ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

CARLA MORENA VITORIA GOMES SILVA

TERRITORIALIZAÇÃO DE QUESTÕES DESTERRITORIAIS: ANÁLISE DAS POLÍTICAS PÚBLICAS ESTADUNIDENSES DE CIBERSEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Rio de Janeiro
2025

CARLA MORENA VITORIA GOMES SILVA

TERRITORIALIZAÇÃO DE QUESTÕES DESTERRITORIAIS: ANÁLISE DAS POLÍTICAS PÚBLICAS ESTADUNIDENSES DE CIBERSEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Texto apresentado como Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares

Orientador: Prof. Dr. LUIZ ROGÉRIO FRANCO GOLDONI

Rio de Janeiro
2025

S586t Silva, Carla Morena Vitoria Gomes.

Territorialização de questões desterritoriais : Análise de políticas públicas estadunidenses de Cibersegurança de Infraestruturas Críticas. / Carla Morena Vitoria Gomes Silva. - 2025.
126 f. : il. ; 30 cm.

Orientação: Dr. Luiz Rogério Franco Goldoni.
Dissertação (Mestrado em Ciências Militares)— Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2025.
Bibliografia: f. 112-126

1.Ciberespaço. 2.Cibersegurança. 3.Infraestruturas Críticas. 4.Estados Unidos . 5.Territorialização I. Título.

CDD 355

CARLA MORENA VITORIA GGOMES SILVA

TERRITORIALIZAÇÃO DE QUESTÕES DESTERRITORIAIS: ANÁLISE DAS POLÍTICAS PÚBLICAS ESTADUNIDENSES DE CIBERSEGURANÇA DE INFRAESTRUTURAS CRÍTICAS.

Dissertação apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Mestre em Ciências Militares.

Aprovada em 29 de janeiro de 2025.

BANCA EXAMINADORA

LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Presidente
Escola de Comando e Estado-Maior do Exército – ECEME

BRENO PAULI MEDEIROS – Prof Dr - Membro
Escola de Comando e Estado-Maior do Exército – ECEME

BIANCA KREMER NOGUEIRA CORREA – Profª Drª – Membro
Fundação Getúlio Vargas – FGV

Ciente:

CARLA MORENA VITORIA GOMES SILVA – Postulante
Escola de Comando e Estado-Maior do Exército – ECEME

AGRADECIMENTOS

A minha família, por terem sido minha âncora ao longo de toda a minha trajetória pessoal. Agradeço, em especial, aos meus pais, Carlos e Rose, por representarem mais do que consigo expressar em palavras. À minha irmã, Camilla Morena, minha eterna super-heroína, e ao meu cunhado, Caio, cuja gentileza é incomparável.

Ao meu orientador, Professor Luiz Rogério Franco Goldoni, por seu zelo, confiança, paciência e conselhos inestimáveis. Sem suas orientações, este trabalho não teria alcançado a viabilidade necessária.

Aos meus amigos, que me acompanharam durante toda essa jornada, peço desculpas pela ausência nos últimos tempos e agradeço por permanecerem ao meu lado, mesmo à distância. Em especial, agradeço a Thamiris Cristini, Marina Moreno e Isabelle Mattos, cuja presença foi essencial para que esta dissertação fosse concluída com êxito. Aos meus amigos de turma – Caio, Nicole, Lucas, Pollyanna, Bruna, Borges, Fortunato e Carlos –, sou eternamente grata por ter compartilhado com vocês esses dois anos tão especiais

Por fim, agradeço à Escola de Comando e Estado-Maior do Exército, ao Instituto Meira Mattos e a todo o seu corpo docente e administrativo pela assistência prestada ao longo desses anos, e à CAPES, pelo apoio financeiro indispensável para a viabilização desta pesquisa.

RESUMO

A natureza parcialmente imaterial do ciberespaço suscita desafios à segurança nacional. A operacionalização do espectro eletromagnético questiona a lógica zonal de território e impulsiona os Estados a construir fronteiras em um domínio que inicialmente foi concebido como ‘livre’. Diante deste contexto, esta pesquisa busca responder a seguinte pergunta: Como as políticas de cibersegurança para infraestruturas críticas dos Estados Unidos refletem uma tensão entre as abordagens territorializantes e liberais do ciberespaço? Como hipótese, postula-se que, nas políticas de cibersegurança dos Estados Unidos, existe uma distinção entre a 'camada superior' do ciberespaço, na qual prevalece uma abordagem liberal que enfatiza a livre circulação de informações, e a 'camada inferior', que adota uma postura mais protecionista focada na segurança das infraestruturas críticas. Tal diferenciação reforça a necessidade de que o ciberespaço seja compreendido por intermédio de uma abordagem estratificada. O objetivo geral consiste em analisar as estratégias de cibersegurança para infraestruturas críticas dos Estados Unidos no século XXI, com o intuito de identificar e compreender como essas estratégias refletem uma tensão entre as abordagens territorializantes e liberais do ciberespaço. O caminho metodológico a ser percorrido será o da Análise de Conteúdo, usando como base documental as estratégias e políticas públicas estadunidenses que versem sobre o ciberespaço.

Palavras-chave: Ciberespaço; Cibersegurança; Infraestruturas Críticas; Estados Unidos; Territorialização

ABSTRACT

The inherently immaterial nature of cyberspace poses distinct challenges to national security. The operationalization of the electromagnetic spectrum challenges traditional territorial logics and compels states to delineate boundaries in a realm once perceived as 'free.' This research aims to answer the following question: How do the cybersecurity policies for critical infrastructures in the United States reflect the tension between territorial and liberal approaches to cyberspace? The hypothesis suggests that in the cybersecurity policies of the United States, there is a bifurcation between the 'upper layer' of cyberspace, where a liberal approach that emphasizes the free circulation of information predominates, and the 'lower layer', which embraces a more protectionist stance centered on the security of critical infrastructures. This dichotomy highlights the imperative for cyberspace to be conceptualized through a stratified approach. The overarching goal is to scrutinize the cybersecurity strategies for critical infrastructures in the United States during the 21st century, aiming to discern and comprehend how these strategies epitomize the tension between territorializing and liberal paradigms of cyberspace. The methodological tool used in this work is that of Content Analysis, using U.S. public strategies and policies concerning cyberspace as the documentary basis.

Keywords: Cyberspace; Cybersecurity; Critical Infrastructure; United States; Territorialization

LISTA DE QUADROS E FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Análise de Conteúdo
AFCYBER	Air Force Cyber Command
ARPANET	Advanced Research Projects Agency Network
BID	Base Industrial de Defesa
CATs	Cyber Action Teams
CCIPS	Computer Crime and Intellectual Property Section
CDCiber	Centro de Defesa Cibernética
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Cyber Investigative Section
CNI	Critical National Infrastructure
CNMF	Cyber National Mission Force
ComDCiber	Comando de Defesa Cibernética
COPS	Community Oriented Policing Services
CPTs	Cyber Protection Teams
CRM	Criminal Division
CSD	Cybersecurity Division
CSIC	Cyberspace Solarium Commission
CSNU	Conselho de Segurança das Nações Unidas
CSS	Central Security Service
DDoS	Distributed Denial of Service
DFI	Declaration for the Future of the Internet
DHS	Department of Homeland Security
DoD	Department of Defense
DoDIN	Rede de Informação do Departamento de Defesa
DOJ	Department of Justice
ECTFs	Eletronic Crimes Task Forces
END	Estratégia Nacional de Defesa
ESG	Election Security Group
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCTFs	Financial Crimes Task Forces

FEMA	Federal Emergency Management Agency
FISC	*Foreign Intelligence Surveillance Court*
FLTCYBER	Fleet Cyber Command
GAO	Government Accountability Office
GGE	United Nations Group of Governmental Experts
IAEA	Agência Internacional de Energia Atômica
IC3	Internet Crime Complaint Center
ICs	Infraestruturas Críticas
IOD	Integrated Operations Division
IP	Internet Protocol
ISD	Infrastructure Security Division
ISR	Intelligence, Surveillance and Reconnaissance
JFCC-NW	Joint Functional Component Command - Network Warfare
FHQ-DODIN	Joint Force Headquarters - DOD Information Network
JMD	Justice Management Division
JTF-CND	Joint Task Force - Computer Network Defense
JTF-CNO	Joint Task Force - Computer Network Operations
JTF-GNO	Joint Task Force - Global Network Operations
MARFORCYBER	Marine Corps Forces Cyberspace Command
MCEN	Marine Corps Enterprise Network
NCD	National Cyber Director
NCIJTF	National Cyber Investigative Joint Task Force
NCS	National Cybersecurity Strategy
NDAA	National Defense Authorization Act
NDS	National Defense Strategy
NMTs	National Mission Teams
NPPD	National Protection and Programs Directorate
NPSA	National Protective Security Authority
NSA	National Security Agency
NSC	National Security Council
NSHS	National Strategy For Homeland Security
NSS	National Security Strategy
OEWG	Open-Ended Working Group

ONCD	Office of National Cyber Director
OTAN	Organização do Tratado do Atlântico Norte
PCIPB	President's Critical Infrastructure Protection Board
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PND	Política Nacional de Defesa
PNCiber	Política Nacional de Cibersegurança
R.I	Relações Internacionais
RMA	Revolution in Military Affairs
SCADA	Supervisory Control and Data Acquisition
SED	Stakeholder Engagement Division
SIGINT	Signals Intelligence
SVR	Foreign Intelligence Service
TCP	Transmission Control Protocol
TICs	Tecnologias de Informação e Comunicação
TNP	Tratado de Não Proliferação de Armas Nucleares
TPP	Parceria Transpacífica
UCSSPACECOM	United States Space Command
USCYBERCOM	United States Cyber Command
URSS	União das Repúblicas Socialistas Soviéticas
USCBP	U.S. Customs and Border Protection
USINDOPACOM	United States Indo-Pacific Command
USSOUTHCOM	United States Southern Command
USSS	United States Secret Service

Sumário

INTRODUÇÃO

A revolução técnico-científica ocorrida na década de 1970 desencadeou transformações que impulsionaram avanços significativos nas áreas da microeletrônica e telecomunicações. Um desses avanços foi o advento da Internet, que moldou os contornos atuais do ciberespaço. Embora o ciberespaço seja frequentemente confundido exclusivamente com a internet, tecnologias precursoras, como o telégrafo e os sistemas de rádio, já constituíam elementos fundamentais desse domínio. No entanto, foi somente com a expansão da internet, a operacionalização do espectro eletromagnético e a difusão dos computadores na segunda metade do século XX que o ciberespaço passou a ocupar uma posição central na sociedade contemporânea (Medeiros, 2024)

Pode-se definir o ciberespaço como um domínio global caracterizado pelo uso do espectro eletromagnético para armazenar, criar, modificar e explorar informações por intermédio das Tecnologias de Informação e Comunicações (TICs) (Kuehl, 2009). Embora o prefixo 'ciber' possa sugerir um ambiente estritamente virtual, autores como Ventre (2012), Libicki (2009) e Rattray (2009), destacam que o ciberespaço possui uma dualidade, estando enraizado tanto na materialidade física quanto na virtualidade. Esta materialidade, ou a 'geografia real' do ciberespaço (Cavelty, 2010), é evidenciada por infraestruturas físicas, tais como cabos de fibra óptica, satélites e torres de transmissão que sustentam a existência desse domínio.

A dualidade material-imaterial do ciberespaço é frequentemente melhor compreendida através de uma abordagem estratificada. Esta abordagem, que será detalhada no primeiro capítulo, é sustentada por autores como Libicki (2009), Ventre (2012) e Sheldon (2011). Embora eles variem quanto ao número de camadas que compõem o espaço cibernético, geralmente reconhecem três estruturas essenciais e interdependentes: (I) a infraestrutura física que sustenta o domínio; (II) os softwares e códigos que facilitam a operacionalização do ciberespaço; e (III) o usuário, a camada cognitiva que interage dentro deste espaço.

A problemática central desta pesquisa foca na primeira camada, isto é, nas infraestruturas do ciberespaço. Com a transição do final do século XX para o início do XXI, a sociedade ingressou em uma nova era dominada pela informação. Embora essa revolução digital tenha oferecido inúmeras vantagens, como o acesso imediato

a vastas quantidades de informação, a suposta eliminação de barreiras geográficas e a abertura de novas fronteiras comerciais, ela também introduziu uma série de vulnerabilidades complexas. Uma das principais vulnerabilidades decorre da expansão das Tecnologias de Informação e Comunicação (TICs), que gerou uma interdependência crescente entre o ciberespaço e as Infraestruturas Críticas.

A natureza imaterial do ciberespaço, manifestada pela operacionalização do espectro eletromagnético, permite que ataques cibernéticos penetrem fronteiras nacionais com facilidade, e expõe as infraestruturas críticas a riscos antes limitados a ataques cinéticos (Medeiros; Goldoni, 2020). Ao passo que o ciberespaço desafia as noções tradicionais de território e fronteiras, surge, consequentemente, um reconhecimento crescente e uma urgência por parte dos Estados em assegurar a soberania nacional neste domínio. Essa percepção de urgência em relação às ameaças cibernéticas deriva, principalmente, de dois fatores: (I) a consciência de uma crescente exposição a vulnerabilidades cibernéticas e (II) o reconhecimento de que uma ampla gama de atores — tanto estatais quanto não estatais — está pronto para explorar tais vulnerabilidades (Cavelty, 2012).

Nos Estados Unidos, por exemplo, a partir do final da década de 1980 e início da década de 1990, surgiram documentos, muitos oriundos do Departamento de Defesa (DoD), que estabelecem uma conexão direta entre ameaças cibernéticas, cibersegurança e infraestruturas críticas. Esta consciência de vulnerabilidade tem raízes no período pós-Guerra Fria, quando se tornou evidente que diversos atores poderiam causar danos significativos à segurança nacional dos Estados Unidos. As TICs, que antes desempenharam um papel crucial na Revolução dos Assuntos Militares[1], passaram a ser vistas não apenas como uma vantagem estratégica dos Estados Unidos, mas também como uma vulnerabilidade (Cavelty, 2010).

Ao passo que a vulnerabilidade descrita acima se torna cada vez mais palpável, a saída encontrada pelos Estados é a busca paulatina da construção de fronteiras virtuais em um domínio inicialmente concebido como ‘livre’. Esta tendência para a

[1] A Revolução dos Assuntos Militares (RMA, do inglês Revolution in Military Affairs) é caracterizada pelo processo de aprimoramento e modernização de estratégias, operações e tecnologias militares através dos avanços tecnológicos (Black, 2009).

regulamentação e a territorialização do ciberespaço é observada por Demchak e Dombrowski (2011 p. 35 , tradução nossa[2]):

> Embora não seja reconhecido como tal nem publicamente endossado pela maioria dos líderes democráticos, um processo de regulação do ciberespaço está acontecendo, construindo os blocos iniciais de cercas virtuais nacionais emergentes. Uma nova "era vestefaliana cibernética" está lentamente emergindo à medida que os líderes de Estado se organizam para proteger seus cidadãos e suas economias individualmente e, inconscientemente, iniciam o caminho para as fronteiras no ciberespaço.

A partir do contexto delineado, a pergunta que orienta esta dissertação é: Como as políticas de cibersegurança para infraestruturas críticas dos Estados Unidos refletem uma tensão entre as abordagens territorializantes e liberais do ciberespaço? Como hipótese, postula-se que, nas políticas de cibersegurança dos Estados Unidos, existe uma distinção fundamental entre a 'camada superior' do ciberespaço, na qual prevalece uma abordagem liberal que enfatiza a livre circulação de informações, e a 'camada inferior', que adota uma postura mais protecionista focada na segurança das infraestruturas críticas. Tal diferenciação reforça a necessidade de que o ciberespaço seja compreendido por intermédio de uma abordagem estratificada

O objetivo geral do trabalho é analisar as estratégias de cibersegurança para infraestruturas críticas dos Estados Unidos no século XXI, com o intuito de identificar e compreender como essas estratégias refletem uma tensão entre as abordagens territorializantes e liberais do ciberespaço. Para atingir este fim, os seguintes objetivos específicos foram delineados: (I) Realizar um debate sobre as dinâmicas de territorialidade e desterritorialidade que ocorrem no e pelo espaço cibernético; (II) Mapear a estrutura organizacional cibernética estadunidense e seus principais atores; e (III) Investigar as abordagens adotadas pelos governos dos EUA no século XXI em relação à Cibersegurança para proteção de infraestruturas críticas.

A escolha de utilização dos Estados Unidos como estudo de caso se justifica ao analisar a minuta que antecede a Política Nacional de Cibersegurança brasileira (PNCiber). Na minuta, observa-se referências explícitas às estratégias de cibersegurança de países com reconhecida expertise na área, particularmente os Estados Unidos e o Reino Unido. Tal menção sugere que os formuladores das

---

[2] No original: *"While it is not recognized as such nor publicly endorsed by most democratic leaders, a cyberspace regulating process is happening, building the initial blocks of emergent national virtual fences. A new "cybered Westphalian age" is slowly emerging as state leaders organize to protect their citizens and economies individually and unwittingly initiate the path to borders in cyberspace."*

políticas de cibersegurança brasileira buscam inspiração no campo internacional. Nesse contexto, torna-se crucial analisar as políticas de segurança cibernética adotadas pelos Estados Unidos, dada a sua relevância para a Defesa Nacional brasileira.

Institucionalmente, a preocupação com o ciberespaço e a segurança cibernética começou a ganhar destaque no Brasil com suas primeiras menções na Política Nacional de Defesa (PND) em 2005, seguida pela Estratégia Nacional de Defesa (END) em 2008. A partir de então, há um esforço contínuo na estruturação institucional na área, observado na criação do Centro de Defesa Cibernética (CDCiber) em 2012 e do Comando de Defesa Cibernética (ComDCiber) em 2016 (Devanny; Goldoni; Medeiros, 2022). A recente instituição da Política Nacional de Cibersegurança, que instituiu um Comitê Nacional de Cibersegurança, juntamente com discussões sobre a criação de uma Agência Nacional de Cibersegurança (ANCiber), reforça a percepção de que a segurança cibernética é uma área de interesse crítico para a sociedade brasileira.

Isto posto, a análise das políticas de cibersegurança dos EUA pode contribuir significativamente para o aperfeiçoamento da Política Nacional de Cibersegurança do Brasil. Um dos princípios da PNCiber a "a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade" (Brasil, 2023, s/p). Logo, ao analisar as abordagens adotadas pelos diferentes governos dos Estados Unidos no que diz respeito à cibersegurança para infraestruturas críticas, esta dissertação pode proporcionar percepções relevantes para o Brasil.

Análise de Conteúdo: Breves considerações

Ademais, para os fins desta pesquisa, será utilizada a Análise de Conteúdo (A.C.) como metodologia. A análise de conteúdo consiste em uma técnica de pesquisa científica que se baseia em procedimentos sistemáticos, validados intersubjetivamente e de caráter público, com o objetivo de gerar inferências válidas a partir de diferentes conteúdos — sejam eles verbais, visuais ou escritos. Essa abordagem busca descrever, quantificar ou interpretar fenômenos em função de seus significados, intenções, consequências ou contextos. Como destacam Sampaio e Lycarião (2021), trata-se de um método que combina rigor científico com flexibilidade

interpretativa. Nesse sentido, Bardin (2011, p. 43) observa que: "A técnica consiste em classificar diferentes elementos nas diversas ‘gavetas’ segundo critérios susceptíveis de fazer surgir um sentido dentro de uma ‘confusão’ inicial."

Embora a prática de catalogar e classificar textos remonte a tempos antigos, a análise de conteúdo ganhou maior relevância científica no contexto das Grandes Guerras Mundiais, no século XX. Foi nesse período que essa técnica começou a ser empregada de forma mais sistemática, especialmente para mensurar padrões em mensagens midiáticas e propagandas de guerra. Lasswell (1927), pioneiro nesse campo, explorou seu uso para avaliar as estratégias comunicacionais de governos em conflito, com especial atenção às táticas persuasivas empregadas pelos regimes.

Durante a Segunda Guerra Mundial, tanto o rádio quanto o cinema foram amplamente utilizados pelos Estados Unidos e pela Alemanha nazista como instrumentos de propaganda. Esse cenário despertou o interesse dos norte-americanos em analisar como os regimes considerados “inimigos” empregavam suas mensagens para conquistar apoio popular e mobilizar suas populações. Krippendorff (2004) destaca que analistas do *Foreign Broadcast Intelligence Service*, ligado ao *Federal Communications Commission* (FCC), usaram análises de transmissões radiofônicas para identificar padrões que pudessem antecipar as táticas dos países do Eixo. Por meio dessas mensagens, foi possível inferir os esforços dos governos adversários para manter o apoio popular às ações militares em seus territórios.

Nesse contexto, a consolidação da análise de conteúdo como técnica reflete uma onda mais ampla de busca por rigor científico, que se intensificou no período pós-guerra. Essa busca tem raízes no movimento positivista dos anos 1920 nos Estados Unidos, que propôs uma redefinição do paradigma da ciência política, pautada na aplicação das mesmas bases metodológicas das ciências naturais (Othon, 2021). Esse movimento deu início à chamada revolução behaviorista nas ciências sociais, que enfatizou a observação sistemática e a mensuração de fenômenos observáveis, promovendo a construção de conhecimento científico objetivo.

As Relações Internacionais (R.I.), enquanto disciplina, também foram influenciadas por essa onda de busca por rigor científico. O impacto do behaviorismo nas R.I. é evidente no chamado Segundo Grande Debate, no qual os behavioristas, conhecidos como cientificistas, confrontaram as correntes tradicionalistas, como o liberalismo e o realismo, criticando-as pela ausência de integração com outras áreas do conhecimento científico. Os tradicionalistas priorizavam a história, o direito, a

filosofia e outros métodos qualitativos de investigação, enquanto os behavioristas defendiam a exclusão de questões normativas e o tratamento da ciência como algo neutro e técnico (Albuquerque, 2021). Assim, focavam na análise quantitativa de dados para gerar conclusões generalizáveis sobre fenômenos sociais (Viotti; Kauppi, 2012).

No que diz respeito à A.C., alguns autores, como Neuendorf (2002), defendem que se trata de uma técnica estritamente quantitativa. Sob essa ótica, apenas métodos que geram resultados quantitativos podem ser considerados A.C. Contudo, a presente pesquisa, apoiada em autores como Bardin (2011), Sampaio e Lycarião (2021), Schreier (2012) e Krippendorff (2004), reconhece a existência de uma vertente qualitativa na A.C., a qual será adotada nesta dissertação. Nesse contexto, a pesquisa rejeita o pressuposto behaviorista da neutralidade da ciência, pois considera que a análise de um objeto ou fenômeno está sujeita às interpretações prévias do pesquisador, as quais moldam suas percepções e influenciam o processo analítico.

É importante ressaltar que reconhecer a impossibilidade da neutralidade da ciência não equivale a negar a possibilidade de objetividade. Embora o sujeito traga experiências prévias, resultantes de suas leituras, vivências e do ambiente em que está inserido, isso não invalida o uso de metodologias rigorosas e sistemáticas que assegurem a objetividade na análise e interpretação de dados. Nesse sentido, Bardin (2011, p. 14) afirma que “a atitude interpretativa continua em parte a existir na análise de conteúdo, mas é sustentada por processos técnicos de validação”. Assim, mesmo que seja impossível eliminar completamente as subjetividades inerentes ao pesquisador, os métodos empregados garantem consistência, validade e replicabilidade à pesquisa.

Sobre sua execução, Bardin (2011) sublinha a importância de três fases cruciais no processo da A.C.: (I) a pré-análise, que consiste na organização do material e na seleção dos documentos a serem examinados; (II) a exploração do material, que envolve a classificação e a codificação do conteúdo; e (III) o tratamento e interpretação dos dados, etapas nas quais as informações são analisadas para extrair significados relevantes à pesquisa.

