**. [*S. l.*], 2019. Disponível em: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html. Acesso em: 23 Sep. 2020.

CERT. **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. [*S. l.*], 2022. Disponível em: https://cert.br/. Acesso em: 17 Jan. 2022.

CÉSAR, Samuel; JÚNIOR, Cruz. **850 A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. [*S. l.: s. n.*], 2013. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/1590/1/TD_1850.pdf. Acesso em: 28 Jan. 2022.

CHARMAZ, Kathy. **Constructing grounded theory : a practical guide through qualitative analysis**. Los Angeles ; London: Sage, 2011.

CLARÍN. **Alerta por un supuesto atentado terrorista en Unicenter Shopping**. [*S. l.*], 2015. Disponível em: http://muy.clarin.com/policiales/unicenter-atentado-amenaza-terrorista-3818.html. Acesso em: 22 Jan. 2022.

CLINTON, Bill. **Executive Order 13010: Critical Infrastructure Protection**. [*S. l.*], 1996. Disponível em: https://www.hsdl.org/?abstract&did=1613. Acesso em: 7 Dec. 2021.

CONSEIL DE L'EUROPE. **CETS 185 - Convention on Cybercrime**. [*S. l.: s. n.*], 2001. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. Acesso em: 23 Sep. 2020.

CONSEIL DE L'EUROPE. **Colombia joined the Budapest Convention on Cybercrime**. [*S. l.*], 2020. Disponível em: https://www.coe.int/en/web/cybercrime/-/colombia-joined-the-budapest-convention-on-cybercrime. Acesso em: 18 Jan. 2022.

COUNCIL OF EUROPE. **Argentina, 33rd country to sign Convention 108+**. [*S. l.*], 2018. Disponível em: https://www.coe.int/en/web/data-protection/-/argentina-33rd-country-to-sign-convention-108-. Acesso em: 14 Jan. 2022.

CSIRT AMÉRICAS. **Csirtamericas**. [*S. l.*], 2022. Disponível em: https://www.csirtamericas.org/. Acesso em: 19 Jan. 2022.

CUNHA, Maria Eduarda. **No Equador, 20 mi de pessoas tiveram dados vazados**. [*S. l.*], 2019. Disponível em: https://exame.com/tecnologia/no-equador-20-mi-de-pessoas-tiveram-dados-vazados/. Acesso em: 23 Sep. 2020.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Critical Infrastructure Sectors | CISA**. [*S. l.*], 2019. Disponível em: https://www.cisa.gov/critical-infrastructure-sectors. Acesso em: 7 Dec. 2021.

DEIBERT, Ronald J. Information technologies and global politics: the changing scope of power and governance. **Choice Reviews Online**, [*s. l.*], v. 40, n. 03, p. 40–182140–1821, 2002. Disponível em: https://doi.org/10.5860/choice.40-1821. Acesso em: 11 Nov. 2021.

DELERUE, François. **A Close Look at France's New Military Cyber Strategy**. [*S. l.*], 2019. Disponível em: https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/. Acesso em: 26 Jan. 2022.

DENNING, Dorothy. Information Warfare And Security. **EDPACS**, [*s. l.*], v. 27, n. 9, p. 1–2, 2000. Disponível em: https://doi.org/10.1201/1079/43255.27.9.20000301/30321.7. Acesso em: 1 Dec. 2021.

DODGE, Martin; KITCHIN, Rob. **Mapping Cyberspace**. [*S. l.*]: Routledge, 2003. Disponível em: https://doi.org/10.4324/9780203165270. Acesso em: 9 Dec. 2021.

DOMBROWSKI, Peter; KELLEHER, Catherine McArdle. **Regional Missile Defense from a Global Perspective**. Stanford: Stanford University Press, 2015. *E-book*.

DUQUE, Marina Guedes. O papel de síntese da escola de Copenhague nos estudos de segurança internacional. **Contexto Internacional**, [*s. l.*], v. 31, n. 3, p. 459–501, 2009. Disponível em: https://doi.org/10.1590/s0102-85292009000300003. Acesso em: 11 Nov. 2021.

ELBE, Stefan. Should HIV/AIDS Be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security. **International Studies Quarterly**, [*s. l.*], v. 50, n. 1, p. 119–144, 2006. Disponível em: https://doi.org/10.1111/j.1468-2478.2006.00395.x. Acesso em: 16 Nov. 2021.

EMPRESA BRASIL DE COMUNICAÇÃO - EBC. **Ataque terrorista contra militares na Colômbia deixa 36 feridos**. [*S. l.*], 2021. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2021-06/ataque-terrorista-contra-militares-na-colombia-deixa-36-feridos. Acesso em: 22 Jan. 2022.

ÉPOCA. **O que o ataque de Israel a hackers do Hamas significa para o futuro da guerra cibernética**. [*S. l.*], 2019. Disponível em: https://epocanegocios.globo.com/Mundo/noticia/2019/05/o-que-o-ataque-de-israel-hackers-do-hamas-significa-para-o-futuro-da-guerra-cibernetica.html. Acesso em: 23 Sep. 2020.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **An evaluation framework for Cyber Security Strategies**. [*S. l.*], 2014. Disponível em: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies. Acesso em: 27 Dec. 2021.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **National Cyber Security Strategies: An Implementation Guide**. [*S. l.*], 2012. Disponível em: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide. Acesso em: 27 Dec. 2021.

FEDERAL BUREAU OF INVESTIGATION. **Update on Sony Investigation**. [*S. l.*], 2014. Disponível em: encurtador.com.br/pBIJK. Acesso em: 25 Nov. 2020.

FERRAÇO, Ricardo. **CPI da Espionagem - Relatório Final**. [*S. l.: s. n.*], 2014. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco. Acesso em: 23 Sep. 2020.

G1. **Maior atentado terrorista da Argentina completa 25 anos sem julgamento de autores**. [*S. l.*], 2019. Disponível em: https://g1.globo.com/mundo/noticia/2019/07/18/maior-atentado-terrorista-da-argentina-completa-25-anos-sem-julgamento-de-autores.ghtml. Acesso em: 22 Jan. 2022.

GERCHMANN, Léo. **Folha de S.Paulo - Terrorismo: Argentina alerta para novo atentado - 21/01/98**. [*S. l.*], 1998. Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft210107.htm. Acesso em: 22 Jan. 2022.

GERMANY. **Cyber Security Strategy for Germany 2021**. [*S. l.*], 2021. Disponível em: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf. Acesso em: 8 Dec. 2021.

