Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos

Structural Analysis of Cybersecurity Strategies of Brazil and the United States

Rev. Bras. Est. Def. v. 9, n. 2, jul./dez. 2022, p. 227–250
DOI: 10.26792/RBED.v9n2.2022.75246
ISSN 2358-3932

ISRAEL AONO NUNES
JULIANA ZANIBONI DE ASSUNÇÃO
VITELIO BRUSTOLIN

INTRODUÇÃO

Embora o termo segurança cibernética venha sendo progressivamente cada vez mais utilizado, não existe um entendimento comum quanto à sua definição (Schatz et al. 2017, 54–5). Essa indefinição não causa grandes prejuízos quando a expressão é utilizada informalmente; no entanto, quando a sua aplicação se estende para documentos estatais, tal fato pode causar problemas consideráveis. Isso porque a ausência de uma definição da terminologia entre países, principalmente os mais desenvolvidos no setor (EUA, Rússia e China, por exemplo), dificulta o desenvolvimento de pontos de vista comuns e uma governança no ciberespaço (Schatz et al. 2017, 56).

A defesa cibernética está um nível acima da segurança cibernética, garantindo a execução de processos e atividades, livre de ameaças (Brustolin 2019, 3). A defesa cibernética também ajudaria a melhorar os recursos e os usos da estratégia de segurança (Galinec, Možnik, and Guberina

Israel Aono Nunes — Oficial do Corpo de Fuzileiros Navais da Marinha do Brasil e Especialista em Estudos Estratégicos e Relações Internacionais pela Universidade Federal Fluminense (UFF). E-mail: israelaono@cos.ufrj.br.
Juliana Zaniboni de Assunção — Graduada em Relações Internacionais pela Universidade Federal Fluminense (2020). Mestrado em Estudos Estratégicos da Defesa e Segurança pela Universidade Federal Fluminense (2022). Doutoranda em Estudos Estratégicos de Defesa e Segurança pela Universidade Federal Fluminense. julianazaniboni@id.uff.br.
Vitelio Brustolin — É professor do Instituto de Estudos Estratégicos (INEST) da Universidade Federal Fluminense (UFF) e Research Scientist da Harvard University. E-mail: viteliobrustolin@id.uff.br.
Os autores são gratos a Rachel Elizabeth Herrick e a Alice Ma, pela assistência imprescindível na finalização deste artigo

2017, 274). A segurança cibernética e a defesa cibernética, portanto, funcionam juntas; ou deveriam funcionar (Brustolin 2019, 3).

Feita essa distinção conceitual, a Política Nacional de Defesa do Brasil (PND), "documento de mais alto nível do País em questões de Defesa" (Brasil, PND 2016), aprovada em 1996, reformulada em 2005, atualizada em 2012, e cuja versão mais recente em vigor é de 2016, estabelece que:

> O amplo espectro de possibilidades no ambiente cibernético requer especial atenção à segurança e à defesa desse espaço virtual, composto por dispositivos computacionais conectados em redes ou não, no qual transitam, processam-se e armazenam-se informações digitais, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações, dos quais depende parcela significativa das atividades humanas. (Brasil, PND 2016).

A Estratégia Nacional de Defesa do Brasil, publicada em 2008, atualizada em 2012, e cuja versão em vigor é de 2016, já havia elencado, desde a sua primeira edição, o setor cibernético como estratégico para o Brasil, ao lado dos setores nuclear e espacial (Brasil, END 2016).

Ainda assim, até 2020, o Brasil nunca havia tido uma estratégia de segurança cibernética. Dentre os fatos mais relevantes para a criação do documento, cabe destacar que, em 2014, o Acórdão nº 3.051 TCU-Plenário, apontou a ausência de um planejamento estratégico do Estado brasileiro quanto aos diversos assuntos relacionados à Segurança da Informação na Administração Pública Federal. Dois anos depois, em 2016, a Comissão Parlamentar de Inquérito dos Crimes Cibernéticos sugeriu ao Gabinete de Segurança Institucional da Presidência da República que elaborasse uma proposta de Política Nacional de Segurança da Informação (Brasil, Câmara dos Deputados 2016). Em 2018, foi publicado o Decreto nº 9.637/2018, que Instituiu a Política Nacional de Segurança da Informação (PNSI), sendo que, no seu Art. 2º, define que Segurança da Informação, no âmbito da Administração Pública Federal abrange:

I — a segurança cibernética;

II — a defesa cibernética;

III — a segurança física e a proteção de dados organizacionais; e

IV — as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Finalmente, em 2020, é aprovada a Estratégia Nacional de Segurança Cibernética (também chamada de E-Ciber), por meio do decreto nº 10.222, de 5 de fevereiro, que descreve segurança cibernética como a área mais crítica e atual a ser abordada, e, por este motivo, foi o primeiro módulo da Estratégia Nacional de Segurança da Informação a ser elaborada.

Por outro lado, a formulação de documentos de segurança cibernética tem trajetória mais antiga nos Estados Unidos, onde a Internet foi inventada. Não cabe aqui delinear a história da rede mundial de computadores, mas vale frisar que ela nasceu como empreendimento militar durante a Guerra Fria, sendo inicialmente chamada de Arpanet (Brustolin 2014, 29). Esta foi desmembrada em 1983, de modo que a parte militar formou a Milnet, e a outra, a base da Internet que temos hoje (Abbate 1999; Scott 1995, 2–4). A consciência de que ataques cibernéticos poderiam se tornar instrumentos de guerra desponta já em 2001, no discurso do ex-presidente estadunidense, Bill Clinton, quando lançou um plano nacional para defender o ciberespaço dos Estados Unidos — resultado, segundo ele, de "um esforço de três anos":

> Vivemos em uma época em que uma pessoa sentada em frente a um computador pode ter uma ideia, viajar pelo ciberespaço e levar a humanidade a novas alturas. Ainda assim, alguém pode se sentar em frente ao mesmo computador, invadir um sistema de computadores e potencialmente paralisar uma empresa, uma cidade ou um governo. [...] Hoje, nossos sistemas críticos, desde estruturas de poder, até controle de tráfego aéreo, são conectados e operados por computadores. Devemos tornar esses sistemas mais seguros para que os Estados Unidos possam ser mais seguros. (Clinton 2000, 13–5).[1]