Para garantir que diferentes pesquisadores obtenham resultados similares, Sampaio e Lycarião (2021, p. 39) apresentam dois princípios fundamentais para a condução da AC: (I) a disponibilização dos critérios e regras utilizados na análise e (II) a acessibilidade ao material analisado. O primeiro ponto é frequentemente

denominado “livro de códigos”, um documento que reúne instruções detalhadas sobre cada variável e categoria, possibilitando que outros pesquisadores compreendam como a codificação deve ser realizada. Esse documento também apresenta exemplos de unidades codificadas, o que assegura maior consistência e replicabilidade ao processo. Nesse sentido, o livro de códigos é essencial para que a A.C. seja um processo intersubjetivamente validado, ao permitir que pesquisadores distintos obtenham resultados semelhantes ao trabalhar com uma mesma base de dados.

Com base nesses princípios, a presente pesquisa adota um semi-livro de códigos apresentada nessa introdução, com o objetivo de garantir a validação intersubjetiva dos resultados. A análise foi realizada a partir dos documentos listados no Quadro 1, que constituem a base de dados utilizada neste estudo. Essa seleção se inspira na tese de Medeiros (2024), que incorporou esses mesmos documentos ao analisar os marcos estratégicos do uso do poder cibernético pelos Estados Unidos. Dessa forma, esta pesquisa estabelece um diálogo metodológico com estudos prévios, ao utilizar um conjunto documental já consolidado como relevante no campo.

QUADRO 1 - BASE DOCUMENTAL DE ESTRATÉGIAS DE SEGURANÇA E DEFESA DOS EUA

Governo	Título	Data de Publicação	Publisher	Cyber-Specific?
Bush	The National Security Strategy of the United States of America	Set/02	White House	☒
	The National Strategy to Secure Cyberspace	Fev/03	White House	☑
	The National Defense Strategy of The United States of America	Mar/05	Deparment of Defense	☒
	The National Security Strategy of the United States of America	Março de 2006	White House	☒
	The National Military Strategy for Cyberspace Operations	Dez/06	Deparment of Defense	☑
	National Defense Strategy	Jun/08	Deparment of Defense	☒
Obama	Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure	Mai/09	White House	☑
	National Security Strategy	Mai/10	White House	☒
	International Strategy for Cyberspace - Prosperity, Security and Openness in a Networked World	Mai/11	White House	☑
	Department of Defense Strategy for Operating in Cyberspace	Jul/11	Deparment of Defense	☑
	National Security Strategy	Fev/15	White house	☒
	The Department of Defense Cyber Strategy	Abr/15	Department of Defense	☑
	Beyonde the Build: Delivering Outcomes through Cyberspace	Jun/15	Deparment of Defense (USCYBERCOM)	☑
Trump	National Security Strategy	Dez/17	White house	☒

	National Defense Strategy	Jan/18	Department of Defense	☒
	Achieve and Maintain Cyberspace Superiority	Abr/18	Department of Defense (USCYBERCOM)	☑
	U.S. Department of Homeland Security Cybersecurity Strategy	Mai/18	Department of Homeland Security	☑
	Summary Department of Defense Cyber Strategy	Set/18	Department of Defense	☑
Biden	National Defense Strategy	Out/22	Department of Defense	☒
	National Security Strategy	Out/22	White House	☒
	National Cybersecurity Strategy	Mar/23	White House	☑
	Cyber Strategy of The Department of Defense	Set/23	Department of Defense	☑

Fonte: Elaboração própria baseada em Medeiros (2024)

Optou-se por adotar o parágrafo como unidade de análise, pois unidades mais amplas, como páginas ou documentos inteiros, não atenderiam ao propósito do estudo. Sobre as categorias, estas foram definidas de forma mista, combinando abordagens dedutivas e indutivas. As categorias de enquadramento camadas e abordagens, apresentadas no Quadro 1, foram inicialmente estabelecidas de maneira dedutiva, com base na literatura a ser discutida no primeiro capítulo. No entanto, a categoria "Capacidade Hostil" foi incluída posteriormente, como resultado de uma codificação teste.

QUADRO 2 - CATEGORIAS E DEFINIÇÕES PARA ANÁLISE DE CONTEÚDO

Seção	Categoria	Descrição
Enquadramento	Requer proteção	Refere-se a passagens que indicam a necessidade da proteção constante do ciberespaço para preservar sua estabilidade e funcionalidade.
	Asset	Refere-se a passagens que tratam o ciberespaço como um recurso estratégico fundamental, utilizado para alcançar diversas finalidades, sejam econômicas, políticas ou de segurança.
	Vulnerabilidade	Passagens que destacam fragilidades associadas à interdependência criada pela conectividade global do ciberespaço, que tornam sistemas nacionais suscetíveis à exploração por agentes maliciosos.
	Capacidade Hostil	Passagens que retratam o ciberespaço como um meio para a realização de ações hostis que podem comprometer a segurança e a estabilidade do território nacional (seja espionagem, desinformação etc.)
	Irrelevante	Não se aplica

Camadas Mencionadas/Enfatizadas	Física	Refere-se à infraestrutura tangível, como cabos, data centers e equipamentos de rede.
	Sintática	Envolve redes, sistemas e protocolos usados para processar e transmitir informações.
	Semântica	Foco nos dados, informações e seu significado.
Abordagem	Liberal	Enfatiza aspectos colaborativos e democráticos do ciberespaço, como a livre circulação de dados, a cooperação internacional, as parcerias público-privadas etc.
	Territorializante	Ciberespaço tratado como domínio estratégico vinculado à soberania estatal e a segurança nacional.

Fonte: Elaboração própria

Ademais, para orientar a análise dos documentos apresentados no Quadro 2, foi desenvolvido um fluxograma para a aplicação sistemática da Análise de Conteúdo, conforme ilustrado no Quadro 3. O fluxograma apresenta as etapas necessárias para a categorização e codificação dos parágrafos, o que assegura a consistência e a replicabilidade nos resultados.

QUADRO 3 - FLUXOGRAMA PARA A ANÁLISE DE CONTEÚDO

Etapa	Pergunta	Ação
1.Enquadramento	Como esse parágrafo enquadra o ciberespaço? (a) Como algo a ser protegido; (b) como um asset; (c) como uma vulnerabilidade; (d) como uma Ameaça ou ferramenta disruptiva	**Sim:** Se somente para (a) somente para (b); somente para (c). somente para (d) ou para (a; b); (a; c); (a; d); (b; c); (b; d); (c; d); e variações, siga para **etapa 2**. **Não:** Irrelevante, não codifique
2.Camada	Este parágrafo menciona alguma camada do ciberespaço?	**Sim:** Continue para **Etapa 3.** **Não:** Enxerga o ciberespaço como um todo, pule para a **Etapa 5**
3.Identificação de camadas	Quantas e quais camadas ele menciona?	**Apenas uma:** Registre e vá para a **Etapa 5** **Mais de uma:** Vá para a **Etapa 4**
4.Ênfase	Qual camada tem maior incidência nesse parágrafo?	**Identifique** a camada predominante no parágrafo
5.Abordagem	Qual abordagem é utilizada para a camada presente/enfatizada?	**Classifique** com base na abordagem identificada (**Territorializante ou Liberal**)

Fonte: Elaboração própria

Para auxiliar na execução da A.C., o software MAXQDA foi utilizado para facilitar o processo de categorização, organização e visualização dos dados. Em termos quantitativos, o uso do software resultou em 8.131 categorizações ao longo dos 22 documentos. No entanto, apesar da utilidade do software, do fluxograma e das

categorias para sistematizar a análise dos documentos, é necessário reconhecer as limitações dessa metodologia. A categorização, ao simplificar os dados, não captura nuances contextuais importantes presentes nos documentos analisados. Para superar essa limitação, a análise de conteúdo foi complementada com uma análise conjuntural dos governos examinados, considerando os contextos político, econômico e histórico que influenciaram a criação dos documentos. Essa complementação permite uma investigação mais profunda e contextualizada.

Isto posto, a dissertação foi organizada em três capítulos, além dessa introdução e das considerações finais. No primeiro capítulo, foram discutidos conceitos fundamentais para a compreensão do estudo, como ciberespaço, suas diferentes camadas, sua relação com as Infraestruturas Críticas bem como o debate acerca da territorialização e desterritorialização no ciberespaço e através dele. O segundo capítulo abordou a estrutura organizacional cibernética dos Estados Unidos, analisando suas principais agências e como as contradições inerentes ao ciberespaço dificultam as delimitações precisas entre as atribuições de segurança e defesa nesse domínio. Já o terceiro capítulo foca nas estratégias de cibersegurança de cada governo analisado. Nesse contexto, foi realizada uma análise de conteúdo de cada documento, com o objetivo de verificar a confirmação da hipótese inicial. Por fim, as considerações finais sintetizaram os principais pontos abordados ao longo da pesquisa.

1. É possível territorializar o ciberespaço? Conceitos e definições sobre ciberespaço, infraestruturas críticas e territorialização.

Este capítulo visa desenvolver uma discussão crítica sobre as dinâmicas de territorialidade e desterritorialidade que ocorrem no ciberespaço. Para que essa discussão seja realizada com profundidade, é essencial definir o que se entende por Ciberespaço, reconhecer suas características singulares e as múltiplas camadas que o compõem. Dada a natureza constantemente evolutiva do ciberespaço, as definições podem rapidamente se tornar obsoletas ou encontrar divergências devido à falta de consenso acadêmico.

O termo “ciberespaço” tem suas raízes em 1982, inicialmente cunhado por William Gibson no conto *“Burning Chrome”*. Gibson usou esse termo para descrever uma realidade virtual criada por meio do uso de computadores. Esse conceito capturou o imaginário popular e foi mais explorado em obras cinematográficas. Notavelmente, filmes como “Tron, uma Odisséia Eletrônica” e “Matrix” não apenas fizeram referências diretas a essa noção, mas também se inspiraram significativamente na ideia da realidade virtual estar entrelaçada com a vida cotidiana (Kellner, 2001; Deibert, 2018; Singer; Friedman, 2014).

Conforme Singer e Friedman (2014) pontuam, a natureza mutável do ciberespaço torna difícil o reconhecimento de suas origens. Frequentemente confundido com a Internet no senso comum, o ciberespaço não se reduz somente a isto. Historicamente, sistemas como a telegrafia e o rádio amador já participavam do ciberespaço e contribuíram para sua complexidade, de modo a desafiar a noção simplista de que o ciberespaço é sinônimo de internet (Cepik; Canabarro; Borne, 2014).

A origem da internet pode ser atribuída à *Defense Advanced Research Projects Agency* (DARPA). A DARPA, agência vinculada ao Departamento de Defesa norte-americano (DOD), emergiu como reação estratégica ao lançamento do satélite soviétio *Sputnik,* e tinha como missão alocar investimentos em inovações tecnológicas que pudessem contribuir para a segurança nacional estadunidense. É neste contexto de competição geopolítica entre Estados Unidos e União Soviética (URSS) que o projeto ARPANET, precursor da internet, é criado. Com a necessidade de uma rede de comunicação que pudesse resistir a um eventual ataque nuclear soviético, o projeto ARPANET deu origem a uma rede de compartilhamento de recursos no âmbito digital

entre computadores não localizados no mesmo espaço geográfico (Castells, 2003; Pecequilo; Junior, 2022).

Os investimentos públicos contínuos da DARPA em microeletrônica permitiram o surgimento de computadores menores, mais acessíveis e com capacidade de processamento superior. O desenvolvimento dessas tecnologias ensejaram uma ruptura no modo de produção capitalista que ficou conhecida como a Revolução Técnico Científica (ou Terceira Revolução Industrial). A expansão das Tecnologias de Informação e Comunicação (TICs) e da internet desempenharam um papel fundamental ao inserir a sociedade no ciberespaço, através da difusão massiva de informações e da virtualização do mundo (Medeiros, 2024). Portanto, ressalta-se a importância de perceber a internet como um avanço significativo no ciberespaço, e não como seu sinônimo.

Sobre o espaço cibernético, Singer e Friedman (2014, p. 25, tradução nossa[3]) oferecem uma definição concisa dele, e o descrevem como "o domínio de redes de computadores (e os usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line". Embora esta definição capte a essência da interatividade e conectividade do ciberespaço, Kuehl (2009) aborda a questão sob uma ótica mais técnica. Ele define o ciberespaço como um domínio global que se manifesta pelo uso de tecnologias eletrônicas e pela exploração do espectro eletromagnético, o que inclui a criação, armazenamento, troca e modificação de informações através de redes interconectadas. A contribuição de Kuehl é fundamental, pois ressalta um componente essencial que Singer e Friedman (2014) não enfatizam: a importância do espectro eletromagnético no funcionamento e na infraestrutura do ciberespaço.

Em uma análise adicional, Kuehl (2009) reflete sobre a importância tecnológica na constituição e operacionalização do ciberespaço. Em contraste com domínios tradicionais — terrestre, marítimo e aéreo —, que existem independentemente da ação humana, o ciberespaço diferencia-se por ter sido construído pelo homem. Essa distinção é reconhecida por diversos autores, que argumentam que o acesso, uso e exploração do ciberespaço dependem exclusivamente de tecnologias desenvolvidas pelo ser humano. No entanto, Kuehl (2009) desafia este ponto de vista ao alegar que

---

[3] No original: *“The realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online.”*

tal interpretação não captura totalmente a realidade. Segundo sua análise, as tecnologias que nos permitem operacionalizar o ciberespaço são análogas a veículos, aviões e satélites usados para explorar os demais domínios. A diferença fundamental, portanto, não reside na necessidade de tecnologia *per se*, e sim na maior visibilidade e tangibilidade dos domínios tradicionais em oposição ao ciberespaço.

1.1 A materialidade do ciberespaço e suas camadas

A compreensão do ciberespaço é frequentemente dificultada por uma percepção compartilhada de que este se trata de um domínio exclusivamente virtual, intangível e imaterial. Contudo, a análise de Rattray (2009, p. 254, tradução nossa[4]), ressalta a materialidade desse domínio, que encontra suas raízes no mundo físico, visto que "é criado pela conexão de sistemas físicos e redes, gerenciados por regras definidas em software e protocolos de comunicação." Ao contrário dos domínios tradicionais, o ciberespaço oscila entre a realidade física e a virtual. Essa dualidade decorre pelo fato de o espectro eletromagnético estar ancorado no tangível por meio de infraestruturas físicas como redes de fibra óptica, estações de rádio e *data centers*. Portanto, a natureza do ciberespaço se caracteriza por uma imaterialidade apenas parcial. Ele manifesta-se principalmente através do espectro eletromagnético, que, apesar de imaterial, origina-se e é mantido por infraestruturas sólidas. Estas, por sua vez, são operadas por seres humanos situados nos limites dos domínios convencionais.

Libicki (2009), ao analisar o espaço cibernético, propõe uma estruturação em camadas que facilita a compreensão da interação entre o material e o imaterial. Segundo o autor, compreender o ciberespaço envolve a identificação de três camadas que o constituem: (I) a camada física; (II) a camada sintática; e (III) a camada semântica. A camada física consiste nos cabos e fios que sustentam o sistema de informação. A camada sintática corresponde às instruções que designers e usuários fornecem às máquinas e aos protocolos usados por estas para se comunicarem entre si. Por fim, a camada semântica relaciona-se às informações contidas na máquina,

[4]No original: *"it is created by the connection of physical systems and networks, managed by rules set in software and communications protocols."*

seja de caráter sintático, ou seja, apenas para a manipulação e controle do sistema, ou para informações passíveis de serem interpretadas pelo usuário.

Sheldon (2011), ao revisar a estrutura conceitual do ciberespaço, introduz a proposta de quatro camadas — infraestrutura, física, sintática e semântica — em contraste com as três tradicionalmente reconhecidas. Esta abordagem fornece uma distinção mais clara entre os elementos tangíveis e intangíveis do ciberespaço. A infraestrutura abarca os componentes físicos essenciais do ciberespaço, enquanto a camada física diz respeito aos aspectos do Espectro Eletromagnético que permitem o funcionamento da infraestrutura. Dessa forma, a infraestrutura define "o que" constitui o ciberespaço, e a camada física explica "como" ele opera.

Libicki (2009) e Sheldon (2011) convergem ao estabelecer, de maneira similar, distinções claras em relação às camadas do ciberespaço. Em sua obra "*Cyber Deterrence and Cyberwar"*, Libicki introduz o conceito de conquista e postula que

> [...] a conquista funciona de forma diferente em camadas diferentes. O acesso físico (ou seja, a conectividade) não significa acesso sintático. O acesso sintático não significa um acesso semântico significativo. E o acesso semântico não resulta necessariamente em mudanças significativas no que as pessoas acreditam sobre o mundo ou mesmo sobre o ciberespaço. (Libicki, 2009, p. 9, tradução nossa[5]).

Para ilustrar a citação de Libicki (2009), consideramos o cenário em que uma mensagem criptografada é interceptada. Embora a interceptação represente uma conquista na camada sintática, ou seja, o acesso aos dados criptografados foi obtido, isso não garante o entendimento do conteúdo sem a chave de descriptografia. Portanto, não se alcança uma conquista na camada semântica, pois sem a chave, a mensagem permanece ilegível e seu significado, incompreendido.

Em confluência com as ideias de Libicki (2009), Sheldon (2011, p. 98, tradução nossa[6]) argumenta que "[...] o controle sobre uma camada não significa controle sobre as outras". Essa distinção, enfatizada por ambos os autores, é crucial para a hipótese deste trabalho. A análise dos documentos oficiais estadunidenses, apresentada em capítulos subsequentes, busca evidenciar que a postura americana varia significativamente entre as camadas física e superior do ciberespaço. Assim, torna-se

---

[5] No original: "*So, conquest works differently at different layers. Physical access (that is, connectivity) does not mean syntactic access. Syntactic access does not mean meaningful semantic access. And semantic access does not necessarily result in meaningful change in what people believe about the world or even about cyberspace."*

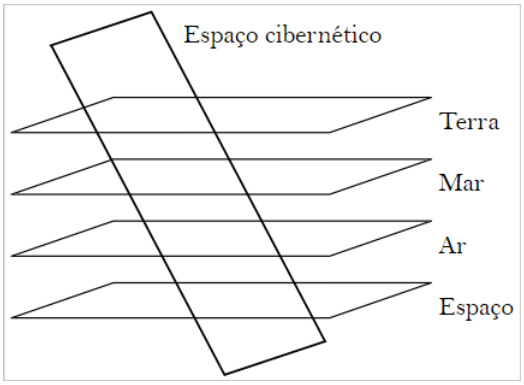
[6] No original: *"[…] control of one layer does not mean control of the others."*

imperativo adotar uma abordagem segmentada para estudar o ciberespaço, a fim de elucidar as nuances das estratégias de cibersegurança dos Estados Unidos.

Semelhante a Libicki (2009), Ventre (2012) desenvolve um modelo tridimensional para a análise do ciberespaço. De acordo com o autor, o ciberespaço compreende as camadas física, de software e cognitiva, o que ressoa as camadas físicas e sintáticas propostas por Libicki. Contudo, o diferencial da abordagem de Ventre (2012) emerge na camada cognitiva, que, ao incorporar interações humanas, destaca a dimensão social do ciberespaço. É por meio da participação e utilização do ciberespaço pela sociedade que este se configura como uma arena de interação e, consequentemente, como um campo de relações de poder.

Sobre o ciberespaço, Ventre (2012) ressalta que uma das suas características fundamentais é a transversalidade em relação aos demais domínios tradicionais. Conforme ilustrado na figura abaixo, essa transversalidade manifesta-se no momento em que se identificam, em todas as outras dimensões, conexões e interações com o ciberespaço, seja por meio da presença de infraestruturas, sistemas, dados, tráfego de IP, etc. Portanto, torna-se claro que, à medida que o ciberespaço se entrelaça com todos os outros domínios tradicionais, ele se estabelece como uma plataforma indispensável para uma vasta gama de atividades sociais, políticas, militares e econômicas, conforme apontado por Kuehl (2009).

FIGURA 1 - A TRANSVERSALIDADE DO CIBERESPAÇO



Fonte: Ventre (2012)

Ao examinar as múltiplas perspectivas sobre o ciberespaço apresentadas anteriormente, é evidente a existência tanto de pontos de consenso como de divergência, de modo a refletir a complexa e contínua evolução do ciberespaço. Um ponto de consenso entre os pesquisadores diz respeito à caracterização do

ciberespaço como um ambiente composto por camadas interdependentes. Mesmo aqueles que não adotam explicitamente uma visão estratificada ao conceituar o ciberespaço, de maneira implícita, reconhecem sua estrutura em camadas ao incluir elementos constitutivos em suas definições. Além disso, o aspecto da informação surge como um denominador comum, o que reforça a concepção de que o ciberespaço é, antes de tudo, um ambiente informacional. As divergências aparecem, particularmente, em relação ao número de camadas que compõem o ciberespaço, com variações que oscilam entre três e quatro, a depender do autor. Contudo, mesmo diante dessas diferenças, observa-se uma interação e complementaridade entre as camadas propostas por diferentes autores.

Dentro do contexto estadunidense, a definição de ciberespaço, conforme articulada em documentos de estratégia nacional, esclarece a percepção do país sobre esse domínio e destaca a importância estratégica atribuída a este. Nesse sentido, a definição presente no dicionário de Termos Militares e Associados do Departamento de Defesa (DoD) dos Estados Unidos será analisada. A escolha pela definição elaborada pelo DoD não se limita ao seu papel na elaboração das estratégias de segurança nacional e considera, também, sua contribuição ao desenvolvimento tecnológico do ciberespaço, conforme evidenciado pela DARPA e o projeto ARPANET anteriormente mencionado. Além disso, será examinada a definição elaborada pela Organização do Tratado do Atlântico Norte (OTAN), cuja análise é pertinente dado que os Estados Unidos são parte influente desta organização.

QUADRO 4 - DEFINIÇÕES E PERSPECTIVAS DO CIBERESPAÇO PARA ESTADOS UNIDOS E OTAN

Ator/ano	Definição e perspectivas do Ciberespaço
Estados Unidos (2005, p. 13, tradução nossa[7])	A nossa capacidade de operar no e a partir do espaço comum global - o espaço, as águas internacionais, o espaço aéreo e o ciberespaço - é importante. Permite-nos projetar poder em qualquer parte do mundo a partir de bases de operações seguras.
	Um domínio global dentro do ambiente de informação que consiste em redes

[7] No Original: *"Our ability to operate in and from the global commons- space, international waters, and airspace, and cyberspace-is important. It enables us to project power anywhere in the world from secure bases of operation."*

Estados Unidos (2021, p.55, tradução nossa[8]).	interdependentes de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores incorporados
OTAN (2017, p .564, tradução nossa[9])	O ambiente formado por componentes físicos e não físicos para armazenar, modificar e trocar dados usando redes de computadores

Fonte: elaboração própria com base em Estados Unidos (2005, 2017) e OTAN (2017)

A comparação da definição de ciberespaço na Estratégia Nacional de Defesa (NDS) de 2005 com aquela no Dicionário de Termos Militares de 2021 revela uma evolução conceitual significativa. Ao igualar o ciberespaço a outras *global commons*[10], tais como o espaço sideral, as águas internacionais e o espaço aéreo, a NDS acaba por refletir as concepções iniciais desse domínio: um espaço livre do controle estatal. Em contrapartida, a definição fornecida pelo Departamento de Defesa (DoD) em 2021, que ecoa a perspectiva de Kuehl (2009), descreve o ciberespaço como um 'domínio global'. Essa variação na definição indica uma mudança na visão dos Estados Unidos, que passa a reconhecer o ciberespaço como um domínio operacional.

Cabe ressaltar que tanto o DoD quanto a OTAN enfatizam os componentes tangíveis — como as infraestruturas tecnológicas — e os intangíveis, como os dados, em suas definições de ciberespaço. Esta abordagem está em confluência com as perspectivas delineadas por autores como Libicki (2009), Ventre (2012), e, notadamente, Sheldon (2011), que sublinham as infraestruturas físicas como os elementos constituintes da materialidade do ciberespaço. No entanto, uma lacuna observada em ambas as definições é a ausência do componente humano do ciberespaço.

Por fim, é importante citar a perspectiva observada por Rocha (2022) sobre a definição de ciberespaço proposta pela OTAN. Ao definir o espaço cibernético como "ambiente formado por componentes físicos e não físicos", a OTAN deixa uma margem considerável para interpretação. Intencionalmente ou não, essa abordagem

---

[8] No original: *"A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*

[9] No original: *"The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."*

[10] Entende-se por *global common* regiões terrestres e espaciais que não pertencem exclusivamente a nenhum estado-nação específico, sendo, portanto, acessíveis coletivamente de acordo com as normas internacionais (Tangredi, 2018).

pode facilitar as operações no ciberespaço pela organização, uma vez que a ambiguidade e amplitude da definição não delimitam claramente o que constitui o ciberespaço.