GIBSON, W. **Burning chrome**. London: Gollancz, 1982.

GIBSON, W. **Neuromancer.** London: Harper/Voyager, 1984.

GILES, Keir; HAGESTAD, William. **Divided by a common language: Cyber definitions in Chinese, Russian and English**. [*S. l.*], 2013. Disponível em: https://ieeexplore.ieee.org/document/6568390. Acesso em: 26 Jan. 2022.

GOBIERNO DE ESPAÑA. **BOE.es - BOE-A-2011-7630 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.** [*S. l.*], 2011. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630. Acesso em: 26 Jan. 2022.

GOBIERNO DE ESPAÑA. **National Cybersecurity Strategy**. [*S. l.: s. n.*], 2019. Disponível em: https://www.dsn.gob.es/ca/file/2989/download?token=EuVy2lNr#:~:text=Spain. Acesso em: 19 Jun. 2021.

GONZÁLEZ, Jaime. **Por que a história do filme "A Entrevista" revoltou a Coreia do Norte?** [*S. l.*], 2014. Disponível em: https://www.bbc.com/portuguese/noticias/2014/12/141222_enredo_theinterview_coreia_rs. Acesso em: 23 Sep. 2020.

GUIANA. **Cybercrime Bill**. [*S. l.*], 2016. Disponível em: https://parliament.gov.gy/documents/bills/6033-cybercrime_bill_2016_-_no._17_of_2016.doc. Acesso em: 19 Jan. 2022.

GUIANA. **Cybersecurity**. [*S. l.*], 2019. Disponível em: https://ndma.gov.gy/pillars/cybersecurity/. Acesso em: 19 Jan. 2022.

GUIANA. **About | Guyana National CIRT**. [*S. l.*], 2022. Disponível em: https://cirt.gy/about. Acesso em: 19 Jan. 2022.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, [*s. l.*], v. 53, n. 4, p. 1155–1175, 2009. Disponível em: https://doi.org/10.1111/j.1468-2478.2009.00572.x. Acesso em: 10 Nov. 2021.

HART, Catherine. **Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties. Cyber-Surveillance in Everyday Life: An International Workshop.** [*S. l.*], 2011.

HUGHES, Laura. China and Russia threaten “free and open” internet, UK warns. **Financial Times**, [*s. l.*], 14 Dec. 2021. Disponível em: https://www.ft.com/content/561fe2ec-1a89-47dc-ba29-c902746ee6bc. Acesso em: 27 Jan. 2022.

HUNDLEY, H.O.; ANDERSON, R.H. Emerging challenge: security and safety in cyberspace. **IEEE Technology and Society Magazine**, [*s. l.*], v. 14, n. 4, p. 19–28, 1995. Disponível em: https://doi.org/10.1109/44.476633. Acesso em: 6 Dec. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000. Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary**. [*S. l.*]: ISO - International Organization for Standardization, 2018.

INTERNATIONAL TELECOMMUNICATION UNION. **About ITU**. [*S. l.*], 2019. Disponível em: https://www.itu.int/en/about/Pages/default.aspx. Acesso em: 30 Dec. 2021.

INTERNATIONAL TELECOMMUNICATION UNION. **Global Cybersecurity Index**. [*S. l.*], 2021. Disponível em: https://www.itu.int/pub/D-STR-GCI.01. Acesso em: 30 Dec. 2021.

INTERNATIONAL TELECOMMUNICATION UNION. **Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity**. [*S. l.*], 2018. Disponível em: https://www.itu.int/pub/D-STR-CYB_GUIDE.01. Acesso em: 30 Dec. 2021.

INTERPOL. **Colombia**. [*S. l.*], 2022. Disponível em: https://www.interpol.int/en/Who-we-are/Member-countries/Americas/COLOMBIA. Acesso em: 18 Jan. 2022.

JACKSON, Nicole J. International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework. **Security Dialogue**, [*s. l.*], v. 37, n. 3, p. 299–317, 2006. Disponível em: https://doi.org/10.1177/0967010606069062. Acesso em: 27 Sep. 2019.

JENSEN, Eric Talbot. **Cyber Deterrence**. Rochester, NY, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2070438. Acesso em: 23 Sep. 2020.

KASSAB, Hanna Samir. In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. **Cyberspace and International Relations**, [*s. l.*], p. 59–76, 2013. Disponível em: https://doi.org/10.1007/978-3-642-37481-4_4

KHANNA, Parag. **O segundo mundo impérios e influência na nova ordem global**. [*S. l.*]: Rio De Janeiro Intrínseca, 2008.

KLIMBURG, Alexander (org.). **National cyber security framework manual**. Tallinn: Nato Cooperative Cyber Defence Centre Of Excellence, 2012.

KREMER, Jan-Frederik; MÜLLERBenedikt; GMBH, Springer-Verlag. **Cyberspace and International Relations Theory, Prospects and Challenges**. [*S. l.*]: Berlin Springer Berlin Springer, 2016.

LATHAM, Robert. **Bombs and bandwidth : the emerging relationship between information technology and security**. New York: New Press, 2005.

LEWIS, James. **Economic Impact of Cybercrime- No Slowing Down**. [*S. l.: s. n.*], 2018. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf. Acesso em: 11 Oct. 2020.

LI, Hao *et al.* Strategic Power Infrastructure Defense. **Proceedings of the IEEE**, [*s. l.*], v. 93, n. 5, p. 918–933, 2005. Disponível em: https://doi.org/10.1109/jproc.2005.847260. Acesso em: 30 Sep. 2020.

LUKASIK, Stephen. Why the Arpanet Was Built. **IEEE Annals of the History of Computing**, [*s. l.*], v. 33, n. 3, p. 4–21, 2011. Disponível em: https://doi.org/10.1109/mahc.2010.11. Acesso em: 8 Dec. 2021.

MCGUINNESS, Damien. How a cyber attack transformed Estonia. **BBC News**, [*s. l.*], 27 Apr. 2017. Disponível em: https://www.bbc.com/news/39655415. Acesso em: 26 Jan. 2022.

MCKENZIE, Timothy M. **Is cyber deterrence possible?** [*S. l.*]: Maxwell Air Force Base, Alabama Air University Press, Air Force Research Institute, 2017.

MCKUNE, Sarah; AHMED, Shazeda. The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda. **International Journal of Communication**, [*s. l.*], v. 12, p. 3835–3855, 2018. Disponível em: https://ijoc.org/index.php/ijoc/article/viewFile/8540/2461. Acesso em: 27 Jan. 2022.