De qualquer forma, conforme mencionado anteriormente, a Estratégia Cibernética Nacional[2] (NCS) dos Estados Unidos, divulgada em setembro de 2018, é apresentada pelo então presidente Donald Trump, como a primeira estratégia "totalmente articulada em 15 anos" (USA, NCS 2018, 1). O documento descreve como a administração irá atuar para:

- Defender a pátria, protegendo redes, sistemas, funções e dados;
- Promover a prosperidade estadunidense, nutrindo uma economia digital segura e próspera e promovendo forte inovação nacional;
- Preservar a paz e a segurança, fortalecendo a capacidade dos Estados Unidos — em conjunto com aliados e parceiros — para deter e, se necessário, punir aqueles que usam ferramentas cibernéticas para fins maliciosos; e
- Expandir a influência estadunidense no exterior para estender os princípios fundamentais de uma política para uma Internet aberta, interoperável, confiável e segura. (USA, NCS 2018, 1).

Cabe destacar que o fato de a Internet ter sido inventada nos Estados Unidos, juntamente com as suas políticas basilares de utilização, justifica que seja feita uma comparação da estratégia cibernética brasileira com a

estadunidense. Neste artigo, portanto, é produzida uma comparação estrutural desses documentos. Em seguida, é desenvolvida uma avaliação qualitativa, com base no *framework* proposto por Luiijf et al. (2013), que se fundamenta na análise de 19 estratégias nacionais de segurança cibernética de 18 países, a partir da qual os autores formataram um modelo estrutural mínimo. Ambas as estratégias que são foco deste artigo são analisadas pelo viés do modelo estrutural supracitado.

O presente estudo se perfaz, portanto, em uma pesquisa exploratória, cuja metodologia é de política comparada, com técnica de coleta de dados de documentação indireta e técnica de análise de dados qualitativa. Na Seção "Um novo domínio operacional" são discutidos alguns conceitos e fatos históricos que norteiam as áreas de segurança e defesa cibernética. A análise metodológica é feita na terceira seção. As considerações finais são apresentadas na última seção.

UM NOVO DOMÍNIO OPERACIONAL

A Internet é "uma arquitetura de sistema que revolucionou as comunicações e os métodos de comércio ao permitir a interconexão de várias redes de computadores em todo o mundo"[3] (Dennis and Kahn, 2020).[4] O ciberespaço — também chamado de espaço cibernético — por sua vez, seria o resultado dos *links* entre computadores e outros dispositivos na Internet:

> Ciberespaço, mundo amorfo, supostamente "virtual" criado por *links* entre computadores, dispositivos habilitados para Internet, servidores, roteadores e outros componentes da infraestrutura da Internet. Ao contrário da própria Internet, entretanto, o ciberespaço é o lugar produzido por esses *links*. (Bussell 2013).[5]

O ciberespaço é o mais novo dos domínios operacionais. Foi apenas em 2016, por exemplo, que o secretário geral da Organização do Tratado do Atlântico Norte (OTAN), Jens Stoltenberg, classificou o ciberespaço como um domínio operacional oficial de guerra (Ablon 2019, 12). Além disso, o ciberespaço tem aspectos peculiares, pois ele permeia todos os outros domínios operacionais:

> As atividades no Espaço Cibernético podem criar liberdade de ação para atividades em outros domínios, assim como atividades em outros domínios, também criam efeitos dentro e através do Espaço Cibernético. O objetivo central da integração dos domínios é a habilidade de se alavancar capacidades de vários domínios para que sejam criados efeitos únicos e, frequentemente, decisivos. (Brasil, Ministério da Defesa 2014, 18).

Cabe destacar que ainda não há um país que tenha total domínio sobre as tecnologias relativas ao ciberespaço. Essas vulnerabilidades podem ser traduzidas em danos substanciais para entes públicos e privados. Nos Estados Unidos, por exemplo, o FBI registrou US$ 4,2 bilhões de prejuízo em crimes cibernéticos, apenas em 2020 (Owaida 2021).[6]

Neste ponto, é crucial apresentar um conceito amplamente empregado de ataque cibernético — também chamado de ciberataque: "uma tentativa de obter acesso ilegal a um computador ou sistema de computadores com o objetivo de causar danos ou prejuízos" (Merriam-Webster's 2018).[7] Ciberataques são um tipo de ciberameaça, também chamada de ameaça cibernética:[8]

> Uma ciberameaça refere-se a qualquer coisa que tenha o potencial de causar sérios danos ao sistema de um computador. Uma ciberameaça é algo que pode ou não acontecer, mas tem potencial para causar sérios danos. As ameaças cibernéticas podem levar a ataques a sistemas de computador, redes e muito mais. (Techopedia 2021).[9]

Hathaway e Crootof (2011) distinguem diferentes tipos de ameaças cibernéticas. Essa distinção também contribui para se verificar as diferenças entre cibercrime e ciberguerra:

Tabela 1
Tipos de ameaças cibernéticas

	Ataque cibernético	**Crime cibernético**	**Guerra cibernética**
Envolve apenas atores não-estatais		√	
Deve ser uma violação da legislação nacional ou internacional, cometida por meio de um sistema de computador		√	
O objetivo deve ser degradar o funcionamento de uma rede de computadores	√		√
Deve ter um objetivo político ou de segurança nacional	√		√
Os efeitos devem ser equivalentes aos de um ataque armado, ou a atividade deve ocorrer no contexto de conflito armado			√

Fonte: Hathaway e Crootof (2011, 833) (tradução própria).

ANÁLISE METODOLÓGICA

Conforme mencionado anteriormente, Luiijf et al. (2013), analisaram 19 estratégias nacionais de segurança cibernética de 18 países. O resultado é a sistematização de pontos em comum e pontos de melhoria, além da propositura de um modelo de estrutura mínima comum para as estratégias. Os autores definem essa estrutura como "um plano de ação baseado em uma visão nacional a fim de alcançar um conjunto de objetivos que contribuem para a segurança do espaço cibernético". (Luiijf et al. 2013, 4).