Com base nessas considerações, a presente pesquisa não teve o intuito de esgotar o debate sobre a definição do ciberespaço, pois sabe-se que sua característica mutável faz com que as definições tenham que ser constantemente readequadas para enquadrar as dinâmicas tecnológicas, econômicas, sociais e políticas que o remodelam. Entretanto, é pertinente destacar que, a partir do que foi exposto, esse trabalho compreende o ciberespaço como um domínio informacional, ancorado na realidade por meio de infraestruturas. Ele opera através das Tecnologias de Informação e Comunicação (TICs) e do espectro eletromagnético que possibilitam o armazenamento, troca, modificação e negação de informação em redes interconectadas. Esta compreensão serve como ponto de partida para a próxima seção, que se dedica a explorar a interação entre o ciberespaço e as Infraestruturas Críticas. Para tal, será utilizado como base a Trindade Conceitual Fundamental do Ciberespaço (T.C.F) como ferramenta analítica, desenvolvida por Medeiros (2019).

1.2. As Infraestruturas Críticas e o Ciberespaço

A segurança das infraestruturas é uma preocupação central de governos ao longo da história, portanto, é imperativo explorar o conceito de Infraestruturas Críticas. O adjetivo ‘crítico’ que acompanha o termo destaca a importância e a essencialidade de determinadas estruturas e sistemas para a sociedade. Ten, Manimaran e Liu (2010, p. 853, tradução nossa[11]) as definem como “sistemas físicos e cibernéticos complexos que sustentam a vida moderna, cuja operação segura é crucial para a segurança nacional e a vitalidade econômica”.

Tendo os Estados Unidos como base para uma breve comparação histórica, o governo de Bill Clinton (1993-2001) inaugurou na década de 1990 a inserção das Infraestruturas Críticas na agenda de segurança nacional (O'Rourke, 2007). *A Presidential Decision Directive 63* (PDD-63), que trata da proteção de Infraestruturas Críticas, delimita — sem limitar — essas infraestruturas como sistemas físicos e

[11] No original: *“complex physical and cyberbased systems that form the lifeline of a modern society, and their reliable and secure operation is of paramount importance to national security and economic vitality.”*

cibernéticos pertencentes aos setores de telecomunicações, energia, sistema financeiro, transporte, água e demais serviços emergenciais (Estados Unidos, 1998).

Logo após o atentado de 11 de setembro, os Estados Unidos assinaram o USA PATRIOT Act (Estados Unidos, 2001), um decreto que, entre outras nuances, fornece à Infraestrutura Crítica uma definição legal. Com base nesse decreto, reconhece-se a essencialidade dos sistemas e ativos, físicos e virtuais, destacando as consequências que sua destruição ou incapacitação pode ter para a segurança, economia e bem-estar nacional. Essa abordagem é reforçada e expandida pela Cybersecurity and Infrastructure Security Agency (CISA), que identifica e protege 16 setores-chave de infraestrutura. Esses setores, que incluem desde o químico e de comunicações até a base industrial de defesa, fazem parte de um ecossistema nacional que, se comprometido, representa riscos significativos à segurança nacional.

Outro exemplo diz respeito ao Reino Unido, que reconhece 13 setores como parte das infraestruturas nacionais — três a menos que os Estados Unidos. Além disso, utiliza uma nomenclatura diferente para as Infraestruturas Criticas, denominada Critical National Infrastructure (CNI). Nesse contexto, *A National Protective Security Authority* (NPSA) do Reino Unido diferencia a infraestrutura nacional da Infraestrutura Crítica e considera como CNI apenas os componentes críticos da infraestrutura, como ativos, instalações, sistemas, redes ou processos, juntamente com os trabalhadores que operam essas infraestruturas. O argumento central da NPSA é que a perda ou comprometimento desses componentes pode ter um impacto significativo na disponibilidade e integridade de serviços essenciais, e sua interrupção pode levar à perda de vidas e a impactos econômicos relevantes (Reino Unido, 2023).

A partir da contextualização apresentada, é possível fazer algumas inferências sobre a conceituação das Infraestruturas Críticas. Primeiramente, Infraestrutura Crítica não é um conceito universal e uniforme. A breve comparação entre as conceituações feitas pelos Estados Unidos e pelo Reino Unido lança luz sobre um dilema fundamental: países conceituam suas Infraestruturas Críticas de maneira singular, levando em consideração fatores específicos. Esse fato, por si só, já elucida a dificuldade existente em cooperações internacionais no que diz respeito a boas práticas em relação as Infraestruturas Críticas.

Segundo, ao analisar as conceituações de ambos os países, percebe-se que são vagas e abrangentes, o que torna as Infraestruturas Críticas um conceito móvel. Comparativamente, no pós-11 de setembro, os Estados Unidos deram um salto

quantitativo na categorização de setores que fazem parte da Infraestrutura Crítica. Desse modo, a subjetividade na conceituação das Infraestruturas Críticas é intencional, pois garante que a definição e a legislação sejam relevantes e aplicáveis a longo prazo (Harašta, 2018). Não obstante, a dificuldade em definir Infraestrutura Crítica é acompanhada de uma oportunidade estratégica para que os atores securitizem e ampliem o escopo do conceito, atendendo a determinados objetivos estratégicos em nome da 'segurança nacional'. É necessário ressaltar que, embora a presente pesquisa parta do princípio de que Infraestrutura Crítica é um conceito móvel, isso não significa negar a existência de uma dimensão prática e pragmática do conceito, como evidenciam as convergências entre as definições americana e britânica.

Por certo, fica evidente o papel das infraestruturas críticas como fundamentais para a estrutura de qualquer sociedade. Como visto nos Estados Unidos, por exemplo, compreende-se que uma desestabilização dessas infraestruturas não apenas prejudicaria setores essenciais, mas também resultaria em perdas financeiras incalculáveis a depender da magnitude do ocorrido. Essa vulnerabilidade não é uma preocupação contemporânea, mas uma constante histórica, como ressalta William D. O'Neill (2010). O autor destaca que, já na Segunda Guerra Mundial, o comprometimento deliberado das infraestruturas críticas era considerado pelos estrategistas americanos como uma estratégia chave para o sucesso militar.

Como consequência dos avanços tecnológicos que impulsionaram a modernização das infraestruturas críticas, suas vulnerabilidades e importância estratégica tornaram-se mais evidentes. A Revolução Técnico-Científica estimulou uma integração significativa entre as infraestruturas críticas e o ciberespaço. Diante do cenário de crescente interdependência entre as Infraestruturas Críticas e o espaço cibernético, a Trindade Conceitual Fundamental do Ciberespaço (T.C.F), proposta por Medeiros (2019)[12], surge como ferramenta analítica que ajuda a compreensão desse contexto.

[12] A dissertação "Ciberespaço e relações internacionais: rumo a construção de um novo paradigma?" defendida por Breno Pauli Medeiros em 2019 deu origem ao artigo *"The Fundamental Conceptual Trinity of Cyberspace"* escrito em conjunto com Luiz Rogério F. Goldoni, publicado em 2020 na revista Contexto Internacional.

A T.C.F destaca três peculiaridades inerentes ao ciberespaço: a multiplicidade de atores, que desafia a ideia tradicional do Estado como detentor do monopólio da força; a incerteza, que dificulta a atribuição de ações a seus autores dentro deste domínio; e a desterritorialidade, que questiona as concepções tradicionais de território e fronteira, pois o espectro eletromagnético não respeita as noções zonais de território[13]. Dado ao escopo e objetivo do trabalho, a peculiaridade que receberá maior destaque é a desterritorialidade, embora a interdependência dessas três características seja fundamental para compreensão do ciberespaço e suas implicações para os preceitos basilares das Relações Internacionais e as dinâmicas no Sistema Internacional.

A questão da multiplicidade de atores em relação à Infraestrutura Crítica se torna evidente ao examinar o desenvolvimento da DARPA e da ARPANET. Como explicitado anteriormente, a ARPANET, antecessora da internet, foi inicialmente concebida para atender a uma necessidade estratégica dos Estados Unidos durante a Guerra Fria. Portanto, a ARPANET representava uma infraestrutura crítica dentro de um contexto militar, objetivada a assegurar comunicações resilientes em face de possíveis ameaças. No entanto, a evolução da ARPANET para a internet em sua forma atual transcendeu seu propósito original. Em 1975, a ARPANET transformou-se em uma rede adaptada para fins comerciais e, com os avanços no desenvolvimento do Protocolo TCP/IP[14], na década de 1990, a internet migrou definitivamente do uso exclusivamente militar para o civil (Ning, 2022).

Com essa transição, a infraestrutura da internet deixou de estar sob controle exclusivamente governamental. Empresas privadas passaram a assumir papéis fundamentais, como provedores de serviços, gerenciamento dos backbones de comunicação e produção de *hardware* e *software* que sustentam a rede global. Essa multiplicidade de atores trouxe uma gama de desafios na gestão e segurança das Infraestruturas Críticas, pois este cenário não se resume apenas as Infraestruturas que sustentam a Internet. Segundo a *National Strategy For Homeland Security* de 2002 (NSHS) (Estados Unidos, 2002), cerca de 85% das Infraestruturas Críticas dos

[13] A noção zonal de território diz respeito a um espaço claramente delimitado por fronteiras

[14] O protocolo TCP/IP é um conjunto de protocolos que possibilita a comunicação entre diferentes computadores.

Estados Unidos são gerenciadas pelo setor privado [15] . Esse dado evidencia a necessidade de parcerias público-privadas eficazes para assegurar o funcionamento e resiliência dessas infraestruturas.

Outro aspecto relevante da multiplicidade de atores é a simbiose cada vez mais presente entre as Infraestruturas Críticas e o ciberespaço. Essa interdependência se intensificou com o avanço das Tecnologias da Informação e Comunicação (TICs), que facilitaram a conexão das infraestruturas civis — incluindo sistemas de comunicação, financeiros, de abastecimento de água e energia — ao ciberespaço. Como resultado, essas infraestruturas dependem cada vez mais de sistemas conectados a redes para sua operacionalização e monitoramento. Um exemplo é o uso do *Supervisory Control and Data Acquisition* (SCADA), sistema que permite a supervisão e o controle automatizados dessas infraestruturas críticas a partir de centros de comando remotos.

Em síntese, a crescente dependência da sociedade em relação ao ciberespaço suscita desafios significativos à segurança nacional. Em contraste com outros domínios nos quais a operacionalização pode ser custosa, o ciberespaço está tão integrado à sociedade moderna que permite a "[...] atores não estatais e pequenos Estados exercerem influência significativa com baixos níveis de investimento" (Nye, 2011, p.128, tradução nossa [16]). Esses desafios foram reconhecidos por Barack Obama (2009-2017), que observou um paradoxo inerente ao ciberespaço:

> Um dos grandes paradoxos de nosso tempo é que as mesmas tecnologias que nos capacitam a fazer grandes coisas boas também podem ser usadas para nos prejudicar e infligir grandes danos [...] Grande parte de nossa infraestrutura essencial - nossos sistemas financeiros, nossa rede elétrica, sistemas de saúde - funciona em redes conectadas à Internet, o que é extremamente capacitador, mas também perigoso, e cria novos pontos de vulnerabilidade que não tínhamos antes (Estados Unidos, 2013, s/p, tradução nossa[17]).

---

[15] Pesquisas recentes questionam a precisão do número de 85%. Rosenzweig (2022) aponta que a origem desse dado remonta à National Strategy For Homeland Security (NSHS) de 2002, que não fornece uma fonte para tal informação. Contudo, essa discussão não diminui a validade do argumento central sobre a necessidade de parcerias público-privadas para o estabelecimento de padrões comuns para o aumento da resiliência das Infraesturturas Críticas e de respostas a incidentes.

[16] No original: *"[...] nonstate actors and small states can play significant roles at low levels of cost."*

[17] No original: *"And it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm […] Much of our critical infrastructure -- our financial systems, our power grid, health systems -- run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before."*

Portanto, pode-se concluir que a crescente integração das infraestruturas, tanto civis quanto militares, no ciberespaço, juntamente com o aumento de atores capazes de operar neste domínio para explorar dependências e vulnerabilidades em busca de vantagens próprias, desafia a premissa de que o Estado detém o monopólio legítimo do uso da força. Embora o papel do Estado continue a ser fundamental nas relações internacionais, o custo relativamente baixo para a operacionalização do ciberespaço contribui para uma redução das disparidades de capacidades, o que permite a atores não estatais tirarem proveito desse domínio para galgar seus objetivos (Medeiros; Goldoni, 2020).

Em adição a multiplicidade de atores, a incerteza resulta desse contexto em que diversos atores exploram o ciberespaço a perseguir benefícios próprios de maneira a não serem responsabilizados. A dificuldade dos Estados em atribuir autoria a ataques cibernéticos, sejam eles de subversão, espionagem ou sabotagem, alimenta uma percepção de impunidade. No entanto, essa percepção não detém completamente os esforços estatais em buscar atribuição para essas operações cibernéticas (Rid, 2012; Schmitt; Vihul, 2014).

Um exemplo de tentativa de atribuição de ataques cibernéticos ocorreu em 2008, durante a Guerra Russo-Georgiana. As raízes dessa guerra datam de conflitos anteriores, como as Guerras da Ossétia do Sul (1992) e da Abecásia (1993), que resultaram na perda de controle georgiano sobre territórios estratégicos para governos locais pró-Rússia (Hollis, 2011; Connell; Vogler, 2017). Desde 2004, as tensões entre a Rússia e a Geórgia escalaram, especialmente tendo em vista a política externa com inclinações pró-ocidentais da presidência de Mikheil Saakashvili (2004-2013).

Durante o conflito em 2008, operações cibernéticas foram executadas em simultâneo às operações militares terrestres, um fenômeno destacado por Rid (2012, p. 13, tradução nossa[18]) como potencialmente "a primeira ocorrência de um ataque cibernético independente em sincronia com uma campanha militar convencional". Os ataques cibernéticos visaram desestabilizar a comunicação governamental da Geórgia e atingiram instituições-chave como o Ministério das Relações Exteriores, setores financeiros e meios de comunicação. Embora as suspeitas recaíssem sobre

[18] No original: "*It may have been the first time an independent cyber attack happened in synchronization with a conventional military operation"*

a Rússia, dado o alinhamento estratégico e temporal dos ataques, Tikk-Ringas, Kaska e Vihul (2010, p. 74, tradução nossa[19]) ressaltam que “não há provas conclusivas de quem estava por trás dos ataques DDoS ou de defacement[20], embora a mídia tenha apontado o dedo para a Rússia”.

Desse modo, percebe-se que a própria arquitetura do ciberespaço privilegia o anonimato e complexifica os desafios enfrentados pelos Estados no que diz respeito a atribuição e responsabilização dos ataques cibernéticos. Como exemplo, os vazamentos da *Wikileaks* em 2017 expuseram parte do arsenal cibernético da *Central Intelligence Agency* (CIA), com destaque ao *Marble Framework*. Esta ferramenta foi projetada para alterar *malwares*[21] de modo que pareçam ter sido desenvolvidos por falantes de línguas distintas, como russo ou chinês (Burgess, 2017). Tal capacidade aumenta o risco de *false flags* e manipulação política do processo de atribuição (Devanny; Goldoni; Medeiros, 2022).

No que diz respeito à desterritorialidade, entende-se que a natureza em parte imaterial do ciberespaço — representada pelo espectro eletromagnético — transcende os limites físicos dos domínios tradicionais. Por possuir uma característica transversal em relação a esses domínios, o espaço cibernético pode gerar impactos diretos no ambiente físico de outros territórios. Assim, o conceito tradicional de território e fronteiras encontra-se confrontado pela existência de um espaço que é simultaneamente global e desprovido de barreiras físicas convencionais.

Um caso emblemático, considerado marcante por causar danos cinéticos para além das fronteiras nacionais, foi o Stuxnet em 2010. Supostamente desenvolvido conjuntamente pelos Estados Unidos e Israel, esse *malware* visava especificamente o Irã. Durante o período de 2006 a 2008, o Conselho de Segurança das Nações Unidas (CSNU) emitiu várias resoluções exigindo que o Irã suspendesse o enriquecimento de urânio. Apesar de o Irã afirmar estar em conformidade com o Tratado de Não Proliferação de Armas Nucleares (TNP), preocupações internacionais

---

[19] No original: *“there is no conclusive proof of who was behind the DDoS or defacement attacks, even though finger pointing at Russia was prevalent in the media”*

[20] DDoS, acrônimo para *Distributed Denial of Service*, é um ciberataque onde o alvo é inundado com tráfego online para que o serviço ou site seja impossível de ser acessado pelos usuários. Já o Defacement, ou deface, é simular a uma “pixação” virtual, consistindo na modificação de páginas da internet que possuam vulnerabilidades. (NIC.br, 2019; CISA, 2024).

[21] Um Malware é um programa inserido de maneira secreta em um sistema com o objetivo de comprometer a confidencialidade, integridade ou disponibilidade do sistema ou dos dados (CSRC, 2024).

surgiram após o país ter adquirido tecnologia de enriquecimento de urânio do Paquistão

Várias instalações de enriquecimento de urânio e plutônio, incluindo uma principal em Natanz, foram estabelecidas. Embora seja possível utilizar o urânio enriquecido para geração de energia, esse também poderia servir à produção de armas nucleares. A incapacidade da Agência Internacional de Energia Atômica (IAEA) de confirmar o uso exclusivamente pacífico dessas instalações exacerbou as preocupações globais. Nesse contexto, o Stuxnet foi projetado para explorar vulnerabilidades nos sistemas de controle e nas turbinas dessas plantas, com o objetivo de danificar e retardar o desenvolvimento de armas nucleares pelo Irã (Lindsay, 2013; Medeiros; Goldoni, 2020; Medeiros, 2024).

O caso Stuxnet ilustra como a desterritorialidade do ciberespaço pode influenciar a balança de poder e as dinâmicas no Sistema Internacional. Apesar de ser um fenômeno 'isolado' — o único ciberataque registrado até então a causar danos cinéticos a uma Infraestrutura Crítica —, o Stuxnet marcou o início do que poderia ser considerado uma 'era *Westfaliana* do ciberespaço', na qual as noções de soberania e controle territorial se estendem para o espaço cibernético. No entanto, surge o questionamento: como é possível construir fronteiras em um domínio essencialmente 'livre' e desterritorializado?

1.3. O ciberespaço como território

Atualmente, há uma tendência perceptível de equiparar o ciberespaço a um espaço geográfico e associá-lo a noções de território, fronteiras e soberania. A análise dessa representação espacializada do ciberespaço passa, primeiramente, pela Geografia e, mais especificamente, pela Geopolítica. O ciberespaço tornou-se — ou sempre foi — um campo no qual se manifestam disputas por poder e soberania, conceitos intrínsecos ao espaço geográfico e que são objetos de estudo da Geopolítica (Portela, 2018).

Ao debater sobre o conceito de território para além das concepções clássicas, Ferreira Neto (2020) destaca duas importantes vertentes conceituais. A primeira considera o território em sua forma tradicional, visto apenas como espaço geográfico sentido pelo homem; a segunda inclui variáveis que, embora não se encaixem completamente no tradicionalismo, ainda exercem influência sobre o território. Na

presente pesquisa a segunda vertente é privilegiada, pois considera-se que o ciberespaço sofre um processo de territorialização. Ao afirmar que o ciberespaço está sujeito à territorialização ou que é caracterizado pela desterritorialidade, aborda-se o cerne das questões territoriais. Toda desterritorialização ou territorialização está, portanto, referenciada a uma problemática territorial, ou seja, a uma concepção de território (Haesbaert, 2004). É com base nessa premissa que essa seção pretende compreender o ciberespaço como um "novo" tipo de territorialidade.

Os conceitos de espaço e território frequentemente são tratados de maneira intercambiável. No entanto, para Raffestin (1993), a equivalência entre os dois termos é errônea. O autor argumenta que o território resulta da apropriação de um espaço por um ator, seja de forma concreta ou abstrata. Esta abordagem é muito similar a uma das três vertentes territoriais propostas por Haesbaert (2004), que são: política, cultural e econômica.

QUADRO 5 - TRÊS VERTENTES BASE DA CONCEPÇÃO DE TERRITÓRIO

Vertente	Definição
Política	Se refere às relações de espaço-poder em geral, ou jurídico-políticas. É a vertente mais difundida, na qual o território é concebido como um espaço delimitado e controlado.
Cultural	Prioriza a dimensão simbólica e é mais subjetiva. O território é visto como produto da apropriação/valorização simbólica de um grupo em relação ao seu espaço vivido.
Econômica	Enfatiza o território como fonte de recurso e/ou incorporado no embate entre classes sociais e na relação capital-trabalho.

Fonte: Elaboração própria com base em Haesbaert (2004)

Coelho Neto (2013) ao considerar definições presentes em diversos dicionários constatou que há uma predominância da abordagem política, isto é, a definição do território como uma extensão terrestre que é controlada por uma determinada jurisdição político-administrativa. Essa abordagem está intimamente conectada a noção de soberania e ao Estado-nação moderno. Com a conclusão da Guerra dos Trinta Anos (1618-1648) através da Paz de Westfália — um conjunto de tratados decisivos para este fim — estabeleceu-se um novo sistema interestatal, atribuindo ao Estado a posição de autoridade soberana central. Essa mudança no cenário político internacional é analisada por Vieira de Jesus (2010, p. 222), que destaca que:

> O sistema de Estados soberanos exigia instituições estatais dentro das fronteiras e o desaparecimento de autoridades que interferissem de fora, para que a autoridade suprema vigorasse dentro do território e tivesse independência política e integridade territorial. Tal autoridade conota

> legitimidade - aqui entendida como o direito de controlar instituições e poderes - e territorialidade, num momento em que as pessoas governadas pelos detentores de soberania são definidas pela locação dentro das fronteiras, não por relações familiares ou por crença religiosa.

Nesse sentido, as fronteiras constituem um elemento-chave na definição de território, pois funcionam como demarcações essenciais que distinguem o que é interno do que é externo. Ventre (2019, p. 79) expressa essa ideia ao declarar que “a fronteira é, acima de tudo, um limite entre o que está dentro e o que está fora”. Portanto, pode-se entender a fronteira como um elemento de delimitação que confere ao território seu caráter zonal. É por meio das fronteiras que o Estado exerce seu poder de controle, e transforma o que era meramente espaço em território (Medeiros, 2019).

No entanto, as transformações proporcionadas pela revolução técnico-científica desestabilizaram a relação tradicional entre território e jurisdição (Israel, 2020). No contexto dessa transformação, a penetração do ciberespaço na estrutura das sociedades incitou teóricos a profetizar o declínio dos territórios. Um exemplo claro é Bertrand Badie (1996), que emergiu como uma voz proeminente ao argumentar em seus escritos e conferências a favor de um "fim do território *westfaliano*". A lógica territorial, então, seria suplantada pela lógica de rede, pois:

> A rede leva sempre consigo um imaginário de transição, entre a liberação de um sistema piramidal e hierárquico de que o Estado é o arquétipo, e a promessa de um sistema futuro, o da associação universal, anunciador de um novo tipo de relação igualitária (Musso, 2004, p. 34).

O que Badie não levou em conta, por exemplo, é que o território não é um conceito imutável; suas definições e conceitos “estiveram se alternando no espaço e no tempo com as ferramentas tecnológicas à disposição da sociedade organizada” (Gottmann, 2012, p. 525). Essa dinâmica fica evidente na definição de espaço geográfico proposta por Milton Santos (1986), pois compreende-se que: (I) o espaço geográfico funciona como um campo de forças sociais; e (II) esse espaço é sempre relativo ao tempo e à estrutura. Portanto, aplicar de maneira pura conceitos territoriais clássicos para compreender o espaço cibernético, um produto da contemporaneidade, não faz sentido. Da mesma forma, não é adequado analisar o ciberespaço com base nas noções de espaço cibernético originárias da ARPANET, visto que este espaço evoluiu (Portela, 2018).