MERCOSUR. **Comunicado conjunto de las Presidentas y los Presidentes de los Estados partes del MERCOSUR**. [*S. l.*], 2014. Disponível em: https://www.mercosursocialsolidario.org/comunicado-conjunto-de-las-presidentas-y-los-presidentes-de-los-estados-partes-del-mercosur/. Acesso em: 11 Nov. 2020.

MOREIRA, Bernardo João do Rego Monteiro; DURAN, Felipe Pessoa. **Sobre a questão da ciber-soberania na China**. [*S. l.*], 2020. Disponível em: https://nupri.prp.usp.br/blog/sobre-a-questao-da-ciber-soberania-na-china/. Acesso em: 27 Jan. 2022.

MYERS, Steven Lee. Estonia removes Soviet-era war memorial after a night of violence. **The New York Times**, [*s. l.*], 27 Apr. 2007. World. Disponível em: https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html. Acesso em: 26 Jan. 2022.

NATIONAL CYBER SECURITY CENTRE. **Joint US - UK statement on malicious cyber activity carried out by Russian government**. [*S. l.*], 2018. Disponível em: https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government. Acesso em: 23 Sep. 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. **Framework for Improving Critical Infrastructure Cybersecurity**, [*s. l.*], v. 1.1, 2018. Disponível em: https://doi.org/10.6028/nist.cswp.04162018

NATIONAL RESEARCH COUNCIL. **Computers at Risk: Safe Computing in the Information Age**. [*S. l.*]: Computer Science and Telecommunications Board, 1991. *E-book*.

NATIONAL RESEARCH COUNCIL. **Cybersecurity Today and Tomorrow: Pay Now or Pay Later**. Washington, DC: The National Academies Press, 2002. *E-book*.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **About us**. [*S. l.*], 2008. Disponível em: https://ccdcoe.org/about-us/. Acesso em: 28 Dec. 2021.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017. Disponível em: https://doi.org/10.1017/9781316822524. Acesso em: 28 Dec. 2021.

NEWMAN, Lily Hay. What Israel's Strike on Hamas Hackers Means For Cyberwar. **Wired**, [*s. l.*], 2019. Disponível em: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/. Acesso em: 17 Oct. 2020.

NISSENBAUM, Helen. Hackers and the contested ontology of cyberspace. **New Media & Society**, [*s. l.*], v. 6, n. 2, p. 195–217, 2004. Disponível em: https://doi.org/10.1177/1461444804041445. Acesso em: 10 Nov. 2021.

NISSENBAUM, Helen. Where Computer Security Meets National Security1. **Ethics and Information Technology**, [*s. l.*], v. 7, n. 2, p. 61–73, 2005. Disponível em: https://doi.org/10.1007/s10676-005-4582-3. Acesso em: 10 Nov. 2021.

NORTON. **Norton Cyber Security Insights Report 2017 Global Results**. [*S. l.: s. n.*], 2018. Disponível em: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2017-ncsir-global-results-en.pdf. Acesso em: 23 Sep. 2020.

OGLOBO. **Como um programa da NSA virou arma de hackers em busca de dinheiro**. [*S. l.*], 2017. Disponível em: https://oglobo.globo.com/economia/como-um-programa-da-nsa-virou-arma-de-hackers-em-busca-de-dinheiro-2133281. Acesso em: 23 Sep. 2020.

OLIVEIRA, Marcos Aurelio Guedes de *et al.* **Guia de Defesa Cibernética na América do Sul**. [*S. l.: s. n.*], 2017. Disponível em:

https://pandia.defesa.gov.br/images/acervodigital/GuiaDefesaCiberneticaAmericaSul.pdf. Acesso em: 11 Oct. 2020.

ORGANIZATION OF AMERICAN STATES. **:: Tratados Multilaterais > Departamento de Direito Internacional > OEA ::** [*S. l.*], 2014a. Disponível em: http://www.oas.org/dil/port/tratados_A-41_Carta_da_Organiza%C3%A7%C3%A3o_dos_Estados_Americanos.htm#ch1. Acesso em: 25 Jan. 2022.

ORGANIZATION OF AMERICAN STATES. **2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean | Publications**. [*S. l.*], 2020. Disponível em: https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf. Acesso em: 12 Jan. 2022.

ORGANIZATION OF AMERICAN STATES. **Democracy for peace, security, and development**. [*S. l.*], 2014b. Disponível em: https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-555/14. Acesso em: 19 Jan. 2022.

ORGANIZATION OF AMERICAN STATES. **OEA - Organização dos Estados Americanos: Democracia para a paz, segurança e desenvolvimento**. [*S. l.*], 2009a. Disponível em: https://www.oas.org/pt/sobre/quem_somos.asp. Acesso em: 25 Jan. 2022.

ORGANIZATION OF AMERICAN STATES. **OEA - Organização dos Estados Americanos: Democracia para a paz, segurança e desenvolvimento**. [*S. l.*], 2009b. Disponível em: https://www.oas.org/pt/topicos/seguranca_cibernetica.asp. Acesso em: 25 Jan. 2022.

ORWELL, George. **1984**. Harlow: Pearson Education, 2008.

PERGHER, Natasha. O Complexo Regional de Segurança da América do Sul: um Estudo de Barry Buzan e Ole Waever. **Revista Perspectiva**, [*s. l.*], 2011.

PRICEWATERHOUSECOOPERS. **Ciberseguridad: sin estrategia para proteger información sensible**. [*S. l.*], 2018. Disponível em: https://www.pwc.com.ar/es/prensa/ciberseguridad-empresas-argentinas-no-protegen-informacion-sensible.html. Acesso em: 14 Jan. 2022.

RADIO TELEVISION MARTI. **Ciberataque informático masivo contra fuerzas armadas y policía de Perú**. [*S. l.*], 2014. Disponível em: https://www.radiotelevisionmarti.com/a/peru-ciberataque-policia-fuerzas-armadas/74026.html. Acesso em: 23 Sep. 2020.

RAUD, Mikk. **China and Cyber: Attitudes, Strategies, Organisation**. [*S. l.*], 2016. Disponível em: https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf. Acesso em: 26 Jan. 2022.

REPÚBLICA ARGENTINA. **Argentina.gob.ar**. [*S. l.*], 2011. Disponível em: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-580-2011-185055. Acesso em: 30 Jan. 2022.

REPÚBLICA ARGENTINA. **Argentina.gob.ar**. [*S. l.*], 2017. Disponível em: https://www.argentina.gob.ar/normativa/nacional/decreto-577-2017-277518/actualizacion. Acesso em: 14 Jan. 2022.