A Estratégia Nacional de Segurança Cibernética (ENSC) dos seguintes países foi analisada: África do Sul, Alemanha, Austrália, Canadá, Espanha, Estados Unidos, Estônia, França, Holanda, Índia, Inglaterra, Japão, Lituânia, Luxemburgo, Nova Zelândia, República Tcheca, Romênia e Uganda (Luijiif et al. 2013, 4).

Identificando a ausência de um consenso dos termos relacionados à segurança cibernética, os autores demonstraram que:

> Apenas oito nações definiram a noção de segurança cibernética. As outras dez nações utilizam texto descritivo ou algum tipo de entendimento público comum. Isso pode causar mal-entendidos nacional e internacionalmente. Como as nações carecem de uma terminologia cibernética, o tratamento colaborativo das ameaças ao espaço cibernético pode ser dificultado. Além disso, as nações têm uma compreensão diferente sobre qual escopo a segurança cibernética deve cobrir. (Luiijf et al. 2013, 27).

Os autores também descreveram que "dada a natureza global da segurança cibernética, os países podem tirar lições das abordagens aplicadas em outras estratégias nacionais de segurança cibernética". Não obstante, destacaram que como cada país tem um contexto legal, político e cultural diferente, é natural que as estratégias sejam diferentes; no entanto, "como a estratégia nacional de segurança cibernética aborda um risco global, em um mundo conectado, são esperados elementos similares" (Luiijf et al. 2013, 26).

Em sua conclusão, ao considerar as diferentes Estratégias Nacionais de Segurança, os autores propuseram a seguinte estrutura, de nove tópicos fundamentais (o décimo, referente a "anexos", é opcional):

1. Sumário executivo;
2. Introdução;
3. Visão estratégica nacional sobre segurança cibernética;

4. Relação da ENSC com outras estratégias, nacionais e internacionais, e estruturas legais existentes;
5. Metodologias padrão;
6. Relação [geral] com outras estratégias, nacionais e internacionais, e estruturas legais existentes;
7. Objetivos(s) de segurança cibernética, de preferência de um a quatro;
8. Esboço de linhas de ação táticas;
9. Glossário, de preferência baseado em um conjunto internacional de definições;
10. Anexos [opcional], (Luiijf et al. 2013, 26 [tradução própria]).

Nas subseções e na seção a seguir, as estruturas das estratégias cibernéticas do Brasil e dos Estados Unidos serão comparadas entre si, de modo que se possa avaliar se há, ou não, convergência nas ações estratégicas e prioritárias definidas por esses documentos. Na sequência, ambas serão analisadas conforme o *framework* proposto por Luiijf et al.

A estrutura da E-Ciber

A Estratégia Nacional de Segurança Cibernética do Brasil é apresentada como a "orientação manifesta do governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética, e terá validade no quadriênio 2020-2023" (E-Ciber 2020, 1).

O item 1.1 é um sumário executivo e descreve que a referida Estratégia foi desenvolvida a partir de um *benchmarking*, ou seja, uma análise comparativa com documentos de outros países — sem, no entanto, apontar quais países foram analisados.

A introdução, item 1.2, define que "a E-Ciber, além de preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto". (E-Ciber 2020, 2).

O item 1.3, metodologia, descreve que, para o desenvolvimento do documento — e levando em consideração a quantidade de assuntos relacionados à segurança cibernética —, foram constituídos três grupos de estudo:

- Subgrupo 1 — governança cibernética, dimensão normativa, pesquisa, desenvolvimento e inovação, educação, dimensão internacional e parcerias estratégicas;

- Subgrupo 2 — confiança digital e prevenção e mitigação de ameaças cibernéticas;
- Subgrupo 3 — proteção estratégica — proteção do Governo e proteção às infraestruturas. (E-Ciber 2020, 3).

O documento também apresenta as etapas empregadas para sua confecção:

Primeira — Diagnóstico — levantamento e mapeamento de iniciativas, atores relacionados e ações existentes;

Segunda — Debates dos subgrupos — reuniões semanais com os atores relacionados e convidados de notório saber;

Terceira — Consulta pública — disponibilização do documento na Internet para contribuições e ampla participação da sociedade em geral; e

Quarta — Aprovação e publicação — finalização da proposta e submissão à aprovação presidencial. (E-Ciber 2020, 3).

No referido item, 1.3, também são identificados os sete eixos temáticos, que são desdobrados na Parte 2 da Estratégia:

Tabela 4
Eixos Temáticos da E-Ciber

Eixos de Proteção e Segurança	Eixos Transformadores
Governança da segurança cibernética nacional	Dimensão normativa
Universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas	Dimensão internacional e parcerias estratégicas
Proteção estratégica	Pesquisa, desenvolvimento e inovação
	Educação

Fonte: Brasil, E-Ciber 2020, 4.

O item 2.1 define a visão da Estratégia Nacional de Segurança Cibernética para o Brasil como "tornar-se país de excelência em segurança cibernética" (E-Ciber 2020, 4–5).

Os objetivos estratégicos estão identificados no item 2.2:

1. Tornar o Brasil mais próspero e confiável no ambiente digital;
2. Aumentar a resiliência brasileira às ameaças cibernéticas; e
3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

As ações estratégicas, descritas no item 2.3, foram relacionadas a partir "dos aspectos abordados na Parte I — Diagnóstico, e das considerações realizadas sobre a situação da segurança cibernética nacional na Parte II — Análise dos Eixos Temáticos" (E-Ciber, 2020, p. 5).

Na tabela abaixo estão listadas cada uma das 10 ações estratégicas definidas no item 2.3 da E-Ciber:

Tabela 5 — Ações Estratégicas da E-Ciber

Principais Ações
1. Fortalecer as ações de governança cibernética
2. Estabelecer um modelo centralizado de governança no âmbito nacional
3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade
4. Elevar o nível de proteção do Governo
5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais
6. Aprimorar o arcabouço legal sobre segurança cibernética
7. Incentivar a concepção de soluções inovadoras em segurança cibernética
8. Ampliar a cooperação internacional do Brasil em segurança cibernética
9. Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade
10. Elevar o nível de maturidade da sociedade em segurança cibernética

Fonte: Brasil, E-Ciber 2020, 5–9.