Durante a história, os Estados têm ampliado suas definições de território para além das fronteiras terrestres tradicionais. Fruto das pressões e competições

sistêmicas no cenário internacional, as dimensões marítima, aérea e extra-atmosférica ganharam contornos de dimensões territoriais. Essa expansão territorial não visou simplesmente a aquisição de mais espaço, mas foi impulsionada pela busca incessante por segurança e pelo controle de recursos estratégicos (Gottman, 2012; Ferreira Neto, 2018).

De maneira similar, o ciberespaço não escapa a essa dinâmica. Tradicionalmente compreendido como uma *global common*, o ciberespaço foi o protagonista da *Declaration of the Independence of Cyberspace*, carta aberta escrita por John Perry Barlow em resposta à Lei de Telecomunicações dos Estados Unidos. Nesse documento, Barlow afirma que o ciberespaço não está sujeito a limites fronteiriços tradicionais e critica a noção de que esse espaço possa ser moldado ou controlado de maneira centralizada por qualquer entidade governamental (Barlow, 1996).

De forma a contrariar as visões utópicas de Barlow, observa-se uma tendência crescente dos Estados em tentar construir fronteiras virtuais que assegurem sua soberania e segurança no domínio cibernético. Assim como o conceito de território, a concepção de fronteira também tem se transformado ao longo do tempo, respondendo às evoluções nas relações sociais, políticas, econômicas e tecnológicas (Mattos, 1990, *apud* Ferreira Neto, 2020). O General Meira Mattos (1990, *apud* Ferreira Neto, 2020), em sua contribuição teórica sobre fronteiras, postula que essas evoluem em conformidade com a história e identifica quatro estágios principais.

No primeiro estágio, há os “vazios de ecúmeno”, que são áreas pouco povoadas no qual grandes espaços vazios funcionam como separadores naturais. O segundo estágio inclui largas zonas inocupadas ou fracamente ocupadas, caracterizadas pela ausência de poder político significativo, impedindo que estas regiões exerçam pressão sobre entidades vizinhas. O terceiro estágio envolve faixas relativamente estreitas, onde a densidade populacional ainda não era suficiente para gerar pressão significativa entre países limítrofes. Finalmente, o quarto estágio é a “fronteira-linha”, definida por critérios variados — naturais, artificiais ou até astronômicos — que delineiam áreas nas quais a densidade populacional intensifica o contato e os interesses dos Estados.

Com os avanços tecnológicos, alguns autores desenvolvem teorias sobre uma nova etapa na evolução das fronteiras. Ferreira Neto (2012, 2018, 2020) destaca a existência da chamada Fronteira-Ponto, uma exclusividade do domínio cibernético.

Esse novo tipo de fronteira emerge da capacidade aprimorada de Detecção — identificar informações sobre ameaças; Processamento — refinar essas informações para tomada de decisão; e Atuação — implementar ações e neutralizar ameaças. Diferentemente das fronteiras tradicionais, que delimitam áreas entre países, as Fronteiras-Ponto são locais específicos nos quais a territorialidade e interesse de diversos atores — isto é, diferentes fluxos informacionais — podem colidir causando danos a “pontos” no território ou fora deste. Esses pontos podem estar localizados tanto na camada física, como nas infraestruturas críticas discutidas, quanto em outras camadas relacionadas ao espaço cibernético.

A partir desta construção teórica, conclui-se que a territorialização se manifesta no ciberespaço e por meio dele. Portanto, é viável conceber a fronteira-ponto como uma interseção entre a territorialização tradicional, que utiliza fronteiras para delimitar o controle e a soberania de um Estado, e a influência do ciberespaço nas dinâmicas geopolíticas contemporâneas. No cerne dessa questão está a informação, o recurso base das disputas territoriais que ocorrem no ciberespaço. Castells já antecipava esse cenário:

> Como afirmei nos primeiros capítulos deste livro, o que é mais distintivo em termos históricos entre as estruturas econômicas da primeira e da segunda metade do século XX é a revolução nas tecnologias da informação e sua difusão em todas as esferas de atividade social e econômica, incluindo sua contribuição no fornecimento da infra-estrutura para a formação de uma economia global. Portanto, proponho mudar a ênfase analítica do pós-industrialismo (uma questão pertinente de previsão social ainda sem resposta no momento de sua formulação) para o informacionalismo. Nesta perspectiva, as sociedades serão informacionais, não porque se encaixem em um modelo específico de estrutura social, mas porque organizam seu sistema produtivo em torno de princípios de maximização da produtividade baseada em conhecimentos, por intermédio do desenvolvimento e da difusão de tecnologias da informação e pelo atendimento dos pré-requisitos para sua utilização (Castells, 2001, p. 268)

Informação é poder. Essa máxima é observada de forma clara nas comparações feitas em relação à importância da informação e do petróleo (The Economist, 2017). A ampla coleta de dados individuais por empresas e órgãos governamentais transformou-se em um ativo crucial para o atual estágio do capitalismo, servindo como um meio de acumulação e reprodução de riqueza (Cassino; Souza; Silveira, 2021) e, consequentemente, para a manutenção do status quo das Grandes Potências. Nesse sentido, os Estados sentem-se cada vez mais compelidos a tentar construir fronteiras — ou territorializar — o espaço cibernético como forma de controlar o acesso a esse recurso vital na era contemporânea.

No que concerne as fronteiras no espaço cibernético, as tentativas de sua delimitação através de uma diversidade de mecanismos projetados para o monitoramento, controle, filtragem e supervisão dos fluxos de informação. Uma das ferramentas mais conhecidas como parte das estratégias de territorialização do ciberespaço são os *firewalls* nacionais. O *Great Firewall* da China exemplifica tal prática ao impor limitações ao acesso de determinados sites, como o Facebook e o Youtube, e ao filtrar certos materiais e conteúdos considerados sensíveis pelo governo (Lambach, 2020; Zhang, 2021; Japaridze, 2023).

A delimitação de fronteiras também pode ocorrer por meio da imposição de determinadas formas de governança. Na governança da internet, por exemplo, dois modelos principais se destacam: o modelo *multi-stakeholder*, que inclui diversos grupos como a comunidade técnica, sociedade civil, meio acadêmico, setor privado e o governo; e o modelo mais centralizado no Estado, que concentra o controle governamental. Esses modelos refletem uma dualidade frequentemente adotada pelo ocidente, no qual há uma polarização entre democracias liberais — vistas como defensoras da liberdade de expressão e promotoras do ciberespaço como um bem comum global — e regimes autoritários, descritos como empenhados na territorialização deste espaço (Deibert, 2016).

Além disso, é perceptível que os Estados estão presos nessas duas lógicas contrárias, mas ao mesmo tempo complementares. Por um lado, sua presença no ciberespaço é imprescindível, dada a importância da conectividade como alicerce para a economia, a segurança nacional e o bem-estar social. Por outro, há um esforço frequente em impor suas fronteiras físicas e, por conseguinte, a soberania nacional em um espaço no qual o espectro eletromagnético desafia e dilui facilmente os conceitos tradicionais de território. Ventre (2019) articula esse impasse como o dilema das fronteiras virtuais, no qual tanto a manutenção de um espaço livre quanto a construção de fronteiras são necessários.

Ao fim e ao cabo, discurso e prática nem sempre coincidem, portanto, pode-se inferir que a prática da territorialização do ciberespaço mostra-se comum a ambos os polos, o que desafia a divisão simplista apresentada. Tomando os Estados Unidos como exemplo, apesar de serem bastiões de um ciberespaço livre e apoiadores do modelo multi-stakeholder, da liberdade de expressão e do livre comércio, adotam cada vez mais políticas protecionistas em prol da sua segurança nacional. A abordagem da administração Joe Biden (2021-) em relação à crescente presença de carros

inteligentes chineses no mercado americano reflete preocupações acentuadas com a soberania dos dados. Os Estados Unidos consideram esses veículos — intrinsecamente ligados a smartphones, sistemas de navegação e infraestruturas críticas — como potenciais vetores para a República Popular da China acessar indevidamente dados sensíveis de cidadãos americanos. Mais alarmante ainda é a possibilidade teórica de o governo chinês poder controlar e desativar esses sistemas à distância (Estados Unidos, 2024).

Com base nisso, esta pesquisa postula que um dos mecanismos basilares para a territorialização do ciberespaço está inserido sob o guarda-chuva da 'cibersegurança'. É em nome da cibersegurança, estreitamente vinculada à segurança nacional, que os Estados justificam a ampliação de sua soberania para o ambiente cibernético.

1.4. A cibersegurança como base da territorialização

Ao abordar a cibersegurança, inicialmente, é necessário explicitar sua intersecção com a segurança nacional, pois isso revela a evolução da percepção e da prioridade que essa agenda recebeu no pós-Guerra Fria. Inicialmente tratada como uma preocupação predominantemente técnica, voltada para a defesa de sistemas de informação, a cibersegurança evoluiu para ser reconhecida como um elemento crítico para a segurança nacional. Este reconhecimento resulta do aumento exponencial das ameaças cibernéticas e da crescente dependência da sociedade em relação aos sistemas informacionais. Esses fatores não apenas desafiam a integridade desses sistemas, mas também ameaçam infraestruturas críticas (Cavelty, 2010).

Portanto, é possível estabelecer uma fase da cibersegurança antes e depois de seu *status* ser elevado a uma prioridade de segurança nacional. Nissenbaum (2005) destaca uma distinção fundamental entre os conceitos de *computer security* e cibersegurança. A *computer security* concentra-se em três pilares essenciais: disponibilidade, integridade e confidencialidade. Suas estratégias visam proteger sistemas computacionais e usuários contra três categorias principais de ataques: (I) aqueles que comprometem sistemas e redes (ou partes destes), tornando-os indisponíveis para os usuários, exemplificados por ataques DDoS, vírus, worms e malwares; (II) ataques que colocam em risco a integridade das informações ou dos sistemas e redes, através da corrupção de dados ou interrupção de códigos; e (III)

ataques que violam a confidencialidade das informações e das comunicações, seja por interceptação ou acesso não autorizado a sistemas ou redes.

Já a cibersegurança é vista por Nissenbaun (2005) sob uma ótica mais ampla e engloba três eixos principais: (I) as ameaças decorrentes do uso de computadores em rede como ferramentas para a organização e comunicação disruptivas; (II) o risco de ataques contra infraestruturas críticas; e (III) as ameaças ao próprio sistema de informação.

Embora seja perceptível que *computer security* e cibersegurança compartilham algumas bases, a distinção entre elas reside no escopo e na amplitude de seus objetivos. A *computer security* tem raízes no campo científico da ciência da computação, enquanto a cibersegurança está mais vinculada e é frequentemente articulada por autoridades governamentais, de forma a associar o conceito de segurança de computadores às noções de segurança nacional. Nissenbaum (2005, p. 65, tradução nossa[22]) articula isso claramente ao discutir que o conceito de segurança dentro da cibersegurança "[...] não é extraído do uso comum, mas do uso desenvolvido na área especializada da segurança nacional".

Sobre isso, Cavelty (2013) argumenta que a associação frequentemente vista como inerente entre ciberespaço e segurança nacional, longe de ser uma premissa naturalmente concebida, precisou ser cuidadosamente construída e legitimada através do discurso político. A capacidade humana de aprender por analogia, ou seja, de compreender o novo através da comparação com o familiar, desempenha um papel crucial nesse processo (Tangredi, 2018). Assim, a forma como o ciberespaço é concebido — através de analogias e metáforas — molda significativamente a formulação de estratégias de segurança. Nesse contexto, Cavelty (2013) identifica três tipos de metáforas que dominam o discurso sobre segurança cibernética: as parasitárias (como *worms* e vírus), espaciais (como ciberespaço e soberania digital) e ecológicas (como organismo e ecosfera). Cada uma dessas metáforas enseja abordagens específicas para a segurança cibernética e justifica a adoção de variadas respostas sociotécnicas.

De forma similar ao que foi feito em relação às definições de ciberespaço e infraestrutura crítica, é pertinente analisar como os Estados Unidos concebem o

---

[22] No original: *"[…] is drawn not from ordinary usage but from usage developed in the specialized arena of national security."*

conceito de cibersegurança e quais das metáforas apresentadas por Cavelty (2013) predominam em suas definições. No documento *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Estados Unidos, 2009, p. 2, tradução nossa[23]), a cibersegurança é definida como:

> Estratégia, política e padrões relacionados à segurança e operações no ciberespaço, abrangendo a gama completa de redução de ameaças, redução de vulnerabilidades, dissuasão, engajamento internacional, resposta a incidentes, resiliência e recuperação de políticas e atividades, incluindo operações de rede de computadores, garantia de informação, aplicação da lei, diplomacia, missões militares e de inteligência conforme elas se relacionam com a segurança e estabilidade da infraestrutura global de informação e comunicações.

Uma definição mais recente, concisa e enxuta presente no dicionário do Departamento de Defesa define a cibersegurança como:

> A atividade ou processo, habilidade ou capacidade, ou estado pelo qual os sistemas de informação e comunicação, bem como as informações neles contidas, são protegidos e/ou defendidos contra danos, uso não autorizado ou modificação, ou exploração (CISA, 2024, s/p, tradução nossa[24])

A partir das definições supracitadas, delineia-se que ambas concordam que, em essência, a cibersegurança reside nas atividades que permitem que os sistemas e as informações neles contidas estejam protegidos. Embora variem em tamanho e em escopo, ambas as definições contêm o elemento infraestrutural do ciberespaço. Observa-se que essas definições concebem a segurança cibernética por meio da metáfora espacial ao focar nas infraestruturas. Cavelty (2013) explica que quando o ciberespaço é visto como território sob ameaça, a segurança cibernética diz respeito às infraestruturas físicas que "[...] podem ser sujeitas ao princípio de territorialidade e soberania" (Cavelty, 2013, p. 118, tradução nossa[25]).

É a partir de tudo que foi discutido que se torna justificável tratar o ciberespaço como um território. Como observado, esse 'novo' domínio enfrenta as mesmas

---

[23] No original: strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.

[24] No original: "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

[25] No original: "[…] that can be subjected to the principles of territoriality and sovereignty."

pressões competitivas que as dimensões terrestres, marítimas e aéreas sofreram. Portanto, a territorialização desse espaço é de extrema importância nas estratégias de segurança nacional, pois se configura como uma condição *sine qua non* para ampliar o controle sobre as demais dimensões tradicionais. É por isso que afirmar que o território westfaliano está em decadência é uma falácia, pois “a complexificação do modelo westfaliano não implica o fim dos territórios, pois não há processo de desterritorialização sem que haja um movimento concomitante de reterritorialização” (Israel, 2020, p. 74).

Com base nestas reflexões, o próximo capítulo focará na análise da estrutura organizacional cibernética dos Estados Unidos. Tem-se em mente que, para posterior análise das políticas de cibersegurança dos Estados Unidos, é necessário, antes, conceber uma compreensão sólida da infraestrutura institucional que conforma o país.

2. A estrutura Organizacional de Cibersegurança dos EUA

O presente capítulo tem como objetivo mapear a estrutura organizacional de cibersegurança dos Estados Unidos. Compreender como são distribuídas as funções e responsabilidades entre as diversas agências que compõem essa estrutura é condição *sine qua non* para analisar as estratégias nacionais de cibersegurança formuladas pelos governos que esta dissertação se propõe a examinar.

Serão analisadas a distribuição de funções e competências das principais agências atuantes na cibersegurança daquele país, dentre elas, o *Department of Homeland Security* (DHS), a *Cybersecurity and Infrastructure Security Agency* (CISA), o *Department of Defense* (DoD), o *United States Cyber Command* (USCYBERCOM), o *Department of* Justice (DOJ), o *Federal Bureal of Investigation* (FBI), o *United States Secret Service* (USS) e o *Office of National Cyber Director.*

Esse estudo exige uma prévia e breve reflexão sobre os conceitos de Segurança e Defesa no domínio cibernético[26], uma vez que as atribuições daquelas instituições frequentemente convergem e, em algumas situações, se sobrepõem entre si, conforme demonstrado por Rocha (2022). Uma breve análise bibliográfica e documental desses conceitos permitirá abordar dois pontos principais: (I) a dificuldade em traçar limites claros entre Segurança e Defesa no ciberespaço; e (II) os casos em que as competências tradicionais dessas esferas são extrapoladas, quando instituições originalmente voltadas à segurança assumem papéis vinculados à defesa, e vice-versa.

As discussões fundamentais sobre os conceitos de Segurança e Defesa concentram-se, em sua essência, na distinção entre atuação interna e externa. Rocha (2022) observa, os atores estatais de segurança são responsáveis pela proteção interna do país, enquanto os de defesa atuam contra ameaças externas, vindas de fora do território nacional. Contudo, na prática, essa divisão teórica nem sempre se sustenta.

O Dicionário Oxford (2024) define segurança como as atividades destinadas a proteger um país, edificações ou indivíduos contra perigos e ataques. Essa definição reforça a ideia de que segurança não é uma condição passiva, mas um esforço

[26] Para informações mais profundas e detalhadas sobre essa discussão ver a dissertação “Governança Securitária do Ciberespaço: Questões sobre Segurança e Defesa” de Henrique riqueiro da Rocha (2022).

contínuo que deve ser conquistado e mantido. De forma complementar, o *Dictionary of Military and Associated Terms* apresenta três abordagens sobre segurança, que serão detalhadas na tabela abaixo:

QUADRO 6 - DEFINIÇÕES DE SEGURANÇA NO DICIONÁRIO DOD

	Definições apresentadas pelo DoD
1	Medidas tomadas por uma unidade, atividade ou instalação militar para se proteger contra todos os atos destinados a prejudicar ou que possam prejudicar sua eficácia (Estados Unidos, 2021, p. 191, tradução nossa[27]).
2	Uma condição resultante do estabelecimento e da manutenção de medidas de proteção que garantem um estado de inviolabilidade contra atos ou influências hostis (Estados Unidos, 2021, p. 191, tradução nossa[28]).
3	Com relação a assuntos confidenciais, a condição que impede que pessoas não autorizadas tenham acesso a informações oficiais que são protegidas no interesse da segurança nacional (Estados Unidos, 2021, p.191, tradução nossa[29])

Fonte: Elaboração própria com base em (Estados Unidos, 2021).

A primeira definição apresentada na tabela reflete a concepção de segurança descrita no dicionário *Oxford*, que enfatiza um conjunto de medidas voltadas à proteção. Por outro lado, o *Department of Defense* (DoD) destaca que essas medidas são implementadas por unidades, atividades ou instalações militares, com o propósito de assegurar a eficácia operacional. Assim, o DoD explicita que a segurança está diretamente ligada a ações militares concretas. De forma semelhante, Stephen Walt (1991), com base em premissas do realismo, argumenta que os Estudos de Segurança, e a segurança em si, devem ser prioritariamente compreendidos no contexto do uso, controle e ameaça da força militar. Essa abordagem prioriza a dimensão militar e trata outras ameaças potenciais — como questões ecológicas,

---

[27] No original*: "Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness."*

[28] No original: "*A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences."*

[29] No original: "*With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security*."

econômicas e sociais — como parte da análise de segurança de um Estado apenas quando apresentam implicações de natureza militar (Tarry, 1999).

A segunda definição aborda a segurança como uma condição ou estado, alcançado por meio do estabelecimento de medidas específicas que garantem proteção contra ações hostis. Wolfers (1952, apud Baldwin, 1997, p. 13, tradução nossa[30]) compartilha dessa perspectiva ao conceituar segurança como a "ausência de ameaças aos valores adquiridos" Nesse sentido, o autor apresenta a segurança como uma condição variável, em que um Estado pode possuir maior ou menor grau de segurança, conforme as circunstâncias e escolhas políticas (Baldwin, 1997). Por outro lado, autores como Brodie (1950) divergem dessa visão gradativa e defendem uma concepção absoluta de segurança. Para Brodie, "se estivermos parcialmente seguros, não estamos seguros de forma alguma" (Brodie, 1950, p. 5, tradução nossa[31]).

A terceira definição aborda a segurança em um contexto mais restrito, vinculada à proteção de informações sensíveis e estratégicas para a segurança nacional. Essa perspectiva é ainda mais relevante em uma sociedade informacional, como descrita por Castells (2001), ao afirmar que as estruturas produtivas modernas se baseiam no conhecimento e na tecnologia. Nesse contexto, a informação possui uma centralidade sem precedentes, e se torna a base para a produtividade, a competitividade e, por extensão, para a segurança nacional.

No que diz respeito à Defesa, o Dicionário Oxford apresenta definições como: o ato de proteger alguém ou algo de um ataque, ou algo que oferece proteção contra ataques inimigos. Essas definições refletem uma abordagem ampla e genérica do termo. Em contraste, os Estados Unidos, em suas estratégias de Defesa ou no dicionário de termos militares do DoD, não apresentam uma definição explícita sobre o que entendem por Defesa. Os únicos termos relacionados que recebem alguma definição no dicionário do DoD são Defesa Aeroespacial (*Aerospace Defense*), Defesa Aérea (*Air Defense*) e Defesa Cibernética (*Cyberspace Defense*). Diferentemente das definições de segurança — que enfatizam medidas de proteção ou a descrevem como um estado ou condição — as definições relacionadas à Defesa incluem ações ofensivas, seja para destruir ou reduzir a eficácia de ataques inimigos. Rocha (2022)

---

[30] No original: *"the absence of threats to acquired values"*
[31] No original: *"If we are only half secure, we are not secure at all"*

interpreta a ausência da definição como uma estratégia deliberada. Ao evitar delimitar o conceito de forma clara, o país amplia as possibilidades de justificar ações sob o pretexto de defesa, inclusive aquelas que poderiam ser consideradas injustificáveis caso o termo fosse precisamente definido.

De acordo com Costa (1999), Segurança e Defesa possuem uma relação hierárquica e lógica. A Segurança sempre precede a Defesa, pois, segundo o autor, "é preciso estabelecer as bases sobre as quais se possa assentar a segurança da nação, ou das nações e de seus cidadãos. Depois, pensar em como se defender, caso estas bases sejam ameaçadas de rompimento" (Costa, 1999, p. 127). Nesse sentido, a Segurança é compreendida como um estado de proteção ou estabilidade, conforme descrito na segunda abordagem presente no Quadro 6, enquanto a Defesa é caracterizada como um ato, uma ação ou uma reação concreta para preservar esse status.

Nesse sentido, pode-se afirmar que o objetivo da Defesa é "evitar, por meio da posse de adequadas capacidades militares, agressões ao patrimônio [...] ou ações que afetem, ainda que indiretamente, interesses nacionais" (Amorim, 2012, p. 341-342). Em outras palavras, a Defesa refere-se ao esforço para assegurar a integridade territorial e a preservação do Estado diante de possíveis ameaças externas. Ainda que o conceito de Defesa aparente ser mais estável ao longo do tempo em comparação ao de Segurança, Rocha (2022) destaca um aspecto crucial: a interpretação e a aplicação do conceito variam entre os Estados, moldadas pelas percepções de ameaças, ambições estratégicas e capacidades disponíveis. Dessa forma, a Defesa adquire significados e formas distintos conforme o contexto específico de cada nação.

A partir disso, é possível compreender, de forma geral, a Segurança como as medidas preventivas adotadas para garantir a proteção de um Estado contra ações hostis, bem como a condição resultante dessas medidas. Por outro lado, a Defesa refere-se à capacidade do Estado de utilizar seus recursos militares para dissuadir forças externas e proteger sua soberania e integridade territorial. Em relação à atuação desses organismos, pode-se estabelecer uma distinção clara: enquanto os atores de Segurança enfrentam ameaças no âmbito doméstico, os de Defesa lidam com ameaças externas. No entanto, o ciberespaço, como ambiente informacional que transcende a lógica zonal (Medeiros; Goldoni, 2020), desafia essa dicotomia entre o interno e o externo. Como apontam Pagliari, Ayres Pinto e Viggiano (2020, p. 153):

> é fato que essa separação - especificamente, na área cibernética - é feita por uma linha tênue que em muitos momentos se desvanece, sendo difícil determinar ações de proteção específicas para cada tipo de ameaça e quem seriam os seus responsáveis diretos.