REPÚBLICA ARGENTINA. **Codigo Penal**. [*S. l.*], 2008. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. Acesso em: 14 Jan. 2022.

REPÚBLICA ARGENTINA. **Estrategia Nacional de Ciberseguridad de La República Argentina**. [*S. l.: s. n.*], 2019. Disponível em: https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf. Acesso em: 14 Jan. 2022.

REPÚBLICA ARGENTINA. **Proteccion de Los Datos**. [*S. l.*], 2000. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. Acesso em: 14 Jan. 2022.

REPÚBLICA BOLIVARIANA DE VENEZUELA. **Ley Especial contra los Delitos Informáticos**. [*S. l.*], 2014. Disponível em: http://www.conatel.gob.ve/ley-especial-contra-los-delitos-informaticos-2/. Acesso em: 19 Jan. 2022.

REPÚBLICA BOLIVARIANA DE VENEZUELA. **Suscerte**. [*S. l.*], 2022. Disponível em: http://www.suscerte.gob.ve/sobre-suscerte/. Acesso em: 19 Jan. 2022.

REPÚBLICA BOLIVARIANA DE VENEZUELA. **VenCERT garantiza seguridad de web oficiales venezolanas**. [*S. l.*], 2015. Disponível em: http://www.conatel.gob.ve/vencert-garantiza-seguridad-de-web-oficiales-venezolanas/. Acesso em: 19 Jan. 2022.

REPÚBLICA DE CHILE. **CSIRT**. [*S. l.*], 2022a. Disponível em: https://www.csirt.gob.cl/. Acesso em: 17 Jan. 2022.

REPÚBLICA DE CHILE. **Política Nacional de Ciberseguridad**. [*S. l.: s. n.*], 2017. Disponível em: https://www.cnc.cl/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf. Acesso em: 17 Jan. 2022.

REPÚBLICA DE CHILE. **Protección a los datos personales como derecho constitucional será una realidad - Senado - República de Chile**. [*S. l.*], 2018. Disponível em: https://www.senado.cl/noticias/datos-personales/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una. Acesso em: 17 Jan. 2022.

REPÚBLICA DE CHILE. **Quiénes somos**. [*S. l.*], 2022b. Disponível em: http://www.internetsegura.cl/quienes-somos/. Acesso em: 18 Jan. 2022.

REPÚBLICA DE COLOMBIA. **Conpes Consejo Nacional de Política Económica y Social Repúplica de Colombia Departamento Nacional de Planeación Política Nacional de Seguridad Digital**. [*S. l.: s. n.*], 2016. Disponível em: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf. Acesso em: 18 Jan. 2022.

REPÚBLICA DE COLOMBIA. **Delegatura para la Protección de Datos Personales | Superintendencia de Industria y Comercio**. [*S. l.*], 2022. Disponível em: https://www.sic.gov.co/delegatura-para-la-proteccion-de-datos-personales. Acesso em: 18 Jan. 2022.

REPÚBLICA DE COLOMBIA. **Ley 1273 de 2009**. [*S. l.*], 2009. Disponível em: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf. Acesso em: 18 Jan. 2022.

REPÚBLICA DE COLOMBIA. **Lineamientos de Política para Ciberseguridad y Ciberdefensa**. [*S. l.*], 2011. Disponível em: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf. Acesso em: 18 Jan. 2022.

REPÚBLICA DEL ECUADOR. **2002-67 Ley de Comercio Electrónico, Firmas y Mensajes de Datos | Ecuador - Guía Oficial de Trámites y Servicios**. [*S. l.*], 2002. Disponível em: https://www.gob.ec/regulaciones/2002-67-ley-comercio-electronico-firmas-mensajes-datos. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL ECUADOR. **Código Orgánico Integral Penal, COIP**. [*S. l.*], 2015. Disponível em: https://vlex.ec/vid/codigo-organico-integral-penal-631464447. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL ECUADOR. **EcuCERT de Arcotel – Centro de Respuesta a Incidentes Informáticos de la ARCOTEL**. [*S. l.*], 2022. Disponível em: https://www.ecucert.gob.ec/. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL ECUADOR. **Política de Ciberseguridad**. [*S. l.*], 2021. Disponível em: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PARAGUAY. **Alfresco» Plan Nacional de Ciberseguridad.pdf**. [*S. l.*], 2017. Disponível em: https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg. Acesso em: 18 Jan. 2022.

REPÚBLICA DEL PARAGUAY. **La Policia Nacional representada por el Departamento Especializado en Cibercrimen**. [*S. l.*], 2020. Disponível em: https://www.policianacional.gov.py/la-policia-nacional-representada-por-el-departamento-especializado-en-cibercrimen/. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PARAGUAY. **Ley Nº 4439 / Modifica y amplia varios articulos de la Ley nº 1160/97 "Codigo Penal."** [*S. l.*], 2011a. Disponível em: https://www.bacn.gov.py/leyes-paraguayas/3777/modifica-y-amplia-varios-articulos-de-la-ley-n-116097-codigo-penal. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PARAGUAY. **Ley Nº 6207 / Crea el Ministro de Tecnologías de La Información Y Comunicación y estabelece su carta orgánica**. [*S. l.*], 2018. Disponível em: https://www.bacn.gov.py/leyes-paraguayas/8933/ley-n-6207-crea-el-ministerio-de-tecnologias-de-la-informacion-y-comunicacion-y-establece-su-carta-organica. Acesso em: 18 Jan. 2022.

REPÚBLICA DEL PARAGUAY. **Ley º 1682 / Reglamenta la Información de Carácter Privado**. [*S. l.*], 2011b. Disponível em: https://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado#:~:text=%2D%20Es%20l%C3%ADcita%20la%20recolecci%C3%B3n%2C%20almacenamiento. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PARAGUAY. **Unidad Especializada de Delitos Informáticos**. [*S. l.*], 2022. Disponível em: Unidad Especializada de Delitos Informáticos. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PERU. **Decreto Legislativo N° 1412**. [*S. l.*], 2018. Disponível em: https://www.gob.pe/institucion/pcm/normas-legales/289706-1412. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PERU. **Estrategia Nacional de Seguridad y Confianza Digital**. [*S. l.*], 2021a. Disponível em: https://cdn.www.gob.pe/uploads/document/file/1985045/Estrategia%20Nacional%20de%20Seguridad%20y%20Confianza%20Digital%20v1.5.pdf.pdf. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PERU. **Ley de Ciberdefensa**. [*S. l.*], 2019. Disponível em: https://cdn.www.gob.pe/uploads/document/file/1671813/Ley%20N%C2%B030999%2C%20Ley%20de%20Ciberdefensa.pdf. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PERU. **Ley N° 30618**. [*S. l.*], 2017. Disponível em: https://www.gob.pe/institucion/dini/normas-legales/887205-30618. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PERU. **Política Nacional de Ciberseguridad**. [*S. l.*], 2020. Disponível em: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf. Acesso em: 19 Jan. 2022.