Feita essa contextualização, é possível identificar-se uma convergência do documento com a preocupação internacional, uma vez que existem ações previstas para o desenvolvimento de um arcabouço legal para a segurança cibernética. Aqui, cabe pontuar que a dissonância entre países na construção desse arcabouço é descrita por Luiijf et al. (2013) como um dos principais empecilhos para um entendimento internacional sobre cibersegurança.

Na Parte I, "apresenta-se um diagnóstico da segurança cibernética, baseado no cenário internacional e o no cenário nacional, com especial atenção às ameaças, aos ataques e às vulnerabilidades cibernéticas, e ao modo como esses elementos impactam a sociedade e as instituições" (E-Ciber 2020, 3).

A Parte II é a mais extensa da E-Ciber. Nela, são analisados cada um dos eixos temáticos definidos no item 1.3, agrupados em duas categorias, eixos de Proteção e Segurança, bem como eixos Transformadores. Os principais tópicos serão apresentados a seguir.

No item 1.1, são abordados aspectos relativos a: "governança cibernética, a metodologia de gestão de riscos, a confiança e segurança no uso do certificado digital, a implantação de modelo centralizado de coordenação da segurança cibernética nacional, e o monitoramento do cenário cibernético" (E-Ciber 2020, 12).

No item 1.2 é destacada a "relevância de recursos e de mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis, entre instituições públicas e privadas, e entre estas e organizações internacionais" (E-Ciber 2020, 17). Na sequência, o documento enfatiza que "o País necessita, ainda, fortalecer e aperfeiçoar seus órgãos de governo que tratam das ameaças e que combatem os crimes cibernéticos", e que, "uma vez que o CTIR Gov[10] é o órgão central do governo que coordena e realiza ações destinadas à gestão de incidentes computacionais, [...] deve ser fortalecido" (E-Ciber 2020, 19).

O item 1.3, é dedicado à Proteção Estratégica, ou seja, a proteção da infraestrutura crítica brasileira, e define que "as organizações a serem protegidas, escopo desta Estratégia, são as pertencentes ao setor de Telecomunicações, ao setor de Transportes, ao setor de Energia, ao setor de Água e ao setor Financeiro" (E-Ciber 2020, 21).

O item 2.1 é direcionado para a Dimensão Normativa, e destaca os avanços proporcionados pela "aprovação de leis importantes para o País, como a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, e a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD)". Contudo, o item também enfatiza que "o nível de articulação e de normatização das instituições brasileiras nos temas relacionados à segurança cibernética ainda é tímido" (E-Ciber 2020, 24). Uma das conclusões apresentadas neste tópico é a necessidade do desenvolvimento de "ações que aprimorem o arcabouço legal da segurança cibernética nacional, por [se] acreditar que essa iniciativa poderá proporcionar o necessário alinhamento estratégico e normativo às ações do País" (E-Ciber 2020, 25).

O item 2.2, com foco em Pesquisa, Desenvolvimento e Inovação, destaca que "as iniciativas de Pesquisa, Desenvolvimento e Inovação — PD&I, na área de segurança cibernética, necessitam de maior prioridade, com o fim de obter maior investimento, mais pesquisadores capacitados na área, e novos projetos" (E-Ciber 2020, 25–6).

O item 2.3, é denominado Dimensão Internacional e Parcerias Estratégicas, e ressalta que "o Brasil experimenta o fenômeno da quarta revolução industrial, onde as tecnologias ganham maior integração, o mundo físico e o ambiente virtual alcançam elevado grau de interação" (E-Ciber 2020, 27). A Estratégia determina que o Brasil deve "buscar acordos bilaterais de cooperação em segurança cibernética com o maior número possível

de países, como demonstração de nosso intuito em estabelecer, nesse campo, relações que sejam adequadas, profícuas, construtivas e transparentes" (E-Ciber, 2020, 28), e reforça a seguinte diretriz:

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

O item 2.4, último a ser analisado, é direcionado à Educação, assunto extremamente relevante para o contexto atual do país, uma vez que "98% da população possui acesso às redes móveis e 60% dos domicílios têm acesso por meio da rede fixa" (E-Ciber 2020, 29) e as "universidades e instituições não formam especialistas suficientes em segurança cibernética", assunto que, no entanto, "deve ser de conhecimento e de domínio de todos os níveis de ensino" (E-Ciber 2020, 31).

O documento ressalta ainda que, no Brasil, há "poucos profissionais especializados em segurança cibernética; baixa conscientização dos usuários; e poucos programas educacionais focados na área" (E-Ciber 2020, 33). Além disso, é enfatizado que a educação em segurança cibernética deve ser desenvolvida em três áreas: Capacitação: dedicada a "profissionais da área ou com funções que requerem competências na área"; Formação: dedicada a "parcela da sociedade que se encontra nos bancos escolares"; e Conscientização: dedicada à "sociedade e seus setores" (E-Ciber 2020, 30).

A estrutura da CNS

A Estratégia Cibernética Nacional dos Estados Unidos possui a seguinte estrutura:

Pilar 1: Proteger a população, a pátria, e o modo de vida estadunidense.

- Redes e informações federais seguras.
- Infraestrutura crítica segura.
- Combate ao cibercrime e aprimoramento dos relatórios de incidentes.

Pilar 2: Promover a prosperidade estadunidense.

- Promover uma economia digital vibrante e resiliente.
- Promover e proteger a tecnologia dos Estados Unidos.
- Desenvolver uma força de trabalho capacitada em segurança cibernética.

Pilar 3: Preservar a paz através da força.

- Aprimorar a estabilidade cibernética através de normas de comportamento responsável.
- Atribuir e interromper comportamento inaceitável no espaço cibernético.

Pilar 4: Avançar a influência estadunidense.

- Promover uma Internet aberta, segura, interoperável e confiável.
- Construir uma capacidade cibernética internacional.