Em muitos casos, como destacam as autoras, a Defesa Cibernética é responsável pela proteção contra ameaças direcionadas ao aparato estatal e às Infraestruturas Críticas, enquanto a Segurança Cibernética foca na proteção contra ameaças relacionadas ao setor privado e ao bem-estar da sociedade civil. Nos Estados Unidos, entretanto, essa separação revela-se difícil de ser estabelecida devido à interdependência crescente entre as esferas pública e privada no ambiente cibernético.

QUADRO 7 - DEFINIÇÕES DE SEGURANÇA E DEFESA CIBERNÉTICA NO DICIONÁRIO DO DOD

Definições apresentadas pelo DoD	
Cyberspace Security	Ações tomadas dentro do ciberespaço protegido para impedir o acesso não autorizado, a exploração ou danos a computadores, sistemas de comunicações eletrônicas e outras tecnologias da informação, incluindo tecnologia da informação de plataforma, bem como as informações contidas neles, para garantir sua disponibilidade, integridade, autenticação, confidencialidade e não repúdio (Estados Unidos, 2024, p. 55, tradução nossa[32])
Cyberspace Defense	Ações tomadas dentro do ciberespaço protegido para derrotar ameaças específicas que violaram ou ameaçam violar as medidas de segurança do ciberespaço e incluem ações para detectar, caracterizar, combater e mitigar ameaças, incluindo malware ou atividades não autorizadas de usuários, e restaurar o sistema para uma configuração segura (Estados Unidos, 2024, p. 55, tradução nossa[33])

Fonte: Elaboração própria com base em Estados Unidos (2024).

A partir das definições apresentadas no Quadro 7, percebe-se que os Estados Unidos conceituam a Segurança Cibernética como a prevenção e a garantia contínua da disponibilidade e integridade de computadores (hardware), sistemas de comunicação e informações armazenadas nesses dispositivos. Essa definição se

[32] No original: Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

[33] No original: Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration

alinha às abordagens 2 e 3 do Quadro 6, por enfatizarem a inviolabilidade e a manutenção das medidas de proteção. Por outro lado, a definição de Defesa Cibernética destaca ações, ofensivas ou defensivas, voltadas à detecção, mitigação ou neutralização de ameaças que visem comprometer as medidas de segurança estabelecidas. Algo a ser ressaltado é que em ambas as definições a expressão "dentro do ciberespaço protegido" é empregada. Tal expressão sugere a existência de delimitações no ciberespaço, que passam a ser tratadas como áreas sob jurisdição do DoD ou, de maneira mais ampla, como espaços pertencentes aos Estados Unidos.

Em suma, embora as funções de Segurança Cibernética e Defesa Cibernética frequentemente se confundam e se sobreponham no ciberespaço, é basilar distingui-las conceitualmente para delimitar as responsabilidades de cada esfera. Rocha (2022) pontua que a Segurança Cibernética possui um caráter mais amplo, ao abranger a proteção de sistemas conectados à internet e a garantia da segurança da população no domínio cibernético. A Defesa Cibernética, por sua vez, refere-se a ações ofensivas, defensivas e exploratórias realizadas pelo Estado para salvaguardar a soberania nacional. Dessa forma, a Defesa Cibernética, como conceito mais objetivo, está subordinada à Segurança Cibernética, o que reforça a relação de interdependência entre as duas esferas.

Dadas as considerações sobre os conceitos de Segurança, Defesa, Segurança Cibernética e Defesa Cibernética, torna-se relevante analisar os diferentes organismos que compõem a estrutura organizacional de Cibersegurança e Ciberdefesa nos Estados Unidos e avaliar se eles se enquadram nas conceituações propostas.

2.1. O *Department of Defense* (DoD): o United States Cyber Command (USCYBERCOM) e a National Security Agency (NSA)

Desde a sua criação, o *Department of Defense* (DoD) tem sido um pilar na defesa nacional dos Estados Unidos. Com o avanço da tecnologia, era inevitável que o ciberespaço se tornasse mais um campo de atuação para o DoD. Assim como a sociedade, os militares dependem fortemente do ciberespaço para realizar suas operações nos domínios convencionais. Como destacado no *2010 Quadrienal Defense Review*:

> Não há como exagerar nossa dependência das redes de informações do DoD para o comando e o controle de nossas forças, a inteligência e a logística das quais elas dependem e as tecnologias de armas que desenvolvemos e colocamos em campo (*Department of Defense*, 2010, p. 37, tradução nossa [34]).

As preocupações com um possível "Cyber Pearl Harbor" ganharam destaque nos discursos políticos e nas discussões sobre defesa nos Estados Unidos durante a década de 1990. Esse temor não era meramente especulativo: anualmente, o Estado-Maior Conjunto do Pentágono realizava exercícios conhecidos como *Eligible Receiver*, projetados para identificar ameaças e explorar possíveis oportunidades futuras. O *Eligible Receiver 97* destacou-se por seu foco em ataques cibernéticos. Nele, um *red team* da National Security Agency (NSA) simulou ações de forças hostis de países como Coreia do Norte, Irã e Cuba. O objetivo era atacar infraestruturas críticas e as capacidades de comando e controle militar do Departamento de Defesa, usando apenas softwares e informações publicamente disponíveis na internet.

Embora muitos documentos permaneçam sigilosos, é possível compreender a dimensão e complexidade do exercício. Fred Kaplan (2016), autor e jornalista norte-americano, descreve que o exercício se desenvolveu em três fases: (I) o *Red Team* lançaria um ataque coordenado nas infraestruturas críticas, especialmente na rede elétrica e nas linhas de comunicação de emergência do 911; (II) ataque massivo nas linhas de comunicação militar (telefone, fax e redes de computador) para provocar disrupção nos sistemas de comando e controle, dificultando a resposta. Durante três meses e meio, o *red team* preparou o ataque, ao analisar as redes e os protocolos militares. O exercício, inicialmente previsto para duas semanas — com possível extensão de mais duas — concluiu-se em apenas quatro dias, com o êxito do *red team* em penetrar as redes do Departamento de Defesa.

A atuação da NSA — órgão que, em seu próprio nome, carrega a palavra 'segurança' (tema explorado nesta seção) — exemplifica a complexidade inerente à distinção entre os conceitos de 'segurança' e 'defesa' cibernética, conforme discutido na introdução deste capítulo. Além disso, a vinculação de uma agência que tem a segurança como elemento central em sua denominação ao Departamento de Defesa

---

[34] No original: *"There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field."*

é, por si só, um aspecto que demanda reflexões mais aprofundadas, as quais extrapolam os limites desta dissertação.

No que tange ao exercício em questão, o caso evidencia, de certa forma, a superioridade da agência de 'segurança' em relação à sua contraparte de 'defesa', uma vez que a operação, inicialmente planejada pelo DoD para durar até quatro semanas, foi concluída em apenas quatro dias, resultado do êxito do time liderado pela NSA.

Nesse sentido, o *Eligible Receiver 97* demonstrou de maneira prática aos militares que, já em 1997, um adversário com o mínimo de qualificação e recursos poderia causar danos consideráveis caso o sistema atacado não estivesse adequadamente protegido (Warner, 2012). Mais do que evidenciar fragilidades nos sistemas de defesa do Pentágono, o exercício sinalizou uma transformação profunda no escopo e na dinâmica dos conflitos militares no final do século XX. Essa transformação, sustentada pelas mudanças sociais, econômicas e tecnológicas proporcionadas pelas inovações no ambiente técnico-científico-informacional, serviu como base para o desenvolvimento do conceito de *Revolution in Military Affairs* (RMA).

A base teórica da RMA emergiu inicialmente na década de 1960 no campo acadêmico soviético, como uma tentativa de compreender as transformações causadas pela Primeira Guerra Mundial no âmbito militar (Medeiros, 2024). Como destacam Storti e Ferreira (2022), durante a década de 1970, os soviéticos aprofundaram a análise sobre as implicações das novas tecnologias, como munições de precisão e mísseis de cruzeiro, para a condução da guerra. A partir dessas reflexões, estabeleceu-se o conceito de "Revolução Técnico-Militar", que tinha como enfoque predominante as inovações tecnológicas aplicadas aos equipamentos bélicos e suas repercussões estratégicas.

O conceito de Revolução Técnico-Militar foi adaptado e expandido nos Estados Unidos, e passou a ter um significado mais amplo. Diferentemente da abordagem soviética, que atribuía aos avanços tecnológicos o papel central na transformação da condução da guerra, a RMA americana incorporou fatores doutrinários, táticos e organizacionais. Em síntese, os Estados Unidos reconheceram que a tecnologia, *per se*, não seria suficiente para promover tais mudanças; inovações organizacionais e doutrinárias eram necessárias para que esses avanços tecnológicos fossem explorados em seu completo potencial (Saint-Pierre e Gonçalves, 2018).

Nesse contexto, o advento do ciberespaço como domínio operacional reforça a centralidade de uma abordagem integradora. Medeiros (2020; 2024) argumenta que o ciberespaço rompe paradigmas tradicionais da guerra ao introduzir características como a desterritorialidade e a incerteza, que permitem a múltiplos atores, estatais e não estatais, alcançar objetivos estratégicos sem as limitações impostas pelos domínios convencionais. Essas dinâmicas exigem das forças armadas adaptações profundas para enfrentar ameaças que desafiam as estruturas tradicionais de defesa.

Exercícios como o *Eligible Receiver 97* evidenciaram de forma empírica a necessidade de mudanças organizacionais e doutrinárias para lidar com a vulnerabilidade das redes militares e das infraestruturas críticas. Ao demonstrar a capacidade de atores com recursos limitados de causar danos estratégicos significativos, o exercício antecipou os desafios impostos pelo ciberespaço e reforçou os princípios centrais da RMA: a integração entre tecnologia, doutrina e organização como resposta às transformações paradigmáticas nos conflitos contemporâneos.

Com base nos princípios estabelecidos pela RMA e nas lições aprendidas com o *Eligible Receiver 97*, o DoD desenvolveu uma nova abordagem operacional, considerada a raiz do que posteriormente se tornaria o *U.S. Cyber Command* (USCYBERCOM). Essa iniciativa concretizou-se com a criação da *Joint Task Force - Computer Network Defense* (JTF-CND) em 1998, cuja principal responsabilidade era proteger as redes do DoD. No ano seguinte, a JTF-CND foi reestruturada como *Joint Task Force - Computer Network Operations* (JTF-CNO), que incorporou, além das atribuições de defesa, a condução de operações ofensivas em redes de computadores. Subordinada ao *U.S. Space Command* (USSPACECOM), essa força-tarefa marcou um avanço significativo na evolução das capacidades cibernéticas do DoD (USCYBERCOM, 2024). Assim, considerando a participação da NSA no exercício de 1997, é possível inferir que a atuação dessa agência influenciou tanto a estrutura organizacional quanto a doutrina de defesa cibernética dos EUA. Esse fato reforça, mais uma vez, os desafios inerentes à delimitação entre os conceitos de segurança e defesa cibernética.

Em 2004, o documento *National Military Strategy of the United States of America* reconheceu o ciberespaço como um domínio operacional, comparável à terra, ao mar, ao ar e ao espaço. Esse reconhecimento teve profundas implicações operacionais para o DoD que, no mesmo ano, reorganizou a JTF-CNO em frentes defensivas e ofensivas, denominadas, respectivamente, *Joint Task Force - Global*

Network Operations (JTF-GNO) e *Joint Functional Component Command – Network Warfare* (JFCC-NW) (USCYBERCOM, 2024). Contudo, em 2008, a invasão de uma rede militar revelou que essa abordagem segmentada entre defesa e ataque era insuficiente para lidar com a complexidade e a interdependência das ameaças no ciberespaço. Em resposta, o então Secretário de Defesa Robert Gates determinou, em 2009, a unificação das duas frentes, que culminou na criação do USCYBERCOM, um subcomando unificado sob a égide do USSTRATCOM.

Além das implicações operacionais, a escolha do termo "domínio" para designar o ciberespaço possui significativas repercussões político-estratégicas. Como argumenta Branch (2020; 2024), ao enquadrar metaforicamente o ciberespaço como um domínio paralelo aos tradicionais — terrestre, marítimo, aéreo e espacial —, as Forças Armadas dos Estados Unidos expandiram sua influência sobre a agenda de cibersegurança do país. Essa metáfora não apenas posicionou o ciberespaço como um espaço estratégico essencial, mas também reforçou a ideia de que ele exige capacidades militares específicas para defesa e operação. Um exemplo claro dessa retórica foi apresentado pelo Vice-Secretário de Defesa William J. Lynn III, que, em 2010, argumentou que a crescente importância do ciberespaço tornava imprescindível a criação de uma estrutura organizacional dedicada no Departamento de Defesa, capaz de responder às ameaças e assegurar a liberdade de ação nesse novo ambiente (Lynn, 2010). Essa perspectiva foi instrumental na criação do USCYBERCOM.

Sobre o comando, pode-se considerar que o USCYBERCOM tem três missões principais, a saber: (I) Operar e defender as redes de informação do DoD (DODIN), os dados e os modernos sistemas de armas que contêm vulnerabilidades que precisam ser protegidas; (II) Criar uma força cibernética capaz de realizar missões defensivas e ofensivas para dar suporte às demais forças; (III) Ser o elemento de resposta do DoD para impedir tentativas de penetração, destruição, danificação ou manipulação da infraestrutura dos Estados Unidos (Eliason, 2016).

No que concerne à sua atuação como um órgão tipicamente de Defesa, pode-se afirmar que as missões do USCYBERCOM estão alinhadas com as definições de Defesa e Defesa Cibernética apresentadas no início do capítulo. Isso fica evidente ao observar as missões supracitadas, nas quais o caráter ofensivo, uma característica tipicamente associada à Defesa Cibernética, é claramente destacado, especialmente na segunda missão, que inclui operações ofensivas de forma explícita. Contudo, a

terceira missão, ao abordar elementos de resposta para problemas domésticos, reflete atribuições tradicionalmente vinculadas a organismos de Segurança. Esse aspecto evidencia uma confluência entre as atribuições de Segurança e Defesa.

Com base nas missões apresentadas, o comando, na época liderado por Paul Nakasone, adotou uma postura mais assertiva no ciberespaço. Nakasone (2020) argumenta que, embora os Estados Unidos tenham sido historicamente eficazes em dissuadir ameaças no contexto da guerra convencional e nuclear, adversários e atores não estatais têm explorado o ciberespaço como uma arena assimétrica para comprometer o poder militar, político e econômico americano.

Essa perspectiva reforça as peculiaridades discutidas no primeiro capítulo desta dissertação: a desterritorialização, a multiplicidade de atores e a incerteza. Essas características inerentes ao ciberespaço tornam as operações cibernéticas uma escolha estratégica mais atraente, pois apresentam custos menores e consequências menos imediatas para os perpetradores, uma vez que ocorrem no limiar do conflito. Com isso, baseado nas premissas de *Defend Forward* e *Persistent Engagement*, o comando cibernético traçou paralelos com a Marinha e a Força Aérea — que "mantêm a paz" ao navegar pelos mares e patrulhar os céus — para que o USCYBERCOM atue de maneira proativa, identifique ameaças cibernéticas e tome medidas preventivas. De acordo com Nakasone (2019):

> Precisamos "Defend Forward" no ciberespaço, assim como fazemos nos domínios físicos. Nossas forças navais não se defendem permanecendo nos portos, e nosso poder aéreo não permanece nos campos de aviação. Elas patrulham os mares e os céus para garantir que estejam posicionadas para defender nosso país antes que nossas fronteiras sejam cruzadas. A mesma lógica se aplica ao espaço cibernético (Nakasone, 2019, p. 11, tradução nossa[35]).

A declaração de Nakasone, ao comparar a defesa do domínio cibernético aos domínios tradicionais, justifica e legitima uma postura mais proativa do USCYBERCOM (Branch, 2020, 2024). Nessa analogia entre patrulhas marítimas e aéreas, o ex-comandante normaliza a condução de operações cibernéticas preventivas pelos Estados Unidos em redes externas. Não somente, mas sua escolha de palavras é relevadora da percepção norte-americana sobre o ciberespaço. A afirmação de que é necessário patrulhar para "defender nosso país antes que **nossas**

[35] No original: "We must "defend forward" in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace."

fronteiras sejam cruzadas” (destaque nosso) e que essa “mesma lógica se aplica ao ciberespaço” evidencia uma tentativa de territorializar esse domínio.

Como destacado no primeiro capítulo, especificamente na seção que aborda o ciberespaço como território, a territorialização dos domínios tradicionais segue uma dinâmica histórica em que pressões geopolíticas levam os Estados a expandir sua soberania sobre espaços anteriormente concebidos como *Global Commons*. Esse movimento busca tanto antecipar ameaças externas (segurança) quanto assegurar recursos estratégicos (poder). Embora essa dinâmica também se aplique ao ciberespaço, sua natureza intrinsecamente desterritorializada torna o processo de territorialização mais complexo.

FIGURA 2 - COMPONENTES DO COMANDO CIBERNÉTICO DOS ESTADOS UNIDOS (USCYBERCOM)

Fonte: Deppa (2017)

O organograma apresentado na Figura 2 ilustra a estrutura organizacional do USCYBERCOM. O comando opera sob a liderança de um comandante, atualmente Timothy D. Haugh, que, de forma *“dual-hatted”*, também ocupa o cargo de diretor da *National Security Agency* (NSA). Não somente, mas o USCYBERCOM é composto por seis forças cibernéticas especializadas que representam diferentes ramificações das Forças Armadas dos Estados Unidos.

Em primeiro lugar, o Army Cyber Command (ARCYBER) apoia o Exército no ciberespaço por meio de operações defensivas e ofensivas. Suas responsabilidades incluem a proteção das Redes de Informação do Departamento de Defesa (DoDIN) e a execução de operações cibernéticas ofensivas contra adversários (Army Cyber Command, 2024).

No que se refere à Marinha, o *Fleet Cyber Command* (FLTCYBER), estabelecido oficialmente em janeiro de 2010, foi criado em conjunto com a reativação da *U.S. Tenth Fleet* (Décima Frota). O FLTCYBER planeja, coordena e conduz atividades operacionais no ciberespaço, com o objetivo de garantir liberdade de ação à Marinha em todos os domínios. A Décima Frota atua como seu braço operacional e entrega os efeitos táticos e operacionais necessários através do espectro eletromagnético (Fleet Cyber Command, 2024).

A criação da *Air Forces Cyber* (AFCYBER, ou Décima Sexta Força Aérea), em outubro de 2019, unificou as atribuições anteriormente distribuídas entre a Vigésima Quinta Força Aérea, responsável por inteligência, vigilância e reconhecimento (*Intelligence, Surveillance, and Reconnaissance*, ISR), e a Vigésima Quarta Força Aérea, que concentrava as operações cibernéticas. Com ênfase na Guerra de Informação (*Information Warfare*), a AFCYBER reúne, sob um único comando, capacidades de ISR, operações cibernéticas, operações de informação, guerra eletrônica, meteorologia e assuntos públicos (*public affairs*) (Air Forces Cyber, 2024).

A *Marine Corps Forces Cyberspace Command* (MARFORCYBER) conduz operações cibernéticas de amplo espectro no domínio cibernético. Suas funções incluem a realização de operações defensivas e ofensivas em apoio ao Corpo de Fuzileiros Navais, às Forças Conjuntas e de Coalizão, além da defesa da Marine Corps Enterprise Network (MCEN) (Marine Forces Cyber Command, 2024).

Nesse sentido, a presença de forças cibernéticas especializadas em todas as ramificações das Forças Armadas dos Estados Unidos evidencia o papel central do ciberespaço na garantia da soberania nacional. Além disso, o conceito de transversalidade, discutido no primeiro capítulo, ressalta a importância do ciberespaço para a projeção de poder. De acordo com Ventre (2011), o ciberespaço é transversal porque estabelece pontos de contato com os domínios tradicionais, ao mesmo tempo em que os influencia e é influenciado por eles. Assim, cada ramificação das Forças Armadas necessita de um componente cibernético para sustentar e ampliar sua capacidade de projeção de poder nesse domínio (Ferreira Neto, 2020).

Além das forças mencionadas, as últimas adições ao USCYBERCOM incluem a *Cyber Mission Force* (CMF), criada em 2012, o *Joint Force Headquarters – DOD Information Network* (JFHQ-DODIN), estabelecido em 2014 e a *Cyber National Mission Force* (CNMF), criada também em 2014. A CMF atua como o braço operacional do USCYBERCOM, com 6.200 militares e civis organizados em 133

equipes divididas em três categorias principais: os *National Mission Teams* (NMTs), que monitoram atividades adversárias e bloqueiam ataques; os *Combat Mission Teams* (CMTs), responsáveis por conduzir operações cibernéticas ofensivas em apoio aos comandos combatentes; e os *Cyber Protection Teams* (CPTs), encarregados de defender a Rede de Informação do Departamento de Defesa (DoDIN).

O JFHQ-DODIN, por sua vez, supervisiona e realiza a defesa operacional do DoDIN. Suas atribuições incluem o monitoramento contínuo e a resposta imediata a incidentes, a fim de proteger a integridade e garantir a resiliência das redes do Departamento de Defesa.

No que concerne a *Cyber National Mission Force* (CNMF), esta desempenha o papel de Força Cibernética Conjunta encarregada de proteger os interesses nacionais dos Estados Unidos no ciberespaço. Nos últimos anos, a CNMF atuou ativamente na segurança eleitoral, além de combater *ransomwares*, ciberespionagem e outras ameaças à cibersegurança dos Estados Unidos. Sobre a segurança eleitoral, o USCYBERCOM e a *National Security Agency* (NSA) integram o *Election Security Group* (ESG), e contam com a parceria do *Federal Bureau of Investigation* (FBI) e do *Department of Homeland Security* (DHS) para proteger o processo eleitoral dos Estados Unidos contra interferência externas (Department of Defense, 2021).

Essa atuação conjunta no ESG reflete a complexidade das atribuições de Segurança e Defesa no ciberespaço. Tradicionalmente, a segurança eleitoral é considerada uma questão doméstica, sendo associada a organismos como o DHS e o FBI. A designação da infraestrutura eleitoral como parte da Infraestrutura Crítica dos Estados Unidos, feita pelo DHS em janeiro de 2017, reforça essa percepção ao vinculá-la à segurança interna (Department of Homeland Security, 2017). Contudo, a participação do USCYBERCOM no ESG evidencia como a Defesa Cibernética, ao lidar com ameaças externas que impactam processos internos, opera sob o guarda-chuva da Segurança Cibernética, e destaca a intedependência entre essas duas esferas.

No que diz respeito à National Security Agency/Central Security Service (NSA/CSS), esta se configura como uma das principais agências da Comunidade de Inteligência (CI) dos Estados Unidos. O que torna sua posição singular é o fato de, simultaneamente, integrar a CI e estar subordinada ao DoD. Durante a formação do USCYBERCOM, foi estrategicamente decidido que o comando aproveitaria a expertise e a infraestrutura já consolidadas da NSA, o que resultou no atual arranjo

double-hatted, no qual o comandante do USCYBERCOM acumula o cargo de diretor da NSA/CSS.

Em relação às suas funções, a NSA desempenha um papel essencial na coleta e análise de informações de sinais eletrônicos[36] (SIGINT). Com o avanço exponencial das tecnologias, o principal desafio da agência se concentra menos na coleta — pois os dados produzidos e disponíveis já são abundantes — e mais na transformação desses dados em informações valiosas (inteligência), que fornecem aos formuladores de políticas, tomadores de decisão e forças armadas dos Estados Unidos uma vantagem informacional em suas operações. No campo da cibersegurança, a missão da NSA/CSS é identificar e neutralizar ameaças aos sistemas de segurança nacional dos Estados Unidos, com foco especial na proteção da Base Industrial de Defesa (BID) e nos modernos sistemas de armas, cuja segurança é indispensável para a manutenção da superioridade militar do país.

Embora formalmente posicionada como uma agência de Segurança Nacional, a NSA transcende as atribuições conceituais tradicionais de um organismo de Segurança. Um exemplo claro dessa atuação são as denúncias de vigilância em massa feitas em 2013 por Edward Snowden, ex-funcionário da agência. Sob a justificativa de combate ao terrorismo e proteção à segurança nacional, a NSA realizava a vigilância de indivíduos, instituições e governos estrangeiros fora do território dos Estados Unidos (Greenwald, 2014).