REPÚBLICA DEL PERU. **Sistema Nacional de Coordinación ante Incidentes Informáticos**. [*S. l.*], 2021b. Disponível em: https://www.peru.gob.pe/pecert/QueEs.html. Acesso em: 19 Jan. 2022.

REPUBLICA ORIENTAL DEL URUGUAY. **Estrategia Nacional de Ciberseguridad de La República Argentina Comisión Especial de Innovación, Ciencia y TecnologíaParlamento.gub.uy**. [*S. l.: s. n.*], 2021. Disponível em: https://legislativo.parlamento.gub.uy/temporales/D2016050433-007207517.pdf. Acesso em: 19 Jan. 2022.

REPÚBLICA ORIENTAL DEL URUGUAY. **1. Marco Ciberseguridad_v4.1.pdf**. [*S. l.*], 2019. Disponível em: https://archivos.agesic.gub.uy/nextcloud/index.php/s/pFXtSiWT47Kdaaz. Acesso em: 19 Jan. 2022.

REPÚBLICA ORIENTAL DEL URUGUAY. **Centro Nacional de Respuesta a Incidentes de Seguridad Informática**. [*S. l.*], 2022. Disponível em: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/. Acesso em: 19 Jan. 2022.

REPÚBLICA ORIENTAL DEL URUGUAY. **Decreto N° 36/015**. [*S. l.*], 2015. Disponível em: https://www.impo.com.uy/bases/decretos/36-2015. Acesso em: 19 Jan. 2022.

REPÚBLICA ORIENTAL DEL URUGUAY. **Ley N° 18331**. [*S. l.*], 2008. Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008#:~:text=%2D%20Toda%20persona%20f%C3%ADsica%20o%20jur%C3%ADdica. Acesso em: 19 Jan. 2022.

REPÚBLICA ORIENTAL DEL URUGUAY. **Transforming with equity Agenda**. [*S. l.: s. n.*], 2020. Disponível em: https://www.gub.uy/uruguay-digital/sites/uruguay-digital/files/documentos/publicaciones/Agenda%2520Digital%25202020%2520ingl%25C3%25A9s.pdf. Acesso em: 19 Jan. 2022.

REPÚBLICA POPULAR DA CHINA. **Lei de Segurança Cibernética da República Popular da China**. [*S. l.*], 2016. Disponível em: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm. Acesso em: 27 Jan. 2022.

RÉPUBLIQUE FRANÇAISE. **Éléments publics de doctrine militaire de lutte informatique offensive**. [*S. l.: s. n.*], 2019. Disponível em: https://www.defense.gouv.fr/content/download/551531/9394285/Politique%20MINARM%20de%20lutte%20informatique%20OFFENSIVE.pdf. Acesso em: 26 Jan. 2022.

RICHTER, André. **Brasil inicia adesão a tratado contra crimes cibernéticos**. [*S. l.*], 2019. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2019-12/brasil-inicia-adesao-tratado-contra-crimes-ciberneticos#:~:text=A%20Conven%C3%A7%C3%A3o%20de%20Budapeste%20%C3%A9. Acesso em: 11 Oct. 2020.

RODRIGUES, Julianny; MÈRCHER, Leonardo. **A cibersegurança americana e a Escola de Copenhague: do paradigma da securitização ao caso Edward Snowden**. [*S. l.: s. n.*], 2017. Disponível em: https://repositorio.uninter.com/bitstream/handle/1/270/1207118%20-

%20JULIANNY%20RIBEIRO%20RODRIGUES.pdf?sequence=1&isAllowed=y. Acesso em: 23 Sep. 2020.

ROE, Paul. **Ethnic violence and the societal security dilemma**. London: Routledge, 2014.

SAFER NET BRASIL. **SaferNet**. [*S. l.*], 2022. Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em: 2 Feb. 2022.

SANTOS, D; CARVALHO, B; CAVALCANTE, S. **Segurança de infraestruturas críticas no Brasil**. [*S. l.: s. n.*], 2010. Disponível em: https://www.iwra.org/member/congress/resource/PAP00-5734.pdf. Acesso em: 26 Jan. 2022.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. 2. ed. [*S. l.*]: Elsevier, 2014.

SILVA, Caroline Cordeiro Viana e; PEREIRA, Alexsandro Eugenio. A Teoria de Securitização e a sua aplicação em artigos publicados em periódicos científicos. **Revista de Sociologia e Política**, [*s. l.*], v. 27, n. 69, 2019. Disponível em: https://doi.org/10.1590/1678987319276907. Acesso em: 10 Nov. 2021.

SINGER, P W; FRIEDMAN, Allan. **Cybersecurity and cyberwar : what everyone needs to know**. Oxford: Oxford University Press, 2014.

SYMANTEC. **ISTR Internet Security Threat Report Volume 24 |**. [*S. l.: s. n.*], 2019. Disponível em: https://docs.broadcom.com/doc/istr-24-2019-en.

TANNO, Grace. A contribuição da escola de Copenhague aos estudos de segurança internacional. **Contexto Internacional**, [*s. l.*], v. 25, n. 1, p. 47–80, 2003. Disponível em: https://doi.org/10.1590/s0102-85292003000100002. Acesso em: 11 Nov. 2021.

TAQUE, Martín Pecoy. **El proyecto de ley uruguayo del año 2021 que pretende la tipificación de los ciberdelitos en Uruguay**. [*S. l.*], 2021. Disponível em: https://laleyuruguay.com/blogs/novedades/el-proyecto-de-ley-uruguayo-del-ano-2021-que-pretende-la-tipificacion-de-los-ciberdelitos-en-uruguay. Acesso em: 19 Jan. 2022.

TEN, Chee-Wooi; MANIMARAN, Govindarasu; LIU, Chen-Ching. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. **IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans**, [*s. l.*], v. 40, n. 4, p. 853–865, 2010. Disponível em: https://doi.org/10.1109/tsmca.2010.2048028. Acesso em: 11 Dec. 2019.

THE UNITED STATES. **About NIST**. [*S. l.*], 2017. Disponível em: https://www.nist.gov/about-nist. Acesso em: 25 Jan. 2022.