Cada um dos quatro pilares é ainda dividido em requisitos e ações prioritárias, conforme apresentado Na Tabela 6, a seguir:

A forma de se apresentar a NCS e E-Ciber precisa ser diferente, já que as estruturas de ambas são anacrônicas. Isso ocorre, sobretudo porque, diferentemente da E-Ciber, as ações da NCS são propostas a partir de objetivos pré-definidos, que buscam atender aos pilares apresentados pela Estratégia Nacional de Segurança[11] (USA 2018, 1). Além disso, não existe, na NCS, a etapa de análise inicial, como apresentada pela E-Ciber, para mapear o setor cibernético do país. Outras diferenças e considerações serão pontuadas nas seções a seguir.

Tabela 6
Ações Prioritárias da CNS

Pilares	Requisitos	Ações prioritárias
1 — Proteger a população, a pátria e o modo de vida estadunidense Objetivo — Gerenciar riscos de segurança cibernética para aumentar a segurança e a resiliência das informações e sistemas de informação da nação	Redes e informações federais seguras	Centralizar a administração e a supervisão da segurança cibernética civil federal
		Alinhar gerenciamento de riscos e atividades de tecnologia de informação
		Aprimorar a cadeia de gestão de riscos federal
		Fortalecer a segurança cibernética de empresas prestadoras de serviços
		Assegurar que o governo lidere em ações e atividades inovadoras
	Segurança da infraestrutura crítica	Definir papéis e responsabilidades
		Priorizar ações de acordo com o risco nacional identificado
		Estabelecer empresas de serviço e tecnologia de comunicações como facilitadores de segurança cibernética
		Proteger a democracia
		Incentivar investimentos em segurança cibernética
		Priorizar investimentos e pesquisas nacionais
		Aprimorar a segurança cibernética marítima e de transportes
		Aprimorar a segurança cibernética espacial
	Combater os crimes cibernéticos e desenvolver o reporte de incidentes	Aprimorar resposta e reporte de incidentes
		Modernizar vigilância eletrônica e leis para crimes cibernéticos
		Reduzir ameaças de organizações criminosas internacionais no espaço cibernético
		Aprimorar meios para a prisão de criminosos no exterior
		Fortalecer parceiros nacionais, e a capacidade das forças policiais para o combate ao crime cibernético

Pilares	Requisitos	Ações prioritárias
2 — Promover a prosperidade estadunidense Objetivo: Preservar a influência dos Estados Unidos no ecossistema tecnológico e o desenvolvimento do espaço cibernético como um motor de crescimento econômico, inovação e eficiência	Incentivar uma economia digital vibrante e resiliente	Incentivar um mercado de tecnologia seguro e adaptável
		Priorizar a inovação
		Investir em infraestrutura de próxima geração
		Promover o livre fluxo de dados através das fronteiras
		Manter a liderança dos Estados Unidos em tecnologias emergentes
		Promover o ciclo completo de segurança cibernética
	Incentivar e proteger a tecnologia dos Estados Unidos	Atualizar mecanismos para revisar a operação e investimentos estrangeiros nos Estados Unidos
		Manter um sistema de propriedade intelectual forte e balanceado
		Proteger a confidencialidade e integridade das ideias estadunidenses
	Desenvolver uma força de trabalho capacitada em segurança cibernética	Construir e sustentar um fluxo de talentos
		Expandir oportunidades de capacitação para os trabalhadores estadunidenses
		Aprimorar a força de trabalho federal em segurança cibernética
		Utilizar a autoridade governamental para destacar e recompensar talentos
3 — Preservar a paz através da força Objetivo: Identificar, combater, interromper, degradar, dissuadir comportamentos no espaço cibernético desestabilizadores e contrários aos interesses nacionais, preservando o domínio dos Estados Unidos no e através do espaço cibernético	Aprimorar a estabilidade cibernética através de normas de comportamento responsável	Incentivar a aderência internacional a normas cibernéticas
	Atribuir e interromper comportamento inaceitável no espaço cibernético	Liderar com inteligência objetiva e colaborativa
		Impor consequências
		Construir uma iniciativa de dissuasão cibernética
		Combater influência cibernética mal intencionada e operações de informação

Pilares	Requisitos	Ações prioritárias
4 — Avançar a influência estadunidense Objetivos: Preservar a abertura a longo prazo, interoperabilidade, segurança e confiabilidade da Internet, que apoia e é reforçada por interesses dos Estados Unidos	Promover uma Internet aberta, segura, interoperável e confiável	Proteger e promover a liberdade na Internet
		Trabalhar com países parceiros, indústria, academia e sociedade civil
		Promover um modelo de governança com múltiplos agentes para a Internet
		Promover uma infraestrutura de comunicações interoperável e confiável de conectividade na Internet
		Promover e manter mercados mundiais para tecnologia dos Estados Unidos
	Construir uma capacidade cibernética internacional	Aprimorar esforços para desenvolvimento de capacidade cibernética

Fonte: Elaboração própria.

Aplicação do modelo estrutural

A Tabela 7, a seguir, delineia as estruturas das estratégias cibernéticas brasileira e estadunidense, a partir do modelo proposto por Luiijf et al. (2013, 26):

Tabela 7
Comparação: E-Ciber e NCS

Tópico	Brasil (E-Ciber)	Estados Unidos (NCS)
1. Sumário Executivo	√ (p. 1)	
2. Introdução	√ (p. 1)	√ (p. 1)
3. Visão estratégica nacional sobre segurança cibernética	√ (p. 4)	
4. Relação da ENSC com outras estratégias, nacionais e internacionais, e estruturas legais existentes	√ (p. 1)	√ (p. 3)
5. Metodologia padrão	√ (p. 2–3)	
6. Relação [geral] entre outras estratégias, nacionais e internacionais, e estruturas legais existentes	√ (p. 1)	
7. Objetivo(s) de segurança cibernética, de preferência de um a quatro	√ (p. 4–5)	√ (p. 6, 14, 20 e 24)
8. Esboço das linhas de ação táticas	√	√
9. Glossário, de preferência baseado em um conjunto internacional de definições		
10. Anexos [opcional]		

Fonte: Elaboração própria.

A Estratégia Nacional de Segurança Cibernética brasileira possui todos os tópicos fundamentais propostos por Luiijf et al. (2013, 26), exceto o glossário — que foi publicado em documentos separados por ambos os países — enquanto foi possível identificar claramente apenas quatro dos nove tópicos propostos no documento estadunidense. Novamente cabe ressaltar que o décimo tópico, anexos, não é fundamental, mas opcional.