Duas questões fundamentais emergem da análise da atuação da NSA. Primeiro, sua prática exemplifica a dificuldade — ou mesmo a dissolução — das fronteiras entre Segurança e Defesa, entre o interno e o externo. Didier Bigo (2001) analisa esse fenômeno por meio da metáfora da *Möbius strip*, uma faixa formada ao unir as extremidades de uma fita retangular após girá-la meia volta. Esse objeto, segundo a matemática, é não orientável, ou seja, não há uma distinção clara entre as partes "superior" e "inferior", o "interno" e o "externo".

De forma similar, a vigilância praticada pela NSA opera em um fluxo contínuo que conecta o interno e o externo de maneira inseparável. Esse processo manifesta-se em duas direções interligadas: (1) do interno para o externo, a NSA projeta seu

---

[36] Sobre os tipos de coleta de inteligência, três se destacam como mais relevantes: HUMINT, IMINT e SIGINT. A HUMINT é caracterizada pela inteligência obtida de fontes humanas; a IMINT, por imagens coletadas; e a SIGINT, pela interceptação de comunicações e sinais eletromagnéticos (Cepik, 2003).

poder para além das fronteiras nacionais, monitorando indivíduos, empresas e governos estrangeiros; e (2) do externo para o interno, essa vigilância retorna ao território doméstico, dado que os fluxos informacionais no ciberespaço transcendem fronteiras físicas (Bauman et al., 2014; Bigo, 2001).

O segundo ponto é que a atuação da NSA reforça que a geografia no ciberespaço ainda importa, e muito. Como bem pontuado por Deibert (2015), os fatores virtuais e imateriais do ciberespaço tornam fácil ignorar toda a tangibilidade que permite que ele exista. Infraestruturas Críticas, como cabos submarinos de fibra óptica, data centers e redes de transmissão, permanecem componentes essenciais para seu funcionamento. Entretanto, "onde a tecnologia está localizada é tão importante quanto o que ela é" (Deibert, 2015, p. 10, tradução nossa[37]).

As revelações de Snowden em 2013 expuseram como os Estados Unidos exploraram essa realidade geográfica a seu favor. Uma parcela significativa dos cabos submarinos de fibra óptica — responsáveis por cerca de 95% das comunicações globais de internet (U.S. Naval Institute, 2023) — atravessa o território norte-americano, e forneceu à NSA uma posição privilegiada para interceptar esses fluxos de dados. Isso evidencia que, embora o domínio cibernético seja amplamente caracterizado pela desterritorialização, o controle e a posse das infraestruturas físicas permanecem elementos fundamentais para a consolidação e a projeção de poder no ciberespaço.

2.2. O *Department of Homeland Security* (DHS)

O *Department of Homeland Security* (DHS) é um dos principais órgãos responsáveis por garantir a segurança nacional dos Estados Unidos frente a uma gama de ameaças, que vão desde terrorismo, tráfico de drogas e desastres naturais até ciberataques. Por incluir em seu escopo ameaças que incidem no ciberespaço, a compreensão do DHS torna-se essencial para alcançar os objetivos específicos propostos neste capítulo. Dessa forma, antes de detalhar as funções e responsabilidades do DHS, é importante entender a conjuntura histórica que permeou sua criação.

---

[37] No original: "*Where technology is located is as important as what it is"*

Antes de sua fundação, as atribuições e atividades do DHS estavam distribuídas entre 40 instituições federais responsáveis pela segurança interna (Hofmanová, 2019). Embora houvesse movimentos desde 1998 para a criação de um único organismo que lidasse com a segurança interna dos Estados Unidos, a formação do DHS só se concretizou após o atentado de 11 de setembro. Onze dias após o ocorrido, o então presidente dos Estados Unidos, George Bush (2001-2009), estabeleceu duas instituições: o *Office of Homeland Security* e o *Homeland Security Council*. Com o governador da Pennsylvania, Tom Ridge, como diretor, o novo gabinete tornou-se parte do executivo da presidência, com a missão de "[...] desenvolver e coordenar a implementação de uma estratégia nacional abrangente para proteger os Estados Unidos contra ameaças ou ataques terroristas" (Estados Unidos, 2001a p. 51812, tradução nossa[38]).

Em 9 de outubro de 2001, a administração Bush anunciou esforços adicionais na luta contra o terrorismo com a criação do *President's Critical Infrastructure Protection Board* (PCIPB). O PCIPB tinha como missão coordenar e supervisionar os esforços federais para a proteção de sistemas de informações essenciais, em conjunto com o *Office of Homeland Security*. O líder desse conselho, nomeado pelo presidente, também exerceria a função de Conselheiro Especial para a Segurança do Ciberespaço.

Em junho do ano seguinte, o presidente George Bush propôs a criação de um departamento permanente, o *Department of Homeland Security*, através da proposta legislativa *Homeland Security Act of* 2002 apresentada ao Congresso. Após todo o trâmite legislativo, o DHS foi formalmente estabelecido em 25 de novembro de 2002 (Borja, 2008; Hofmanová, 2019). Atualmente, o departamento conta com seis missões principais que delineiam seu plano estratégico: (I) Contraterrorismo e ameaças à segurança interna; (II) Proteção de fronteiras; (III) Segurança do ciberespaço e infraestruturas críticas; (IV) Proteção da economia; (V) Fortalecimento da preparação e resiliência; (VI) Fortalecimento do departamento.

É inquestionável, portanto, que o atentado de 11 de setembro redefiniu o paradigma de segurança dos Estados Unidos e foi decisivo para a criação do *Department of Homeland Security*. Ao posicionar o terrorismo transnacional como uma

---

[38] No original: "*to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."*

questão primordial de segurança, criou-se a necessidade da reconfiguração do aparato burocrático para responder a ameaças em um mundo globalizado (Mabee, 2007). Esta reconfiguração institucional materializou-se em um departamento voltado à proteção interna dos Estados Unidos em um contexto paradoxal: enquanto as fronteiras físicas demandam proteção reforçada, sua porosidade torna-se inevitável diante das exigências contemporâneas de livre circulação de bens, informações e pessoas.

A inclusão do ciberespaço nas missões do *Departament of Homeland Security* revela, portanto, um esforço de adaptação a essas novas dinâmicas globais. Primeiramente, essa inclusão demonstra que, mesmo antes de ser formalmente reconhecido como um domínio operacional pelos Estados Unidos, o ciberespaço já era percebido como um vetor potencial de ataques. Essa percepção remonta ao governo de Bill Clinton (1993-2001), quando eventos como o atentado de Oklahoma e a expansão comercial da Internet aproximaram as agendas de cibersegurança e proteção de Infraestruturas Críticas (Calvety, 2009). Ainda que os ataques de 11 de setembro tenham acelerado a reorganização institucional, a prioridade atribuída ao ciberespaço já havia sido estabelecida como uma pauta central da segurança nacional norte-americana.

Além disso, o enquadramento do ciberespaço no DHS reflete de forma clara as discussões apresentadas no primeiro capítulo, ao destacar o ciberespaço como um domínio complexo, marcado por extrema mutabilidade e por tensões inerentes entre a lógica territorial e a lógica liberalizante. Essas tensões resultam, sobretudo, da natureza desterritorializada do ciberespaço. As contradições tornam-se ainda mais explícitas ao analisar o conceito de *Homeland Security* — Segurança Interna — definido pelo *Homeland Security Act of 2002*. O documento reitera que *Homeland Security* se refere a medidas de proteção, detecção e resposta a ataques terroristas que ocorrem nos Estados Unidos e em seus territórios (Estados Unidos, 2002, s/p, tradução nossa).

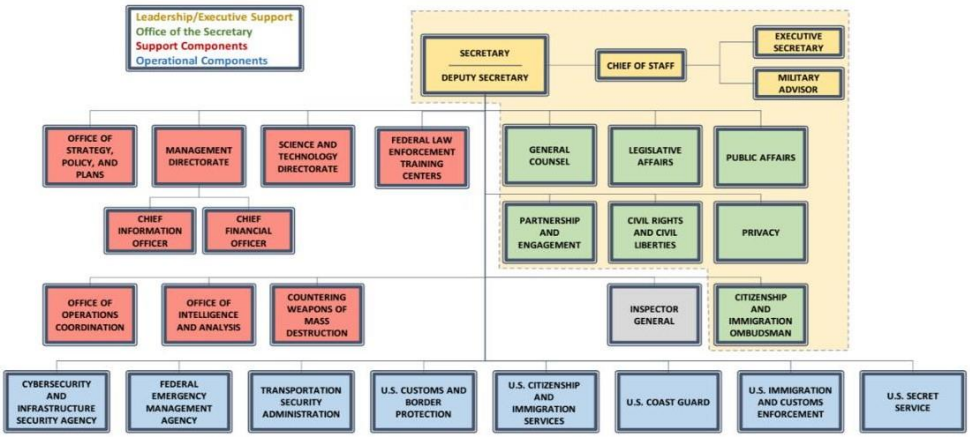
Por um lado, pode-se inferir que o *Departament of Homeland Security* se apoia na camada física do ciberespaço — as Infraestruturas Críticas — para adotar uma abordagem territorial clássica, com foco nos ativos tangíveis localizados dentro do território americano. Dessa forma, os Estados Unidos, por intermédio do DHS, seguem uma lógica westfaliana de território e soberania para assegurar a segurança nacional e, ao enquadrar o ciberespaço no âmbito do departamento responsável pela

segurança interna, buscam, em certa medida, nacionalizar o espaço cibernético. Por outro lado, as camadas semânticas e sintáticas, compostas por fluxos de dados, softwares, protocolos e informações, transcendem a lógica zonal, o que exige do departamento a adaptação de suas estratégias, mediante a consolidação de parcerias público-privadas e o fortalecimento da cooperação internacional.

Mais uma vez, o conceito de transversalidade, proposto por Daniel Ventre (2011), apresenta-se como uma ferramenta analítica relevante para compreender o enquadramento da cibersegurança no DHS. Integrada a áreas como a proteção da economia, das fronteiras e o combate ao terrorismo, a cibersegurança reflete não apenas a tensão entre as lógicas liberalizante e territorializante do ciberespaço, mas também evidencia a interconexão das ameaças cibernéticas com outras questões estratégicas da segurança nacional. Essa lógica fica clara nas missões do DHS, que reconhecem que as ameaças originadas no ciberespaço ou a ele vinculadas não podem ser dissociadas das demais áreas de interesse nacional.

Para exemplificar o raciocínio anterior, observa-se que as múltiplas missões do DHS dependem, em maior ou menor grau, do ciberespaço para serem realizadas de forma eficiente. No âmbito da missão de contraterrorismo e enfrentamento de ameaças à segurança interna, o ciberespaço desempenha um papel central, permitindo a identificação, a detecção e a prevenção de ataques terroristas. Isso ocorre porque, segundo o próprio departamento, além de ser utilizado como vetor de ataques, o espaço cibernético também pode ser instrumentalizado para disseminar propaganda, compartilhar material de treinamento e recrutar indivíduos dentro dos Estados Unidos (Department of Homeland Security, 2024). De maneira similar, a relevância do ciberespaço é igualmente evidente na missão de proteção de fronteiras, que cada vez mais exige sistemas robustos de vigilância e detecção para a triagem e identificação de potenciais suspeitos. Da mesma forma, a proteção da economia está diretamente vinculada à segurança dos sistemas financeiros, das Infraestruturas Críticas que sustentam as cadeias de suprimentos e da capacidade de resiliência frente aos crimes cibernéticos, os quais, em 2023, representaram um prejuízo de US$ 12,5 bilhões para os Estados Unidos (Federal Bureau of Investigation, 2023).

FIGURA 3 - ORGANOGRAMA DO DEPARTMENT OF HOMELAND SECURITY



Fonte: *Department of Homeland Security* (2023)

No que diz respeito a sua configuração interna, o *Department of Homeland Security* é organizado de forma integrada, com oito componentes operacionais, sete componentes de suporte e, no topo da hierarquia, o Secretário e o Secretário Adjunto, conforme apontado na Figura 2. Os componentes operacionais são responsáveis pela execução das atividades do departamento, enquanto os componentes de suporte formulam diretrizes sobre política, gestão, pesquisa, treinamento e inteligência, com o objetivo de facilitar as ações operacionais. Por fim, o Secretário coordena e supervisiona todas essas atividades.

2.2.1. A Cybersecurity and Infrastructure Security Agency (CISA)

No âmbito da cibersegurança, destaca-se o protagonismo da *Cybersecurity and Infrastructure Security Agency* (CISA). Até 2018, os esforços para a proteção do ciberespaço dos Estados Unidos estavam dispersos em diferentes frentes e não eram satisfatórios. O relatório *"DHS Needs to Better Address Its Cybersecurity Responsibilities"* do *Government Accountability Office* (GAO) de 2008 concluiu que, embora o DHS fosse essencial para a proteção de um agrupamento significativo das Infraestruturas Críticas, seus esforços não produziram nenhum plano substancial para lograr a proteção efetiva dessas infraestruturas (Government Accountability Office, 2008).

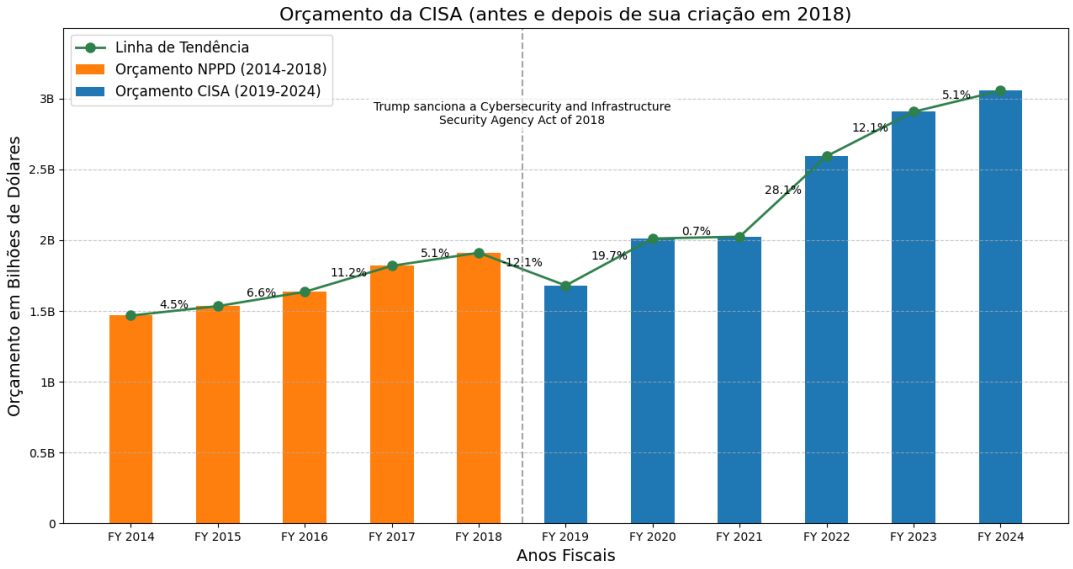
Além disso, o DHS ainda competia por capital político e econômico com duas outras agências já bem estabelecidas na cibersegurança: a *National Security Agency*

(NSA) e o *Federal Bureau of Investigation* (FBI). De acordo com Deppisch (2019), os líderes da NSA acreditavam cada vez mais que o DHS era incapaz de combater ameaças cibernéticas. Foi Kirstjen Nielsen, secretária do DHS nomeada por Donald Trump (2017-2021), que advogou por reformas mais expressivas na área de cibersegurança do departamento. Nielsen acreditava que o *National Protection and Programs Directorate* (NPPD) – antigo braço responsável pela cibersegurança no DHS — deveria ser transformado em uma agência operacional.

Com a promulgação do *Cybersecurity and Infrastructure Security Act of 2018*, o *National Protection and Programs Directorate* (NPPD) foi renomeado como Cybersecurity and Infrastructure Security Agency (CISA) e seu status foi elevado de diretoria para agência. Na prática, as atribuições da CISA permaneceram as mesmas do NPPD, mas, ao se tornar uma agência federal, a CISA se beneficiou de um maior orçamento e de maior autoridade para o estabelecimento de diretrizes (Cimpanu, 2018; Estados Unidos, 2018).

Atualmente, a CISA lidera os esforços de segurança cibernética federal e proteção de Infraestruturas Críticas nos Estados Unidos. A agência é composta por seis divisões principais: (1) a *Cybersecurity Division* (CSD), que lida com ameaças cibernéticas, desenvolve tecnologias de defesa e apoia práticas de segurança; (2) a *Infrastructure Security Division* (ISD), que trabalha com proprietários de infraestruturas críticas para reduzir riscos e aumentar a resiliência, além de atuar em áreas como educação e setor químico; (3) a *Emergency Communications Division* (ECD), que fornece recursos de comunicação interoperáveis e coordena padrões de comunicação de emergência; (4) o *National Risk Management Center* (NRMC), que analisa e mitiga riscos no setor público e privado e responde a incidentes; (5) a *Integrated Operations Division* (IOD), que unifica relatórios operacionais para melhorar o compartilhamento de informações; e (6) a *Stakeholder Engagement Division* (SED), que promove a colaboração e coordenação entre as partes interessadas.

FIGURA 4 - ORÇAMENTO DA CYBERSECURITY AND INFRASTRUCTURE AGENCY (2014-2024)



Fonte: Elaboração própria com base em (Estados Unidos 2021, 2022, 2023).

A Figura 3 apresenta o orçamento da CISA no período de 2014 a 2024 e destaca pontos relevantes. Primeiramente, observa-se que o NPPD, entidade predecessora da CISA, teve um aumento constante em seu orçamento entre 2014 e 2018. Contudo, após a promulgação do *Cybersecurity and Infrastructure Security Agency Act of 2018*, ocorreu uma redução significativa de 12,1% no orçamento do NPPD, o que marcou uma mudança nessa trajetória. Apesar de ampla investigação, não foram identificados elementos concretos que justificassem a redução de 12,1% no orçamento do NPPD. Ainda assim, pode-se especular que a transição do NPPD de uma diretoria para uma agência tenha demandado ajustes iniciais no orçamento.

No entanto, entre 2019 e 2020, o orçamento aumentou expressivamente em 19,7%, de US$ 1,6 bilhões para cerca de US$ 2 bilhões. Entre 2020 e 2021, o crescimento foi modesto, com um acréscimo de apenas 0,7%, o qual refletiu as restrições orçamentárias impostas pela pandemia de COVID-19. Em 2022, ocorreu uma expansão significativa, com um aumento de 28,1%, que elevou o orçamento para aproximadamente US$ 2,6 bilhões; esse aumento indica uma retomada do fluxo de recursos observado anteriormente e possivelmente represado em 2021. Para os anos fiscais de 2023 e 2024, os aumentos foram de 12,1% e 5,1%, respectivamente, o que conduziu o orçamento da CISA a cerca de US$ 3 bilhões.

Em partes, o crescimento orçamentário contínuo disponibilizado à CISA reflete o comprometimento do governo americano com a cibersegurança e a proteção de Infraestruturas Críticas. No entanto, ao analisar a porcentagem do orçamento do DHS destinada à CISA, percebe-se que ainda há uma baixa prioridade para a agência em relação às demais. Embora a CISA tenha visto aumentos significativos em seu orçamento, a proporção desses recursos no contexto total do DHS ainda é irrisória. Por exemplo, nos anos fiscais de 2019 a 2024 a porcentagem do orçamento do DHS destinada à CISA varia entre 2% e 3% (Estados Unidos, 2021, 2022, 2023).

Além de analisar o orçamento da CISA, é interessante comparar a proporção de recursos destinada a outras agências do DHS. Por exemplo, a *Federal Emergency Management Agency* (FEMA) e a *U.S. Customs and Border Protection* (USCBP) recebem, respectivamente, 31% e 18% do orçamento total do DHS. Isso demonstra que, embora o governo americano reconheça a importância e a urgência de investir em cibersegurança, outras demandas ainda recebem mais atenção. Por outro lado, o baixo investimento em cibersegurança poderia indicar que a área demanda menos recursos do que as demais. Mesmo sem números concretos, não é necessário esforço para compreender que a proteção de todas as fronteiras terrestres, portos e aeroportos dos EUA demandam consideravelmente mais pessoal do que aquele empregado na CISA. E que mesmo considerado um possível elevado valor dos hardwares e softwares utilizados pela CISA, esse não deve superar os dos modernos equipamentos.

2.2.2. O *U.S Secret Service* (USSS)

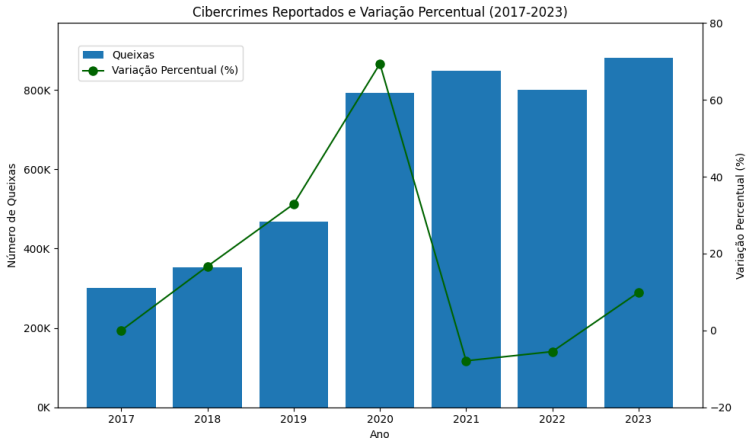
O Serviço Secreto dos Estados Unidos é uma das agências federais de aplicação da lei mais antigas. Criado em 1865, seu contexto de origem remete à Guerra Civil americana (1861-1865), quando cerca de um terço da moeda em circulação no país era falsificada. Diante desse cenário, o Serviço Secreto dos Estados Unidos foi estabelecido sob a égide do Departamento do Tesouro com o objetivo de garantir a estabilidade financeira do país através do combate à falsificação de moedas (United States Secret Service, 2024).

Com o passar dos anos, as atribuições do Serviço Secreto se expandiram. Em 2003, a agência deixou de fazer parte do Departamento do Tesouro para integrar o *Department of Homeland Security* (DHS). Atualmente, as principais áreas de atuação

do Serviço Secreto são os crimes financeiros, como a prevenção e investigação de delitos relacionados à moeda estadunidense, títulos do Tesouro e demais fraudes, bem como a proteção do Presidente, Vice-Presidente, familiares, ex-membros do governo federal, candidatos a eleições e chefes de Estado em visita (United States Secret Service, 2024).

À medida que o sistema financeiro se modernizou, as funções do Serviço Secreto se ampliaram para o ciberespaço. Já em 2004, o Serviço Secreto desenvolveu uma Cyber Investigative Section (CIS), considerada uma das primeiras unidades com foco exclusivo na aplicação da lei em crimes cibernéticos com teor financeiro. Assim como o FBI, o principal meio de atuação do Serviço Secreto é por meio de uma força-tarefa conjunta. Antes de 2020, o Serviço Secreto operava através de duas forças-tarefa distintas: a *Eletronic Crimes Task Forces* (ECTFs) e a *Financial Crimes Task Forces* (FCTFs). Entretanto, a realidade imposta pela pandemia da COVID-19 (SARS-CoV-2) catalisou mudanças na estratégia da agência.

FIGURA 5 - CIBERCRIMES REPORTADOS E VARIAÇÃO PERCENTUAL (2017-2023)



Fonte: Elaboração própria com base em (Internet Crime Complaint Center 2021; 2023)

O gráfico acima apresenta os crimes cibernéticos reportados ao *Internet Complaint Center* (IC3) de 2017 a 2023, e informa tanto o número absoluto de queixas quanto a variação percentual anual. Observa-se um aumento constante nos primeiros cinco anos. De 2017 a 2018, houve um crescimento de aproximadamente 16% nas denúncias. Entre 2018 e 2019, esse aumento saltou para 32%. Com o cenário da pandemia da COVID-19 em 2020, as denúncias dispararam, com um aumento de 69% em relação ao ano anterior. Após esse pico, o crescimento percentual desacelerou,

mas o número absoluto de queixas continuou a subir, e alcançou mais de 800.000 em 2023.