THE UNITED STATES. **DOD Dictionary of Military and Associated Terms As of**. [*S. l.: s. n.*], 2019. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf. Acesso em: 26 Jan. 2022.

THE UNITED STATES. **International Copyright Piracy: A Growing Problem with Links to Organized Crime and Terrorism**. [*S. l.*], 2013. Disponível em: http://commdocs.house.gov/committees/judiciary/hju85643.000/hju85643_0f.htm. Acesso em: 31 Jan. 2022.

THE UNITED STATES. **The White House, The National Strategy to Secure Cyberspace, February 2003. Unclassified. | National Security Archive**. [*S. l.*], 2003. Disponível em: https://nsarchive.gwu.edu/document/21412-document-16. Acesso em: 2 Dec. 2021.

THE UNITED STATES. **USA Patriot Act**. [*S. l.*], 2018. Disponível em: https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2116-usa-patriot-act. Acesso em: 30 Jan. 2022.

THE WHITE HOUSE. **Remarks by the President on Securing Our Nation's Cyber Infrastructure**. [*S. l.*], 2009. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure. Acesso em: 23 Sep. 2020.

THE WHITE HOUSE. **MAY 2011 Prosperity, Security, and Openness in a Networked World**. [*S. l.: s. n.*], 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 10 Nov. 2020.

THE WHITE HOUSE. **National Cyber Strategy**. [*S. l.: s. n.*], 2018. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 23 Sep. 2020.

U.S. EMBASSY IN ARGENTINA. **United States and Argentina Strengthen Partnership on Cyber Policy**. [*S. l.*], 2017. Disponível em: https://ar.usembassy.gov/united-states-argentina-strengthen-partnership-cyber-policy/. Acesso em: 14 Jan. 2022.

UNICEF. **Cyberbullying: O que é e como pará-lo**. [*S. l.*], 2022. Disponível em: https://www.unicef.org/brazil/cyberbullying-o-que-eh-e-como-para-lo#:~:text=Cyberbullying%20%C3%A9%20o%20bullying%20realizado. Acesso em: 27 Jan. 2022.

UNITED NATIONS. **United Nations Information Service Vienna**. [*S. l.*], 2015. Disponível em: http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html. Acesso em: 23 Sep. 2020.

UNITED NATIONS. **E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development With addendum on COVID-19 Response**. [*S. l.*]: United Nations, 2020. Disponível em: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf. Acesso em: 17 Jan. 2022.

UNITED STATES. **Text - S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act of 2014**. [*S. l.*], 2013. Disponível em: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text. Acesso em: 27 Dec. 2021.

US CONGRESS. **Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001**. [*S. l.: s. n.*], 2001. Disponível em: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf. Acesso em: 31 Jan. 2022.

VAMOSI, Robert. **The Myth Of That $1 Trillion Cybercrime Figure | SecurityWeek.com**. [*S. l.*], 2012. Disponível em: https://www.securityweek.com/myth-1-trillion-cybercrime-figure. Acesso em: 23 Sep. 2020.

VILLA, Rafael Antonio Duarte. A segurança internacional no pós-guerra fria: um balanço da teoria tradicional e das novas agendas de pesquisa. **Bib: Revista Brasileira de Informação Bibliográfica em Ciências Sociais**, [*s. l.*], v. 62, n. 2° semestre, p. p. 19-31, 2006.

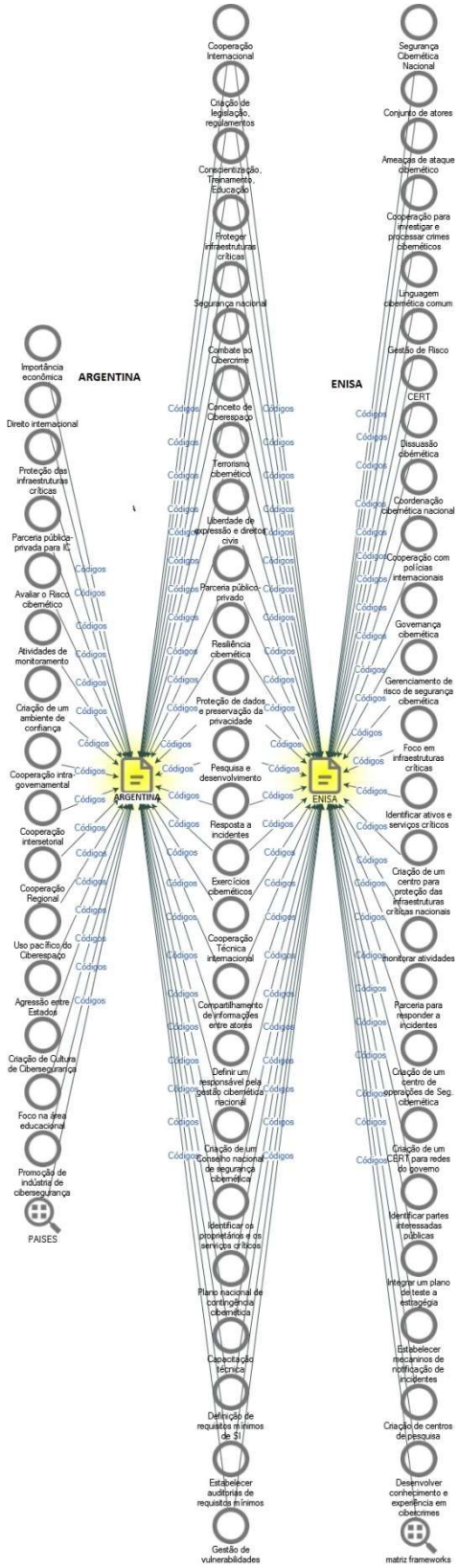
VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cyber security. **Computers & Security**, [*s. l.*], v. 38, n. 1, p. 97–102, 2013. Disponível em: https://doi.org/10.1016/j.cose.2013.04.004. Acesso em: 1 Sep. 2019.

WAEVER, Ole. **Ole Waever — Securitization and Desecuritization.pdf**. [*S. l.*], 1995. Disponível em: https://drive.google.com/file/d/1iyvJ0m1BBM977vzPx8VmviGy32hkzGiX/view. Acesso em: 17 Nov. 2021.

WALTZ, Kenneth N. **Theory of International Politics**. Long Grove, Ill.: Waveland Press, 1979.