Cada estratégia encaixada no *framework* apresentado acima aborda um risco global, além disso, "em um mundo conectado, são esperados elementos similares" (Luiijf et al. 2013, 26). Logo, quando os autores enfatizam a necessidade de elementos como um glossário, de preferência baseado em um conjunto internacional de definições, ou a relação da ENSC com outras estratégias, nacionais e internacionais, e estruturas legais existentes, estão procurando conectar as estratégias, de modo que atuem com problemas transnacionais, tais quais ataques e crimes cibernéticos em geral.

Nas considerações finais, abaixo, será avaliado se essa diferença estrutural entre os documentos brasileiro e estadunidense se refletem em incongruências nas ações prioritárias previstas por ambos.

CONSIDERAÇÕES FINAIS

Apesar da diferença estrutural, identificada na comparação a partir do modelo proposto por Luiijf et al. (2013), ao analisarmos as ações estratégicas definidas pela E-Ciber, é possível constatar uma convergência com as ações prioritárias determinadas pela NCS, conforme apresentado na Tabela 8, a seguir. Esse é um indicativo de que foi realizado um benchmarking nas estratégias de outros países no desenvolvimento do documento brasileiro, como descrito na própria E-Ciber.

Tabela 8
Comparação das ações propostas pelas estratégias do Brasil e dos EUA

Ações estratégicas: E-Ciber[12]	Requisitos e ações prioritárias: NCS[13]
Fortalecer as ações de governança cibernética	Promover um modelo de governança da Internet com múltiplos participantes
Estabelecer um modelo centralizado de governança no âmbito nacional	Centralizar ainda mais o gerenciamento e a supervisão da segurança cibernética civil em âmbito federal
Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade	Trabalhar com países, indústrias, academia e membros da sociedade civil com interesses convergentes

Ações estratégicas: E-Ciber[12]	Requisitos e ações prioritárias: NCS[13]
Elevar o nível de proteção do Governo	Garantir que o governo utilize as melhores e mais modernas práticas
Elevar o nível de proteção das Infraestruturas Críticas Nacionais	Proteger infraestruturas críticas
Aprimorar o arcabouço legal sobre segurança cibernética	Aumentar a estabilidade cibernética por meio de normas de comportamento e de responsabilidade
Incentivar a concepção de soluções inovadoras em segurança cibernética	Promover e proteger as inovações desenvolvidas nos Estados Unidos
Ampliar a cooperação internacional do Brasil em segurança cibernética	Construir uma capacidade cibernética internacional
Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade	Desenvolver uma força de trabalho capacitada em segurança cibernética
Elevar o nível de maturidade da sociedade em segurança cibernética	Promover uma Internet aberta, interoperável, confiável e segura

Fonte: Elaboração própria.

Conforme descrito no próprio documento, a Estratégia Nacional de Segurança Cibernética do Brasil foi desenvolvida com base em uma metodologia *bottom-up*. Para o desenvolvimento dessa metodologia, foram realizadas reuniões de diagnóstico, debates e consultas públicas. A E-Ciber descreve que essas consultas permitiram "o levantamento de informações relevantes, que resultariam numa concepção estratégica nacional sistêmica". (E-Ciber 2020, 4).

Também é notório que, para a efetivação dessa metodologia, primeiramente foi produzido um diagnóstico do cenário cibernético nacional e, em um segundo momento, foram analisados os eixos temáticos identificados. O próprio documento esclarece que "em virtude da análise diagnóstica e do estudo dos eixos temáticos, apresentam-se os objetivos estratégicos e, em seguida, as ações estratégicas elaboradas com o fim de atingir os objetivos especificados" (E-Ciber 2020, 3).

Por outro lado, a Estratégia Cibernética Nacional dos Estados Unidos foi desenvolvida de acordo com os pilares descritos na Estratégia Nacional de Segurança. Desse modo, primeiramente foram definidos os requisitos a serem atendidos e, em seguida, descritas as ações prioritárias para alcançar tal finalidade. Um modelo *top-down* sempre se inicia com uma decisão inicial das autoridades governamentais; a partir do momento que os objetivos são definidos, a política é desenvolvida pelos escalões subordinados de modo que corresponda às expectativas definidas na decisão inicial (Watson

2014, 447). Desta maneira, podemos caracterizar o desenvolvimento da NCS como *top-down*, uma vez que antes que o documento fosse desenvolvido, os objetivos a serem atingidos já estavam definidos.

Quando as duas estratégias são comparadas a partir do modelo proposto por Luiijf et al. (2013), verificamos que ambas são consideravelmente diferentes, mesmo que a sua proposta seja fundamentalmente a mesma. No entanto, o modelo proposto relaciona apenas os tópicos comuns que deveriam ser apreciados por qualquer ENSC. Desse modo, ao invés de se aprofundar em divergências entre os documentos, destaca pontos de convergência que deveriam existir.

Logo, quando verificamos que o documento brasileiro aplicou a metodologia *bottom-up* em sua estruturação, enquanto que o estadunidense aplicou metodologia *top-down*, evidencia-se uma das principais razões para os documentos divergirem tanto estruturalmente. Ainda assim, conforme pontuado na Tabela 8, as ações estratégicas da E-Ciber e as ações prioritárias da NCS são convergentes.

Além disso, a análise estrutural nos permite concluir mais dois pontos:

1. A partir do modelo proposto por Luiijf et al. (2013), pode-se comprovar que a estratégia brasileira passou por um "*benchmarking* sobre estratégias correlatas de outros países" (E-Ciber 2020, 2). Isso é evidenciado pelo fato de que todos os tópicos elencados por Luiijf et al. estão presentes em sua estrutura. Curiosamente, apesar de a E-Ciber possuir uma seção de Referências, onde 66 documentos, artigos e obras são apresentados, o trabalho de Luiijf et al. não foi citado. Provavelmente, o trabalho desses autores chegou até a E-Ciber por intermédio do exemplo de estrutura de outras estratégias produzidas após a publicação do artigo, em 2013.
2. Complementarmente, ao compararmos a metodologia de desenvolvimento da E-Ciber com a NCS, podemos concluir que:
   2.1. o modelo estadunidense não foi utilizado como base para o brasileiro, o que seria pouco usual, dado que a Internet e suas diretrizes fundamentais foram criadas nos EUA e a NCS foi publicada quase um ano e meio antes que a E-Ciber; ou
   2.2. o modelo estadunidense foi pouco utilizado, sendo preterido em favor de outros, uma vez que as metodologias aplicadas em ambas as estratégias são fundamentalmente opostas e a estrutura delas é consideravelmente diferente. Esta conclusão parece ser a mais provável, sobretudo quando se constata a convergência identificada nas ações propostas em ambos os documentos.