Compreende-se que a pandemia da COVID-19 acelerou uma tendência já em curso de adoção de tecnologias digitais, em virtude da necessidade de distanciamento social. Este cenário intensificou a operacionalização do ciberespaço tanto por parte da sociedade quanto pelo aparato administrativo estatal e privado. A necessidade de atendimentos remotos para diversas atividades cotidianas resultou em mudanças significativas: bancos priorizaram e automatizaram serviços digitais, lojas se adaptaram ao e-commerce e a própria educação migrou para o modelo *online* (LALLIE et al., 2021; MEDEIROS et al., 2020).

Simultaneamente à maior adoção de tecnologias digitais, observa-se o aumento dos crimes cibernéticos. A rápida expansão dos serviços digitais ofereceu aos criminosos a oportunidade de explorar essa nova vulnerabilidade. De acordo com David Warburton (2020), os ataques de *phishing* aumentaram em 220% em relação à média anual durante o pico da pandemia. Diante desse cenário, o Serviço Secreto integrou as duas forças-tarefa existentes na *Cyber Fraud Task Force* (CFTF). Em pronunciamento sobre a criação do CFTF, Michael D'Ambrosio, à época Diretor Assistente do Serviço Secreto, enfatizou que:

> à medida que a Nação continua a lidar com a onda de crimes cibernéticos associados à pandemia da COVID-19, os CFTFs liderarão o esforço para responsabilizar todos aqueles que buscam explorar este momento perigoso para seu próprio ganho ilícito (United States Secret Service, 2020, s/p).

Dessa forma, A CFTF atua a partir do trabalho conjunto com outras agências de investigação, setor privado e setor acadêmico para o combate ao cibercrime por meio da prevenção, detecção e mitigação de incidentes cibernéticos. Para alcançar seus objetivos, a CFTF treina os parceiros de aplicação da lei em nível estadual no *National Computer Forensics Institute* (NCFI) do Serviço Secreto, organiza reuniões periódicas para discutir tendências em mitigação, detecção, prevenção e cooperação entre as organizações, bem como produz boletins trimestrais sobre os crimes cibernéticos em evidência.

Tanto os crimes cibernéticos quanto os crimes contra o Sistema Financeiro norte-americano e sua moeda ultrapassam as fronteiras nacionais, o que reflete a dimensão global dessas ameaças. O próprio Serviço Secreto em sua missão, reconhece essa realidade ao afirmar: “Também protegemos a integridade de nossa

moeda e investigamos crimes contra o sistema financeiro dos EUA cometidos por criminosos ao redor do mundo e no ciberespaço" (United States Secret Service, 2024.2, s/p, tradução nossa[39]). Nesse contexto, embora a agência esteja subordinada ao DHS e seja caracterizada como um organismo de Segurança, suas funções extrapolam claramente os limites tradicionais dessa conceituação.

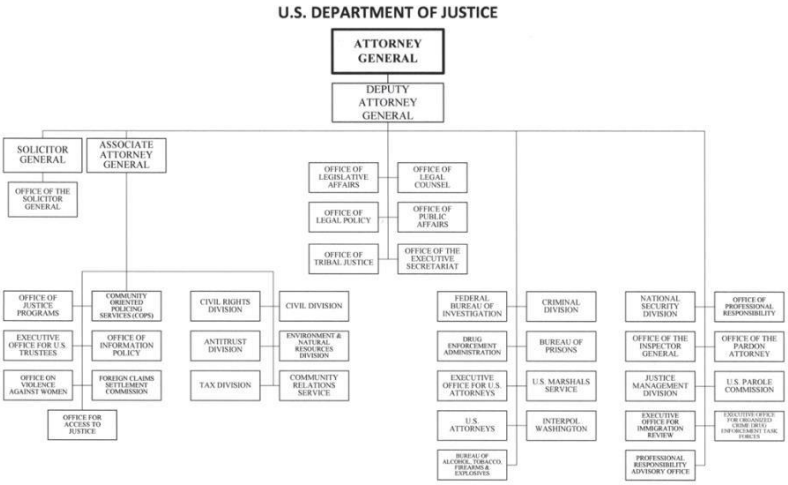
O papel do dólar como moeda fiduciária do Sistema Financeiro Internacional, amplamente utilizado em transações ao redor do mundo, faz com que crimes financeiros associados a ele transcendam as fronteiras nacionais, e demandam uma atuação transnacional por parte das autoridades competentes. Paralelamente, a responsabilidade de garantir a segurança física do presidente dos Estados Unidos não se limita ao território nacional, estendendo-se a viagens e eventos internacionais, o que reforça o caráter global das operações da agência. Assim, observa-se que a integridade da moeda e a proteção do chefe de Estado projetam a influência e a jurisdição dos Estados Unidos para além de suas fronteiras, consolidando a natureza transnacional das suas funções

2.3. O Department of Justice (DOJ) e o Federal Bureau of Investigation (FBI)

Como demonstrado até agora, os esforços necessários para garantir um grau adequado de cibersegurança nacional envolvem diversos departamentos e agências. Um componente crucial nesse esforço multissetorial é o *Department of Justice* (DOJ). Como missão, o DOJ é encarregado de fazer cumprir a lei e defender os interesses nacionais, portanto, o combate a crimes cibernéticos e a garantia da cibersegurança estão incluídos no escopo dessa missão.

[39] No original: *"We also protect the integrity of our currency and investigate crimes against the U.S. financial system committed by criminals around the world and in cyberspace."*

FIGURA 6 - ORGANOGRAMA DO DEPARTMENT OF JUSTICE



Fonte: Department of Justice (2023)

Dentre todos os escritórios e agências que compõem a estrutura do DOJ (ver figura 6), dois componentes se destacam no que diz respeito a crimes cibernéticos e à cibersegurança: o *Federal Bureau of Investigation* (FBI) e a *Criminal Division* (CRM). É importante destacar que, embora o FBI e a CRM sejam proeminentes, não são os únicos a atuar na área cibernética. A *Civil Division* (CIV), a *Community Oriented Policing Services* (COPS) e a *Justice Management Division* (JMD), por exemplo, também desempenham papéis essenciais no plano estratégico do DOJ para o ciberespaço.

No que concerne ao FBI, este cumpre um papel dual, pois atua simultaneamente como membro pleno da Comunidade de Inteligência dos Estados Unidos e como principal braço investigativo do DOJ. Além de investigar os crimes de sua competência, o FBI fornece a outras agências serviços de inteligência e aplicação da lei, tais como identificação de impressões digitais e exames laboratoriais, os quais dão suporte tanto às investigações do próprio FBI quanto às de entidades parceiras (Federal Bureau of Investigation, 2024a).

Em relação à cibersegurança, a estratégia do FBI alinha-se às preocupações do ex-general Paul Nakasone e tem como objetivo alterar o cálculo de custo-benefício das operações cibernéticas mediante a imposição de riscos e consequências aos perpetradores de crimes cibernéticos. A estratégia cibernética do FBI reconhece que os esforços unilaterais são insuficientes para combater ameaças cibernéticas. Além

disso, propõe que as ações do escritório devem ser sequenciadas com as de entidades parceiras para maximizar a eficácia dos esforços conjuntos.

As operações sincronizadas são coordenadas pela *National Cyber Investigative Joint Task Force* (NCIJTF), uma força-tarefa da Comunidade de Inteligência liderada pelo FBI. A NCIJTF tem como missão integrar, coordenar e compartilhar informações relacionadas a todas as investigações domésticas de ameaças cibernéticas. Para esse fim, a força-tarefa conta com a estreita colaboração de trinta agências, entre as quais estão a *Central Intelligence Agency* (CIA), o DOD, o DHS e a NSA (Kraft; Marks, 2012).

O primeiro ponto relevante sobre a atuação do FBI como organismo de Segurança é a referência a “ameaças cibernéticas domésticas”, que revela a questão conceitual da dicotomia entre o interno e o externo, ou entre o doméstico e o internacional, no contexto do ciberespaço. Embora o FBI seja amplamente definido como uma organização de segurança nacional voltada para inteligência e aplicação da lei, com atuação tradicionalmente restrita ao território dos Estados Unidos, o caráter desterritorializado do ciberespaço desafia essas delimitações.

Essa complexidade conceitual não impede que o FBI adote estratégias concretas para lidar com as ameaças cibernéticas. Nesse sentido, a agência definiu cinco pilares fundamentais no escopo de suas atividades. O primeiro pilar consiste na presença de *cyber squads* altamente treinados nos 56 escritórios do FBI distribuídos pelo território norte-americano. Essas equipes operam em conjunto com outras forças-tarefa, integrando esforços de agências parceiras para fortalecer a resposta contra crimes cibernéticos. Aqui, observa-se uma atuação, até então, doméstica e coerente com a missão do FBI como organismo de Segurança.

O segundo pilar, no entanto, já introduz um elemento que desafia as delimitações conceituais de Segurança e Defesa. O FBI estabelece a existência de *Cyber Action Teams* (CATs), grupos especializados com capacidade de mobilização em escala nacional e internacional. Conforme o próprio FBI destaca, os CATs podem ser deslocados globalmente em questão de horas para responder a grandes incidentes cibernéticos: “O Cyber Action Team [...] pode ser mobilizado em todo o mundo em questão de horas para responder a grandes ameaças e ataques

cibernéticos [...]" (Federal Bureau of Investigation, 2023b, tradução nossa[40]). Essa atuação internacional do FBI revela uma extrapolação de suas atribuições como um organismo tradicionalmente de Segurança.

O terceiro pilar envolve os *Cyber Assistant Legal Attachés*, oficiais especializados em questões cibernéticas que atuam em embaixadas dos Estados Unidos ao redor do mundo. A presença desses profissionais em território estrangeiro fortalece a cooperação internacional e facilita a resolução de crimes cibernéticos que frequentemente atravessam múltiplas jurisdições. Aqui, mais uma vez, o FBI extrapola o que se compreende tradicionalmente por um organismo de Segurança e reflete a dificuldade de se estabelecer claramente atribuições de Segurança e Defesa quando se trata do ciberespaço e crimes cibernéticos.

O quarto pilar refere-se à administração do *Internet Crime Complaint Center* (IC3), que funciona como o centro de denúncias de crimes cibernéticos. Esse ponto permanece condizente com as atribuições de um organismo de Segurança, em vista que o foco se dá na coleta e processamento de informações sobre crimes cibernéticos ocorridos em território norte-americano. Por fim, o quinto aspecto é o *CyWatch*, que desempenha o papel de centro de operações e suporte 24 horas para rastrear incidentes e comunicar-se com os escritórios ao redor do país (Federal Bureau of Investigation, 2024b).

No que concerne à *Criminal Division* (CRM), a divisão tem a responsabilidade de elaborar, aplicar e supervisionar a aplicação das leis federais de sua competência. Em 1996, foi criada dentro da CRM a *Computer Crime and Intellectual Property Section* (CCIPS), cujo objetivo principal é combater o crime cibernético e a violação de propriedade intelectual. Sua criação surge em um contexto de expansão das Tecnologias de Informação e Comunicação (TICs) e da privatização e comercialização da Internet em 1995 (Naughton, 2016). Esses dois fatores — a ampliação do acesso à internet e a crescente popularização dos computadores pessoais — estabeleceram um terreno fértil para o surgimento e a disseminação dos crimes cibernéticos.

Nesse cenário, o CCIPS: (I) conduz e apoia investigações e processos judiciais; (II) orienta investigadores e promotores quanto às melhores práticas de coleta de evidências eletrônicas; (III) fornece apoio jurídico e técnico especializado ao DOJ, a

---

[40] No original: *"the Cyber Action Team [...] can deploy across the globe within hours to respond to major cyber threats and attacks […]"*

agências investigativas e outras entidades parceiras; (IV) promove políticas internacionais que favoreçam a aplicação das leis de crimes cibernéticos e de propriedade intelectual; (V) realiza análises investigativas; entre outras atividades (Department of Justice, 2024a).

Como uma expansão dos esforços iniciados em 1996, a CRM criou, em dezembro de 2014, dentro do CCIPS, a *Cybersecurity Unit*. Essa unidade de cibersegurança surgiu com o propósito de atuar como um centro de aconselhamento jurídico e técnico no que diz respeito aos estatutos de vigilância eletrônica e de crimes cibernéticos. Seu objetivo é aplicar ou adaptar esses estatutos para combater os crimes cibernéticos de forma eficiente, sem comprometer a privacidade do usuário. A unidade de cibersegurança oferece suporte e orientação às autoridades de aplicação da lei dos Estados Unidos e de países aliados para conduzir investigações cibernéticas no limite da legalidade. Dessa forma, contribui para o aprimoramento das legislações relacionadas à segurança cibernética, com foco na proteção das redes e das vítimas individuais. Além disso, considerando a necessidade de esforços multissetoriais, a unidade promove boas práticas de segurança digital no setor privado (Department of Justice, 2024b).

Em síntese, a partir da análise da atuação do FBI percebe-se que os Estados Unidos, por meio desse organismo, buscam moldar a governança do ciberespaço de acordo com seus interesses nacionais. A promoção de políticas internacionais para favorecer a aplicação de leis sobre crimes cibernéticos expande a atuação do FBI como um organismo de Segurança e, portanto, pode ser interpretada como uma oportunidade estratégica enxergada para projetar a soberania e expandir a jurisdição dos Estados Unidos além de suas fronteiras nacionais (Israel, 2020).

2.4. Office of National Cyber Director

A criação do *Office of National Cyber Director* (ONCD) foi proposta pela *Cyberspace Solarium Commission* (CSC), uma comissão estabelecida pela *National Defense Authorization Act* (NDAA) para o ano fiscal de 2019. Essa comissão, de caráter bipartidário e bicameral, tem como objetivo desenvolver um consenso estratégico para a defesa dos Estados Unidos no ciberespaço contra ataques cibernéticos significativos (Cyberspace Solarium Commission, 2024).

Em março de 2020, a comissão elaborou um extenso relatório aberto de quase 200 páginas. O prognóstico do cenário americano, descrito no documento, não difere do que já foi explicitado na presente dissertação: observa-se uma crescente dependência da sociedade moderna em relação às tecnologias, que constituem uma vulnerabilidade significativa devido ao risco de interrupções em setores vitais. Com base nessas constatações, o relatório apresenta inúmeras recomendações, divididas em seis pilares: (I) reformar a estrutura organizacional dos Estados Unidos para o ciberespaço; (II) fortalecer normas e ferramentas não-militares; (III) promover resiliência em âmbito nacional; (IV) remodelar o ecossistema cibernético; (V) operacionalizar a cooperação em cibersegurança com o setor privado; e (VI) preservar e empregar o instrumento militar do poder nacional. No que concerne as reformas na estrutura organizacional dos Estados Unidos, o relatório recomendou o estabelecimento de um *National Cyber Director* (NCD).

O apelo às mudanças institucionais ganhou força em 2021 devido ao grande ataque cibernético à *SolarWinds*, uma fabricante americana de softwares. De acordo com os últimos relatórios da FireEye, o ataque teve como autoria o grupo APT29 (ou Cozy Bear), considerado pelos Estados Unidos um advanced persistent threat actor (APT) ligado ao *Foreign Intelligence Service* (SVR) russo (FireEye, 2020). O grupo conseguiu se infiltrar na *SolarWinds* e inserir um *backdoor*[41] em uma atualização futura do software *SolarWinds Orion*, uma plataforma de gerenciamento e monitoramento de redes. Pelo fato de a empresa ter uma grande amplitude de mercado, estima-se que cerca de 18.000 clientes foram afetados pelo *malware SUNBURST* quando o software foi atualizado. Dentre os afetados estão o Departamento de Estado, de *Homeland Security*, do Comércio e do Tesouro dos Estados Unidos (Barrett, 2020).

Tomadas as proporções do ataque, a iniciativa de um *National Cyber Director,* advogada não somente pela comissão, ganhou a força necessária para deixar de ser apenas uma recomendação e se concretizar na materialidade. A partir do *National*

[41] Backdoor, do inglês "porta dos fundos", refere-se a um método de acesso a um sistema computacional que contorna os mecanismos de autenticação e segurança padrões. Embora possa ser implementado intencionalmente por desenvolvedores para fins de manutenção remota, o backdoor apresenta riscos significativos à segurança. Atores maliciosos podem explorar essa vulnerabilidade para obter acesso não autorizado, extrair informações sensíveis ou comprometer a integridade do sistema sem deixar rastros detectáveis.

Defense Authorization Act (NDAA) para o ano fiscal de 2021, o *Office of The National Cyber Director* (ONCD) foi formalmente criado. No geral, algumas funções do NCD são: (I) Conselheiro do presidente: O NCD tem o papel de principal conselheiro da presidência sobre a implementação de políticas e estratégias cibernéticas; (II) Aconselhar a Casa Branca e as agências governamentais, como o *National Security Council* (NSC), *o Homeland Security Council* (HSC) e as demais agências e departamentos; (III) Liderar a implementação das políticas e estratégias cibernéticas em âmbito nacional, ou seja, avaliar o desempenho das agências, seu orçamento e, com base nisso, recomendar mudanças na organização; (IV) Preparar planos de resposta do governo federal a ataques cibernéticos; (V) Liderar resposta coordenada a ataques cibernéticos; (VI) Liderar o relacionamento com o setor privado e parceiros internacionais (Costello; Montgomery, 2021).

O primeiro a ocupar o cargo de *National Cyber Director* dos Estados Unidos foi Chris Inglis. Inglis apresenta qualificações acadêmicas relevantes para o cargo, evidenciadas por seus mestrados em Ciência da Computação pela Universidade Johns Hopkins e em Engenharia Mecânica pela Universidade de Columbia. Sua extensa experiência profissional no setor de inteligência, que totaliza 41 anos, inclui 28 anos de serviço na *National Security Agency* (NSA), onde atuou em diversas funções, entre elas a de Diretor Adjunto por sete anos e meio.

As declarações de Inglis evidenciam o impacto significativo do ataque à *SolarWinds* nos objetivos de sua gestão como NCD. Ele identifica as vulnerabilidades na cadeia de suprimento de *softwares* como uma das três categorias de ameaças sistêmicas globalmente difundidas que requerem atenção constante. Consequentemente, sua gestão concentrou-se em quatro objetivos principais: (I) Promover a coerência entre as agências federais, assegurando recursos, desenvolvimento de padrões, diretrizes e prioridades comuns; (II) Aprimorar continuamente a colaboração público-privada em cibersegurança; (III) Avaliar o desempenho dos recursos investidos e aconselhar os departamentos e agências sobre atualizações e mudanças alinhadas às prioridades da administração; e (IV) Aumentar a resiliência da tecnologia atual e futura no ecossistema digital americano (Inglis, 2021).

Chris Inglis deixou o cargo em fevereiro de 2023, após quase dois anos de atuação. Fontes indicam que sua renúncia ocorreu devido a divergências com Anne Neuberger, Conselheira adjunta de segurança nacional dos Estados Unidos desde

2021 (Turton; Mason, 2023). Em dezembro de 2023, Harry Coker Jr foi confirmado pelo Senado como o segundo NCD. Coker apresenta um perfil similar ao de Inglis, com extensa experiência na comunidade de inteligência. Sua trajetória inclui 17 anos de serviço na *Central Intelligence Agency* e o cargo de diretor executivo da NSA de 2017 a 2019.

De certa forma, é possível identificar uma continuidade entre a gestão de Coker e a de Inglis, tanto em termos de objetivos quanto de desafios, que não se alteraram substancialmente nesse período. Para Coker, a coerência federal é uma das principais prioridades da sua administração. Contudo, um dos maiores desafios é a questão da responsabilização legal por ataques cibernéticos, que deve ser transferida para os fabricantes de software, um tema que já estava em discussão na gestão de Inglis (Starks, 2024).

Em suma, a análise evidencia que a atuação do ONCD está alinhada ao papel esperado de um organismo responsável por assessorar o presidente dos Estados Unidos em assuntos de Segurança Cibernética. Entretanto, destaca-se o fato de o ONCD assumir a liderança na resposta a incidentes cibernéticos, ainda que nenhuma menção explícita a ações ofensivas esteja presente em suas atribuições.

2.5. Reflexões sobre a estrutura Organizacional de Cibersegurança dos EUA

A análise da estrutura organizacional de cibersegurança dos Estados Unidos apresentada neste capítulo não pretendeu ser exaustiva em relação a cada componente do vasto *cosmos* necessário para garantir, ou ao menos tentar garantir, a cibersegurança nacional. Devido às limitações espaciais e temporais, o objetivo foi elucidar os principais atores e suas funções dentro desse complexo sistema e extrair considerações pertinentes para o presente estudo.

Em primeira análise, observou-se uma questão central que permeia de modo geral todas as agências: a generalidade das descrições de suas funções. Em grande parte dos documentos e descrições disponíveis em seus respectivos sites, as atribuições das agências são apresentadas de maneira ampla e genérica. Devido à utilização de um mesmo vocabulário — isto é: "garantir a resiliência", "apoio a operações", "parceria público-privada" — estas acabam por se confundir. A ausência de documentos ou fontes abertas sobre as competências de cada órgão sugere a existência de uma "caixa preta" sobre como essas agências de fato atuam na prática.

De certo modo, justifica-se a amplitude e generalidade existentes. Visto que a cibersegurança é um tema sensível, no qual os Estados Unidos enfrentam ameaças cotidianas, a divulgação mais detalhada do funcionamento de cada agência poderia aumentar as vulnerabilidades, ao fornecer aos adversários a vantagem do conhecimento operacional de cada departamento. Em contrapartida, essa abordagem dificulta a realização de pesquisas acadêmicas sobre o tema.

A falta de clareza sobre o funcionamento das agências não afeta apenas a compreensão externa, mas também levanta questões sobre a eficiência interna dessas instituições. A renúncia do primeiro National Cyber Director ocorreu justamente pela ausência de compartilhamento de informações entre as agências, o que dificultava a execução das atividades do seu escritório. Além disso, a falta de distinção entre funções, ao menos nos documentos, sugere uma duplicidade de esforços e uma ineficiência operacional nessa estrutura organizacional.

O aumento das ameaças e a crescente complexidade do ciberespaço intensificam a urgência de uma reestruturação organizacional, necessária para melhorar a coordenação entre as agências. Essa necessidade ficou evidente após o ataque à SolarWinds em 2020 e a subsequente criação do *Office of National Cyber Director*, em 2021. Embora haja um foco significativo na coerência federal para alcançar objetivos comuns, o papel crucial do setor privado adiciona camadas de complexidade. Como exposto no primeiro capítulo, grande parte das Infraestruturas Críticas dos Estados Unidos é operada por entidades privadas, o que impõe desafios complexos no alinhamento de objetivos, no compartilhamento de informações e na criação de padrões de segurança comuns. Apesar dos esforços e das estratégias para superar esses obstáculos, a legislação vigente ainda não exige a adoção de determinados mecanismos.

Nesse sentido, apesar da complexidade da estrutura organizacional dos EUA e da multiplicidade de atores envolvidos, há desafios significativos relacionados ao escopo de suas atuações. Embora compreensível, a falta de transparência dificulta a análise crítica e a avaliação do funcionamento dessas organizações. A criação do *Office of National Cyber Director* representa uma tentativa clara de trazer coerência aos esforços dispersos dessas agências, que frequentemente apresentam sobreposição de funções e competem por capital político. No entanto, resta observar se, após um primeiro mandato marcado por dificuldades, o escritório conseguirá cumprir esse objetivo.

De forma geral, observa-se nos órgãos analisados uma sobreposição de atribuições de Segurança e Defesa, em alguns casos mais evidente do que em outros. Isso ocorre porque, como destacado no início do capítulo, a natureza desterritorial do ciberespaço dificulta a aplicação precisa desses conceitos. Mais especificamente, verifica-se que o DoD, por meio do USCYBERCOM, adota uma postura que busca territorializar o ciberespaço, fundamentada nos conceitos de *Defend Forward* e *Persistent Engagement*. Além disso, sua atuação não se restringe a questões de defesa, estendendo-se a problemas tradicionalmente associados à segurança, como o engajamento na segurança eleitoral. A NSA, por compartilhar o mesmo comandante com o USCYBERCOM, reflete essa mesma ambiguidade. Embora formalmente definida como uma agência de segurança, suas operações estendem a soberania dos Estados Unidos para fora das fronteiras nacionais.