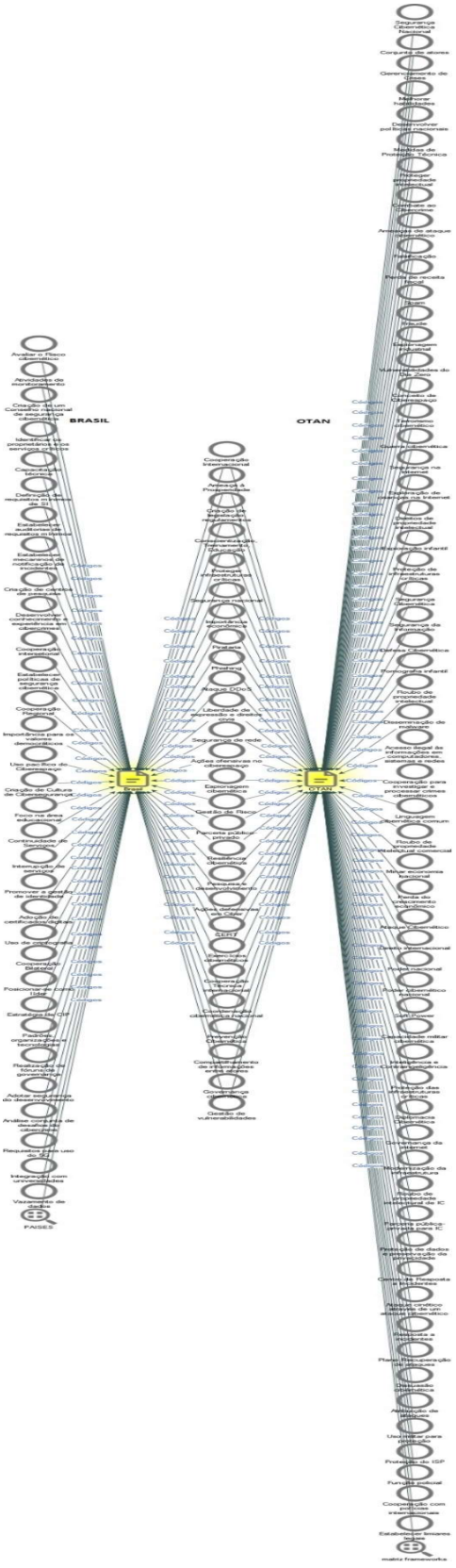
ZETTER, Kim. **Contagem Regressiva Ate Zero Day**. [*S. l.*]: Brasport, 2017.

ANEXO A: Convergência de codificação entre a estratégia Argentina com o framework da ENISA



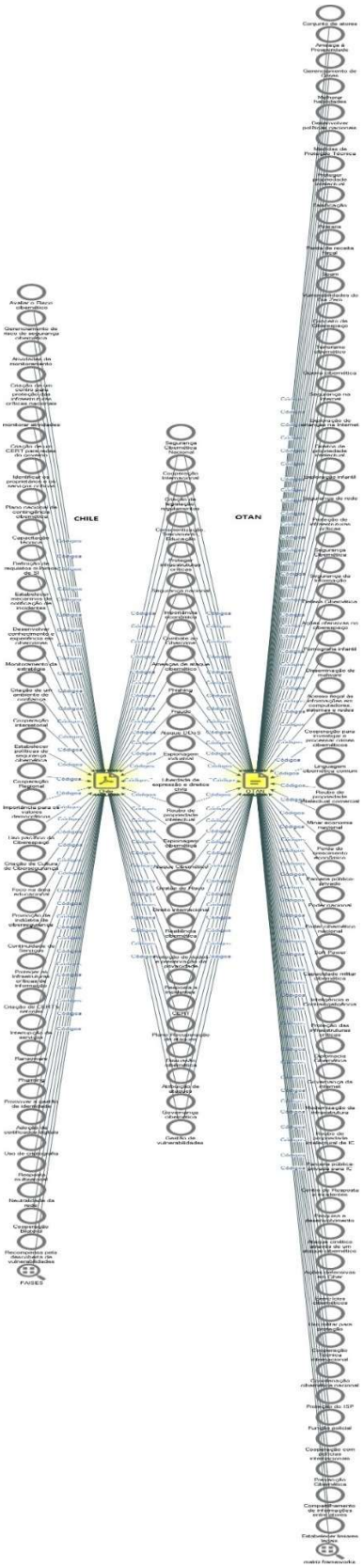
Fonte: Elaborado com dados extraídos por meio da ferramenta Nvivo

ANEXO B: Convergência de codificação entre a estratégia brasileira com o *framework* da OTAN



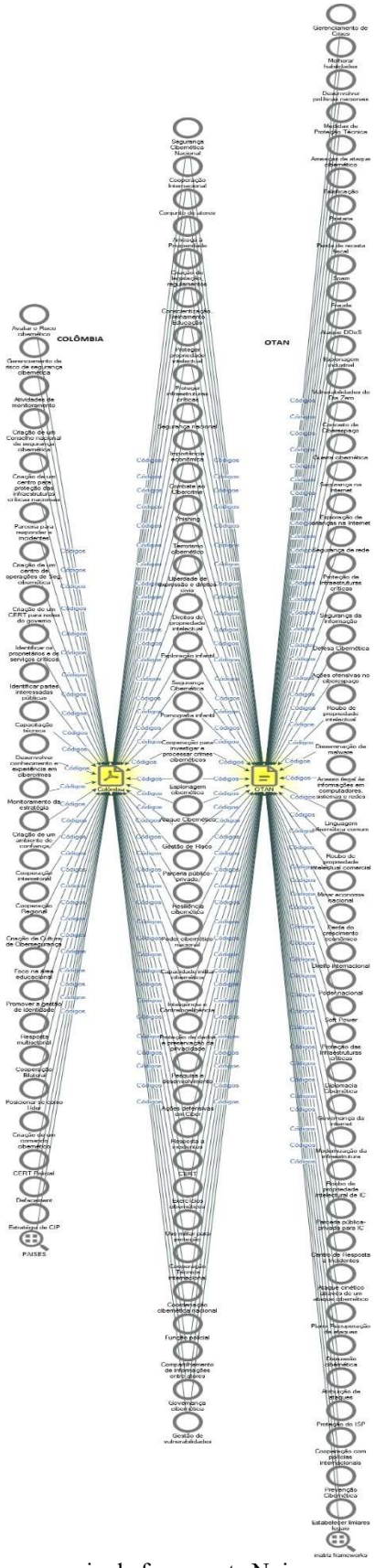
Fonte: Elaborado com dados extraídos por meio da ferramenta Nvivo

ANEXO C: Convergência de codificação entre a estratégia chilena com o *framework* da OTAN