Desse modo, a metodologia e o recorte deste artigo permitiram a comparação estrutural da Estratégia Nacional de Segurança Cibernética do Brasil e da Estratégia Cibernética Nacional dos Estados Unidos. Ao longo da primeira seção, foram apresentadas as premissas dessa análise. Os conceitos e a contextualização histórica que norteiam a segurança e defesa cibernética — bem como o fato de que o espaço cibernético é um novo domínio operacional para as forças armadas — foram discutidos na segunda seção. Na seção subsequente, foi feita a descrição da estrutura básica das estratégias que são objetos deste estudo, assim como a análise metodológica.

Evidentemente, diversas outras análises ainda poderão ser produzidas, aprofundando cada diretriz dessas estratégias nacionais de segurança cibernética. Contudo, não há avaliação de mérito que possa ser produzida sem a prévia ambientação histórica, conceitual e estrutural dos documentos comparados.

REFERÊNCIAS

Abbate, Janet. 1999. *Inventing the Internet.* Cambridge: MIT Press.

Ablon, Lillian et al. 2019. *Operationalizing Cyberspace as a Military Domain:* Lessons for NATO. Santa Monica, CA: RAND Corporation. www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf

Barak, Ohad. 2015. *Cyber Warfare Revolution? 1982-2014.* Bar-Ilan University. Department of Political Studies. DOI:10.1016/S2212-5671(15)01077-1, www.academia.edu/27917250/Cyber_Warfare_Revolution_1982_2014

Bendovcshi, Andreea. 2015. *Cyber-attacks — Trends, patterns and security countermeasures.* Bucharest Academy of Economic Studies. DOI: 10.1504/IJCIS.2013.051608. www.sciencedirect.com/science/article/pii/S2212567115010771?via%3Dihub.

Bing, Christopher, and Joel Schectman. 2019. *Inside the UAE's secret hacking team of American mercenaries.* Reuters. www.reuters.com/investigates/special-report/usa-spying-raven.

Brasil. Câmara dos Deputados. 2016. "Relatório sobre crimes cibernéticos faz recomendações a outros órgãos". *Agência Câmara de Notícias.* www.camara.leg.br/noticias/486619-relatorio-sobre-crimes-ciberneticos-faz-recomendacoes-a-outros-orgaos/.

Brasil. Ministério da Defesa. 2014. *Doutrina Militar de Defesa Cibernética.* Estado Maior Conjunto das Forças Armadas: MD31-M-08

Brasil. Tribunal de Contas da União. 2014. *Acórdão nº 3.051 TCU-Plenário*. www.cjf.jus.br/publico/biblioteca/Acord%C3%A3o%2030512014.pdf.

Brasil. 2021. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. www.ctir.gov.br.

Brasil. 2016. Estratégia Nacional de Defesa — END. Decreto Legislativo nº 179, de 2018.

Brasil. 2020. Estratégia Nacional de Segurança Cibernética — E-Ciber. Decreto nº 10.222, de 5 de fevereiro de 2020.

Brasil. 2016. Política Nacional de Defesa — PND. Decreto Legislativo nº 179, de 2018.

Brasil. 2018. Política Nacional de Segurança da Informação — PNSI, Decreto nº 9.637, de 26 de dezembro de 2018.

Brustolin, Vitelio. 2019. "Comparative Analysis of Regulations for Cybersecurity and Cyber Defence in the United States and Brazil". *Revista Brasileira de Estudos de Defesa* 6, no. 2 (Jul./Dez.): 93-123. DOI 10.26792/RBED.v6n2.2019.75149, 2019. https://rbed.abedef.org/rbed/article/view/75149.

Brustolin, Vitelio. 2014. *Inovação e desenvolvimento via Defesa Nacional nos EUA e no Brasil*. Tese (Doutorado), UFRJ; Harvard. https://scholar.harvard.edu/brustolin/phd-thesis.

Bussell, Jennifer. 2020. *Cyberspace*. Encyclopaedia Britannica. www.britannica.com/topic/cyberspace.

Cavelty, Myriam Dunn. 2012. "The Militarisation of Cyber Security as a Source of Global Tension". In *Strategic Trends 2012:* Key Developments in Global Affairs, edited by D. Mockly. Zurich: Center for Security Studies (CSS), ETH Zurich. https://ssrn.com/abstract=2007043.

CISCO Cisco Systems, Inc. 2021. *Common types of cyber attacks*. www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

Clausewitz, Carl von. 1976. *On War*, edited by Michael Howard, and Peter Paret. Princeton: Princeton University Press. Publicado originalmente em 1832.

Clausewitz, Carl von. 1980. *Vom Kriege* 19. ed., edited by Werner Hahlweg (Hinterlassenes Werk des Generals Carl von Clausewitz. Vollständige Ausgabe im Urtext. Troisdorf: Dümmler). Publicado originalmente em 1832.

Clinton, William J. 2000. "Remarks on the National Plan for Information Systems Protection and an Exchange with Reporters". In *Public Papers of the Presidents of the United States*. Book I: 13–5 (Jan.). U. S. Government Publishing Office. www.govinfo.gov/content/pkg/PPP-2000-book1/html/PPP-2000-book1-doc-pg13-2.htm.

Daultrey, Sally. 2017. *Cyber Warfare:* A Primer. SSRN. DOI: http://dx.doi.org/10.2139/ssrn.3803732. https://ssrn.com/abstract=3803732.

Dennis, Michael Aaron, and Robert Kahn. 2020. "Internet". *Encyclopaedia Britannica*. www.britannica.com/technology/Internet.

Galinec, Darko, Darko Možnik, and Boris Guberina. 2017. "Cybersecurity and cyber defence: national level strategic approach". *Automatika Journal for Control, Measurement, Electronics, Computing and Communications*. DOI: 10.1080/00051144.2017.1407022, www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022?scroll=top&needAccess=true.

Galinec, Darko, Darko Možnik, and Boris Guberina. 2017. "Cybersecurity and cyber defence: national level strategic approach". *Automatika, Journal for Control, Measurement, Electronics, Computing and Communications* 58, no. 3: 27–86. DOI: 10.1080/00051144.2017.1407022.

Giles, Christopher. 2020. "Nagorno-Karabakh: The Armenian-Azeri 'information wars'". *BBC News*. www.bbc.com/news/world-europe-54614392.

Greathouse, Craig B. 2014. *Cyberspace and International Relations Theory, Prospects and Challenges; Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?* Dahlonega, GA, USA: University of North Georgia. DOI: 10.1007/978-3-642-37481-4.

Hathaway, Oona A.; Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Sppiegel. 2011. *The Law of Cyber-Attack*. Faculty Scholarship Series. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.

Jacobsen, Jeppe Teglskoy. 2014. "Clausewitz and the Utility of Cyberattacks in War". *International Journal of Cyber Warfare and Terrorism*. Copenhagen: Danish Institute for International Studies. DOI: 10.4018/ijcwt.2014100101. https://dl.acm.org/doi/abs/10.4018/ijcwt.2014100101.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 2013. "Nineteen National Cyber Security Strategies". *International Journal of Critical Infrastructures (IJCIS)* 9, no. 1/2. DOI: 10.1504/IJCIS.2013.051608.

Merriam-Webster's. *Merriam-Webster's Collegiate Dictionary*. 2018. 11. ed. Springfield: Merriam-Webster Incorporated. www.merriam-webster.com/dictionary/cyberattack.

Owaida, Amer. 2021. "FBI: Cybercrime losses topped US$ 4.2 billion in 2020". *We Live Security*. www.welivesecurity.com/2021/03/18/fbi-cybercrime-losses-topped-us42billion-2020.

Rosencrance, Linda. 2019. "Definition: Cyberwarfare". *TechTarget*. https://searchsecurity.techtarget.com/definition/cyberwarfare.

Schatz, Daniel, Rabih Bashroush, and Julie Wall. 2017. "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law* 12. DOI: 10.15394/jdfsl.2017.1476. https://commons.erau.edu/jdfsl/vol12/iss2/8/.

Scott, Ruthfield. 1995. "The Internet's History and Development from Wartime Tool to the Fish-Cam". *Crossroads Magazine* 2, no. 1 (Set.). DOI: 10.1145/332198.332202. https://dl.acm.org/doi/10.1145/332198.332202.

Techopedia. 2021. *Cyberthreat*. Techopedia Inc. www.techopedia.com/definition/25263/cyberthreat.

USA, United States of America. 2018. *National Cyber Strategy of the United States of America*. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em 18 de maio de 2022.

USA, United States of America. 2017. *National Security Strategy of the United States of America*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Walls, Andrew, Earl Perkins, and Juergen Weiss. 2013. *Definition: Cybersecurity*. Stamford, USA: Gartner Inc.

Watson, Nigel. 2014. "IWRM in England: bridging the gap between top-down and bottom-up implementation". *International Journal of Water Resources Development* 30, no. 3: 445–59, DOI: 10.1080/07900627.2014.899892.

Zelalem, Zecharias. 2020. "An Egyptian cyber attack on Ethiopia by hackers is the latest strike over the Grand Dam". *Quartz Africa*. https://qz.com/africa/1874343/egypt-cyber-attack-on-ethiopia-is-strike-over-the-grand-dam.

Zinets, Natalia. 2016. "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'". *Reuters*. www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC.

NOTAS

1. "*We live in an age when one person sitting at one computer, can come up with an idea, travel through cyberspace, and take humanity to new heights. Yet, someone can sit at the same computer, hack into a computer system and potentially paralyze a company, a city, or a government. (…) Today, our critical systems, from power structures to air traffic control, are connected and run by computers. We must make those systems more secure so that America can be more secure.*"
2. "National Cyber Strategy."
3. "*Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect.*"
4. www.britannica.com/technology/Internet.
5. www.britannica.com/topic/cyberspace. "*Cyberspace, amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links.*"
6. www.welivesecurity.com/2021/03/18/fbi-cybercrime-losses-topped-us-42billion-2020.
7. "*Definition of cyberattack: an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm.*"
8. "*Cyberthreat.*"
9. "*A cyberthreat refers to anything that has the potential to cause serious harm to a computer system. A cyberthreat is something that may or may not happen, but has the potential to cause serious damage. Cyberthreats can lead to attacks on computer systems, networks and more.*" (Techopedia 2021).
10. "Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo." Vide: www.ctir.gov.br.
11. "National Security Strategy."
12. Brasil, E-Ciber 2020, 5–9.
13. USA, NCS (2018, "Table of Contents").

ANÁLISE ESTRUTURAL DAS ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA DO BRASIL E DOS ESTADOS UNIDOS

RESUMO

Comparação estrutural da Estratégia Nacional de Segurança Cibernética do Brasil com a Estratégia Cibernética Nacional dos Estados Unidos, além de análise fundamentada no *framework* proposto por Luiijf et al. (2013). Na conclusão, demonstra-se que a Estratégia brasileira foi desenvolvida com metodologia *bottom-up*, enquanto a estadunidense foi estruturada com metodologia *top-down*.

Palavras-chave: Estratégia de Segurança Cibernética; Estratégia de Defesa Cibernética; Brasil; Estados Unidos.

ABSTRACT

In this paper we make a structural comparison of Brazil's National Cybersecurity Strategy with the National Cyber Strategy of the United States. In addition, we also perform an analysis based on the framework proposed by Luijiif et al. (2013). In the conclusion, we demonstrate that the Brazilian Strategy was developed with bottom-up methodology, while the US Strategy was structured with top-down methodology.

Keywords: Cybersecurity Strategy; Cyber Defense Strategy; Brazil; United States.

Recebido em 28/04/2021. Aceito para publicação em 24/05/2023.