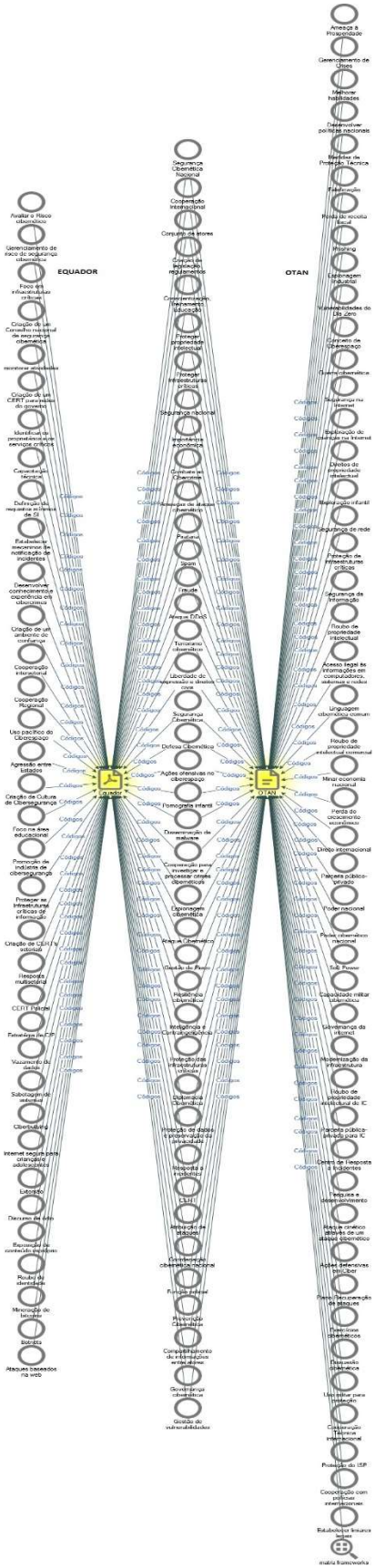
Fonte: Elaborado com dados extraídos por meio da ferramenta Nvivo

ANEXO D: Convergência de codificação entre a estratégia colombiana com o *framework* da OTAN



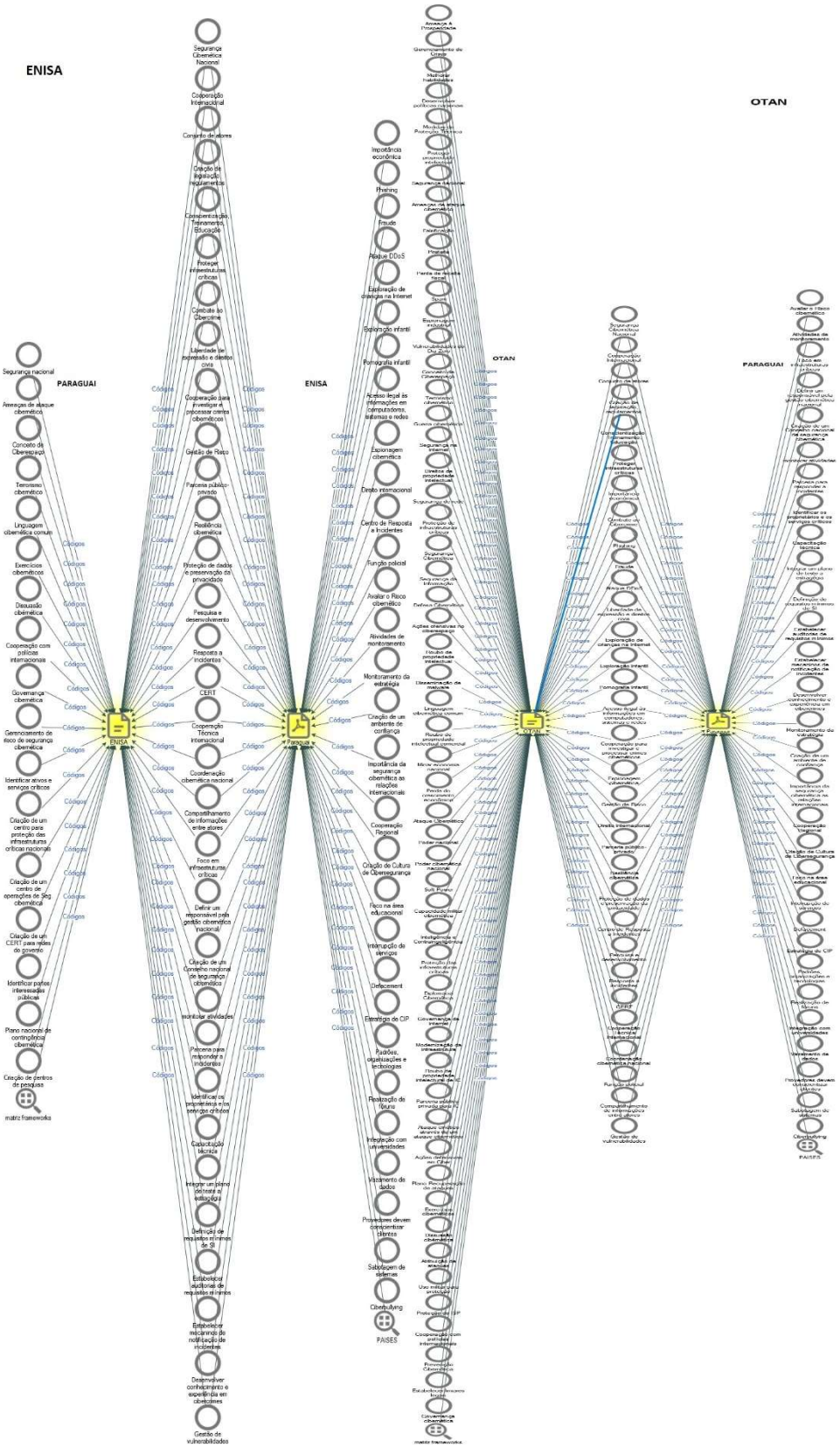
Fonte: Elaborado com dados extraídos por meio da ferramenta Nvivo

ANEXO E: Convergência de codificação entre a estratégia equatoriana com o *framework* da OTAN



Fonte: Elaborado com dados extraídos por meio da ferramenta Nvivo

ANEXO F: Convergência de codificação entre a estratégia paraguaia com os *frameworks* da ENISA e da OTAN



Fonte: Elaborado com dados extraídos por meio da ferramenta Nvivo