No que concerne ao DHS, embora o departamento, com seu foco voltado para ameaças à segurança interna, territorialize o ciberespaço ao incorporá-lo em sua missão, evidencia que este domínio se tornou central para compreender as dinâmicas contemporâneas entre segurança e defesa no século XXI. Ademais, ainda que o Serviço Secreto esteja subordinado ao DHS, configurando-o como um organismo de Segurança, sua atuação exige parcerias e presença internacional, tanto para enfrentar crimes cibernéticos quanto para garantir a proteção física do Presidente em contextos globais. De maneira similar, o FBI, também um organismo tipicamente de Segurança, necessita de parcerias internacionais para investigar os crimes cibernéticos que atravessam múltiplas jurisdições.

Isto posto, a análise do complexo organizacional de cibersegurança dos Estados Unidos evidencia a tensão constante entre as lógicas territorializantes e liberais que permeiam as suas atribuições no ciberespaço. No próximo capítulo, essa dinâmica será aprofundada por meio da análise de conteúdo das estratégias de cibersegurança desenvolvidas ao longo das administrações presidenciais recentes

3. As Estratégias de Cibersegurança dos EUA: Tensão entre discurso liberal e territorializante

Após apresentar a base teórico-conceitual do ciberespaço no primeiro capítulo e mapear o complexo organizacional de cibersegurança dos Estados Unidos no segundo, este terceiro capítulo concentra-se em examinar as abordagens adotadas pelos governos norte-americanos no século XXI para a cibersegurança e a proteção de Infraestruturas Críticas. Este esforço é essencial para responder à questão central desta pesquisa: como as políticas de cibersegurança dos Estados Unidos refletem a tensão entre abordagens territorializantes e liberais do ciberespaço?

Como destacado no capítulo dois, especialmente na seção sobre o Department of Homeland Security (DHS), o governo norte-americano já considerava, mesmo antes dos ataques de 11 de setembro, a possibilidade de que organizações terroristas utilizassem o ciberespaço de forma geral — e a Internet, em particular — para causar danos às instituições e às Infraestruturas Críticas do país (Cepik; Canabarro; Borne, 2014).

A administração de Bill Clinton (1993-2001), ao estabelecer a President's Commission on Critical Infrastructure Protection (PCCIP), já reconhecia que a principal causa das vulnerabilidades nas Infraestruturas Críticas era a existência de interdependências não controladas entre diferentes ativos dessas infraestruturas. Essas interdependências eram mediadas pelo ciberespaço, cuja evolução tecnológica acelerada resultou em uma crescente dependência mútua entre os componentes das Infraestruturas Críticas (Harašta, 2018).

As preocupações com possíveis ataques cibernéticos a Infraestruturas Críticas norte-americanas já eram evidentes na década de 1990. *A National Security Strategy for a New Century* (Estados Unidos, 1999, p. 2, tradução nossa) destacava: (Estados Unidos, 1999, p. 2, tradução nossa[42]):

> Também enfrentamos ameaças às infraestruturas nacionais essenciais, que cada vez mais podem assumir a forma de um ataque cibernético, além de um ataque físico ou sabotagem, e podem ter origem em grupos terroristas ou criminosos, bem como em Estados hostis.

[42]No original: *"We also face threats to critical national infrastructures, which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage and could originate from terrorist or criminal groups as well as hostile states."*

Embora essas preocupações já estivessem presentes nos anos 1990, impulsionadas pelo aumento do terrorismo doméstico e pela crescente digitalização das Infraestruturas Críticas, os atentados de 11 de setembro de 2001 atuaram como um catalisador. Esse evento acelerou a sobreposição das agendas de cibersegurança, combate ao terrorismo e proteção de Infraestruturas Críticas, resultando na sua integração de forma institucionalizada. A partir de então, essas questões passaram a ocupar um papel central nas estratégias de segurança nacional dos Estados Unidos.

3.1. O governo Bush (2001-2009): A Institucionalização da Vigilância em massa

De forma evidente, a agenda de segurança nacional dos Estados Unidos, após os atentados de 11 de setembro, direcionou quase todos os seus esforços para o combate ao terrorismo. Questões relacionadas ao ciberespaço, por exemplo, estão ausentes *na National Security Strategy of The United States of America* (Estados Unidos, 2002). No entanto, a crescente disseminação da Internet, impulsionada por sua privatização e posterior comercialização na década de 1990, tornou inevitável a inclusão do ciberespaço como um ponto importante na agenda de segurança nacional.

Conforme já destacado no primeiro capítulo, Internet e ciberespaço não são sinônimos, embora estejam intimamente conectados. A Internet (e, particularmente, a *World Wide Web*) desempenhou um papel fundamental ao facilitar a inserção da sociedade no ciberespaço. Segundo dados do *U.S. Census Bureau*, em 2003, 54,7% das residências nos Estados Unidos possuíam acesso à Internet, e 61,8% contavam com um computador (Department of Commerce, 2005). Diante desse cenário, o governo norte-americano formulou, em 2003, uma estratégia específica para o ciberespaço: a *National Strategy to Secure Cyberspace* (NSSC) (Estados Unidos, 2003).

Um ponto importante a destacar dessa estratégia é a constante caracterização do ciberespaço como um domínio pertencente e operado pela população e instituições estadunidenses. O documento afirma que “O objetivo deste documento é envolver e capacitar os americanos a proteger as partes do ciberespaço que eles possuem,

operam, controlam ou com as quais interagem" (Estados Unidos, 2003, p. vii, tradução nossa[43]).

Essa afirmação revela uma clara tentativa de delimitar um ciberespaço estadunidense. Embora, por um lado, existam discursos que reconheçam o ciberespaço como um "bem comum" global, a NSSC sugere, por outro, que partes desse domínio podem ser submetidas à jurisdição e ao controle dos Estados Unidos. Isso expõe um paradoxo significativo: enquanto a natureza do ciberespaço é, por definição, desterritorializada devido aos fluxos do espectro eletromagnético, a materialidade de suas infraestruturas críticas — controladas e operadas pelos Estados — permite que esse espaço seja fragmentado e inserido em uma lógica westfaliana de soberania e jurisdição nacional.

No que concerne à relação entre o ciberespaço e as Infraestruturas Críticas, a NSSC reconhece a forte dependência dessas infraestruturas em relação ao ciberespaço e o define como o "sistema nervoso" que as sustenta. Conforme discutido no capítulo 1, o uso de metáforas e analogias na concepção do ciberespaço não é neutro, uma vez que influencia diretamente a formulação de políticas e estratégias voltadas à sua proteção (Cavelty, 2013). A metáfora do "sistema nervoso" não é apenas ilustrativa, mas também estratégica, pois implica que qualquer ataque cibernético pode desestabilizar setores críticos do Estado. Nesse sentido, a NSSC não apenas enfatiza a simbiose entre o ciberespaço e as Infraestruturas Críticas, mas também legitima a necessidade de uma abordagem territorializante, na qual a proteção do ciberespaço se torna imperativa e se justifica pela centralidade desse domínio para o funcionamento da economia, da segurança e da defesa nacional.

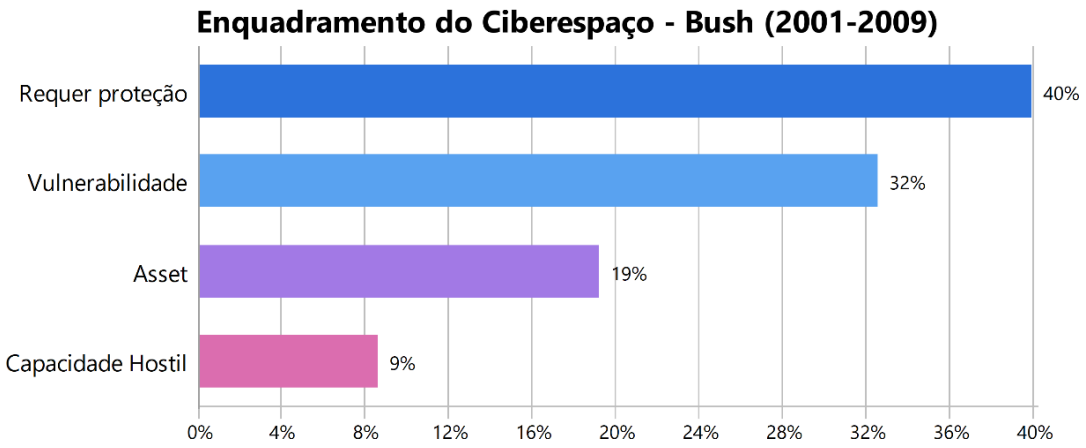
Essa lógica de territorialização do ciberespaço se materializa na criação do *Department of Homeland Security* em 2002 e reflete a institucionalização da agenda de cibersegurança dentro da estrutura de segurança nacional dos Estados Unidos. O departamento ganha destaque no documento devido à sua recente inauguração e ao papel central que lhe é atribuído na proteção das Infraestruturas Críticas. De acordo com a NSSC, cabe ao departamento elaborar um plano nacional para a segurança das Infraestruturas Críticas, coordenar respostas a incidentes com o setor privado,

[43] No original: "*The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact"*

bem como estabelecer, em parceria com outras entidades governamentais, diretrizes para a adoção de melhores práticas, dentre outras responsabilidades.

A Figura 7 evidencia que, durante o governo Bush, das 434 categorizações totais, 173 segmentos apresentaram o enquadramento 'requer proteção', o que corresponde a 40% das unidades de contexto analisadas. Nota-se, desde já, que essa ênfase na necessidade de proteção e nas medidas voltadas à segurança do ciberespaço mantém-se constante ao longo dos diferentes governos.

FIGURA 7 - CATEGORIA ENQUADRAMENTO – GOVERNO BUSH (2001-2009)



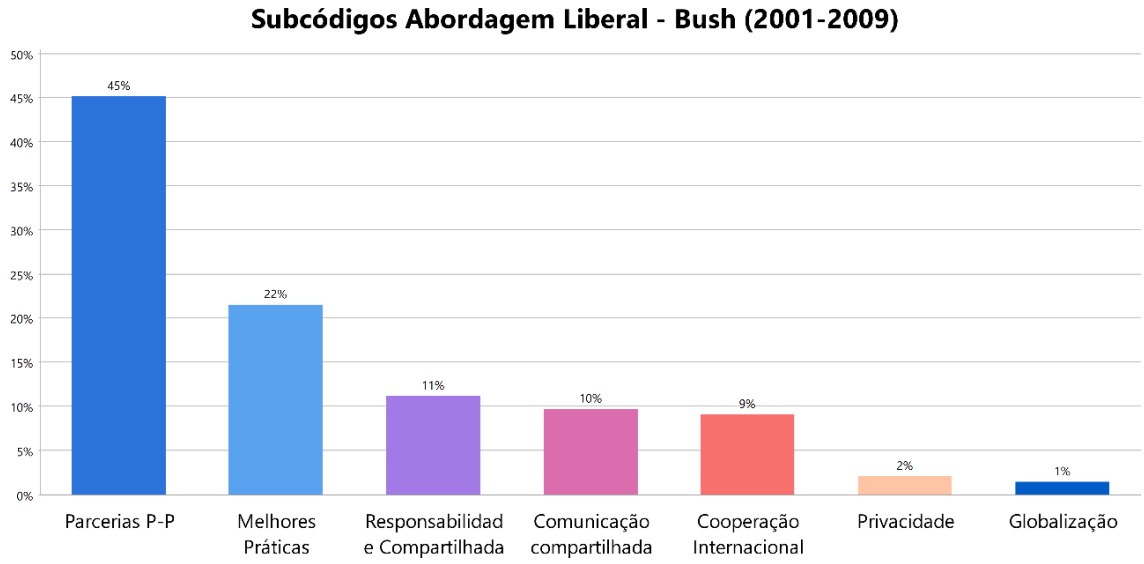
Fonte: Elaboração própria

Além disso, 32% das Unidades de Contexto analisadas enquadram o ciberespaço como uma vulnerabilidade dos Estados Unidos. Esse dado reflete o reconhecimento, por parte do governo Bush, de que o ciberespaço, embora seja considerado um asset estratégico (19%), também representa um ponto de fragilidade suscetível à exploração por atores maliciosos. Contudo, a segurança desse domínio não é simples. O documento destaca: “A segurança do espaço cibernético é um desafio estratégico difícil que exige um esforço coordenado e concentrado de toda a nossa sociedade - o governo federal, os governos estaduais e municipais, o setor privado e o povo americano” (Estados Unidos, 2003, p.vii, tradução nossa[44]).

[44]No original: Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.

Nesse sentido, embora exista essa tentativa de fragmentação entre um ciberespaço dito “americano” e o ciberespaço global, há o reconhecimento pelo Governo Bush que esse domínio é amplamente operado pelo setor privado. Como ilustra a Figura 8. De 144 segmentos codificados, as parcerias público-privadas configuram 65 delas, o que corresponde a 45% das Unidades de Contexto analisadas.

FIGURA 8 - ABORDAGEM LIBERAL – BUSH (2001-2009)



Fonte: elaboração própria

Observa-se que, devido à maior parte das Infraestruturas Críticas estar sob a responsabilidade do setor privado, o governo Bush adotou um discurso oficial que atribui ao setor privado o papel de linha de frente na proteção do ciberespaço, enquanto o governo federal atua apenas em situações de crises ou emergências nacionais. Nesse contexto, os documentos do período enfatizam significativamente as melhores práticas (22%) que o setor privado pode implementar para aumentar a resiliência das Infraestruturas Críticas.

Adicionalmente, os documentos destacam a ideia de responsabilidade compartilhada (11%) como um pilar central da estratégia de cibersegurança, com a inclusão direta do cidadão americano na proteção do ciberespaço. De acordo com a NSSC, o objetivo ao desenvolver essa estratégia era não apenas alertar a população sobre a relevância da agenda, mas também: “produzir uma estratégia na qual muitos americanos pudessem sentir que tinham um papel direto no desenvolvimento e com a qual se comprometeriam.” (Estados Unidos, 2003, p.2, tradução nossa). Nessa estratégia, o *Department of Homeland Security* possui papel central na elaboração de

programas para a conscientização da população, com o objetivo de capacitá-los na proteção do ciberespaço.

Embora o discurso oficial dos Estados Unidos sobre o ciberespaço enfatize a noção de 'responsabilidade compartilhada', suas estratégias refletem uma continuidade histórica enraizada no mito do Destino Manifesto e na Doutrina Monroe. Conforme destacam Machado e Simionato (2015), desde a formação do país como Estado-nação, a grande estratégia americana tem sido moldada, de forma central, por essas concepções ideológicas.

O mito do Destino Manifesto baseia-se em uma visão messiânica que atribui aos Estados Unidos a missão providencial de defender e disseminar os valores de liberdade e democracia. Essa narrativa, que inicialmente justificou a expansão territorial rumo ao Oeste no século XIX, consolidou-se como um 'Destino Manifesto Global', especialmente durante a Guerra Fria, quando foi instrumentalizada para enquadrar a disputa geopolítica com a União Soviética como uma luta entre liberdade e tirania. Nesse contexto, como destaca Santos (2022), a essência do Destino Manifesto transcende a expansão territorial e inclui a disseminação do sistema de valores norte-americanos.

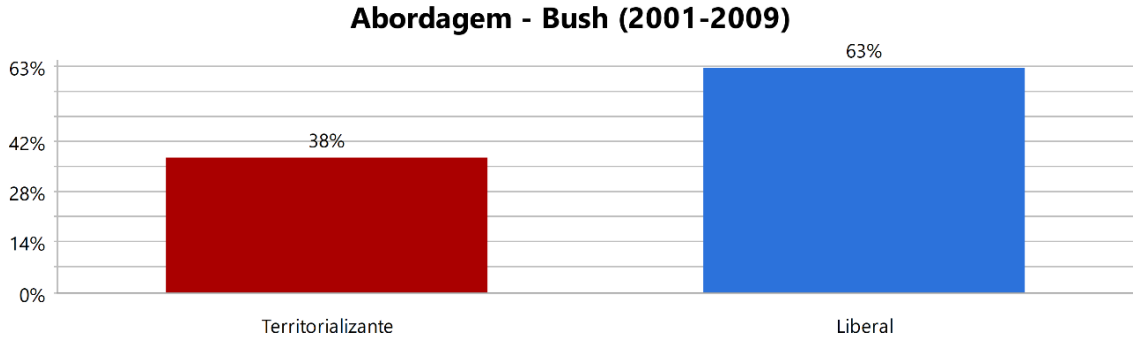
De maneira complementar, a Doutrina Monroe, proclamada em 1823 pelo presidente James Monroe (1817-1825), estabeleceu uma política externa fundamentada no princípio da não interferência europeia no Hemisfério Ocidental. Sob o lema de “América para os americanos”, os Estados Unidos “ consolidam sua zona de influência ao reivindicar para si o direito de proteger os países das Américas de intervenções extracontinentais (Pecequilo, 2016).

Essas mesmas visões, adaptadas e ressignificadas, manifestam-se no tratamento do ciberespaço pelo governo Bush. Assim como a Doutrina Monroe buscava impedir interferências de potências externas no Hemisfério Ocidental, a retórica de responsabilidade compartilhada presente nas políticas de cibersegurança americanas sugere a construção de um “Ciberespaço para os americanos”, um domínio no qual os Estados Unidos reivindicam como parte da sua esfera de influência e que deve permanecer sob controle americano contra ameaças externas.

Da mesma forma, Bush resgata a visão messiânica ao afirmar que “[...] nossa nação foi escolhida por Deus e comissionada pela história para ser um modelo de

justiça para o mundo" (Estados Unidos, 2000, s/p, tradução nossa[45]). Essa retórica se traduz nas políticas de cibersegurança por meio da ênfase na adoção e no reforço de melhores práticas (21%), evidenciando a tentativa norte-americana de projetar seus valores e normas no ciberespaço e por meio dele.

FIGURA 9 - DISTRIBUIÇÃO DAS ABORDAGENS LIBERAL E TERRITORIALIZANTE – BUSH (2001-2009)



Fonte: Elaboração própria

Embora a Figura 9 evidencie a predominância de uma abordagem liberal nas estratégias voltadas ao ciberespaço durante o governo Bush, é relevante destacar que esse período foi marcado por políticas de caráter fortemente territorializante, o que expõe uma significativa discrepância entre o discurso e as ações efetivamente implementadas. O exemplo mais emblemático desse contexto é a promulgação do *USA Patriot Act*, em 2001, que conferiu legitimidade ampliada às agências de inteligência (Estados Unidos, 2001).

Sob a justificativa de combate ao terrorismo no contexto da Guerra ao Terror, a autorização concedida por Bush, em outubro de 2001, permitiu que a NSA monitorasse o conteúdo de comunicações e os metadados relacionados, como ligações telefônicas e trocas de e-mails, sem a necessidade de aprovação prévia da *Foreign Intelligence Surveillance Court* (FISC ou FISA). Segundo Harris (2014), essa medida marcou o início do chamado *Military-Internet Complex.*

De forma específica, para que as interceptações da NSA ocorressem, dois critérios precisavam ser atendidos: (I) a comunicação deveria envolver algum indivíduo oriundo de país estrangeiro e (II) o indivíduo deveria estar sob suspeita de

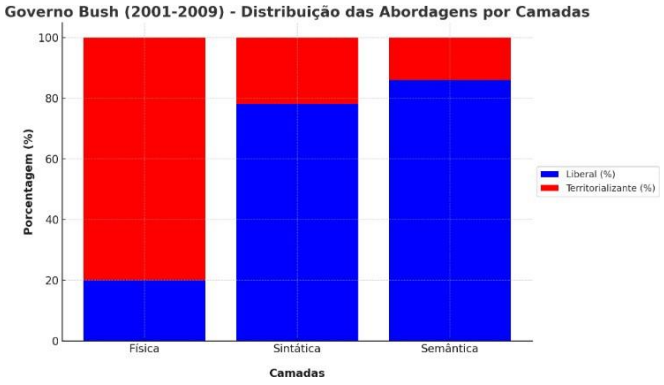
[45] No original: "[…] *our nation is chosen by God and commissioned by history to be a model to the world of justice"*

envolvimento com atividades terroristas (National Security Agency, 2009). Com base nisso, retoma-se o debate sobre a NSA apresentado no segundo capítulo e a metáfora da Möbius Strip desenvolvida por Didier Bigo (2001), destacando que essa decisão reforça dois pontos centrais.

Em primeiro lugar, conforme já pontuado no segundo capítulo, mas que merece ênfase, a vigilância exercida pela NSA reafirma a ideia de que as fronteiras entre segurança e defesa, entre o interno e o externo, tornam-se muito mais fluidas no domínio cibernético. Em segundo lugar, o programa de vigilância descrito ilustra de maneira precisa o fluxo contínuo representado pela metáfora da Möbius Strip. A agência, ao justificar suas ações sob o pretexto de combate ao terrorismo, projeta a jurisdição e a soberania dos Estados Unidos para além das fronteiras nacionais, monitorando indivíduos estrangeiros. Entretanto, essa vigilância também retorna ao território doméstico, uma vez que, para viabilizar a interceptação, é necessário que um americano esteja envolvido na comunicação.

Portanto, embora 63% das Unidades de Contexto analisadas nos documentos do governo Bush — o que corresponde a 208 segmentos — apresentem características liberais, o uso do aparato institucional para vigiar comunicações internas e externas evidencia que o governo promoveu um claro movimento de territorialização do ciberespaço, ao ampliar o alcance de sua jurisdição e soberania tanto sobre o ciberespaço quanto por meio dele.

FIGURA 10 - DISTRIBUIÇÃO DAS ABORDAGENS POR CAMADAS – BUSH (2001-2009)



Fonte: Elaboração própria

No que diz respeito ao enquadramento das camadas, a Figura 10 apresenta a distribuição das abordagens liberal e territorializante nas camadas física, sintática e semântica durante o governo Bush. Em síntese, as camadas semântica e sintática

apresentam aproximadamente 80% de segmentos associados à abordagem liberal, enquanto o tratamento da camada física, conforme previsto na hipótese deste trabalho, mostra-se majoritariamente territorializante.

3.2. Governo Obama (2009-2017): O c*apitalismo de Vigilância* e a Militarização do Ciberespaço

O governo Obama (2009-2017) se insere em um momento histórico em que a informação e os dados assumem um papel central como mecanismos de concentração de poder e acumulação de capital, viabilizados pela vigilância em massa através do ciberespaço. Embora a busca por superioridade informacional não seja uma novidade ao longo da história, a relevância estratégica dos dados digitais alcança, nesse período, uma nova dimensão e consolida-se como um dos principais ativos estratégicos do século XXI.

Alguns processos foram fundamentais para a consolidação dessa importância. Em primeiro lugar, a datificação social atingiu patamares elevados devido à popularização dos smartphones, especialmente com o lançamento do *iPhone* pela *Apple*, em 2007 e do sistema Android pela Google em 2008 (Pecequilo; Marzinotto Jr, 2022). A chamada 'computação de bolso' aprofundou a inserção do indivíduo no ciberespaço e transformou radicalmente a forma como as pessoas se relacionam, tanto com o mundo digital quanto entre si. Os smartphones passaram a funcionar como sensores portáteis, que geram, coletam e compartilham dados em tempo real, o que ampliou de forma expressiva o fluxo de informações existente (Cukier; *Mayer-Schonberger*, 2013). Em termos quantitativos, a penetração da internet nos Estados Unidos passou de aproximadamente 70% da população no início do governo Obama para cerca de 86% ao final de seu mandato, demonstrando a rápida expansão do acesso digital durante o período (Petrosyan, 2024).

Concomitantemente a essas mudanças sociais, os Estados Unidos enfrentavam uma das piores recessões desde a Grande Depressão de 1929. A crise no setor imobiliário de 2008, conhecida como crise do subprime, teve origem na concessão massiva de empréstimos hipotecários de alto risco a tomadores sem capacidade de pagamento. Esses empréstimos foram convertidos em títulos financeiros e negociados globalmente, e, quando os devedores começaram a

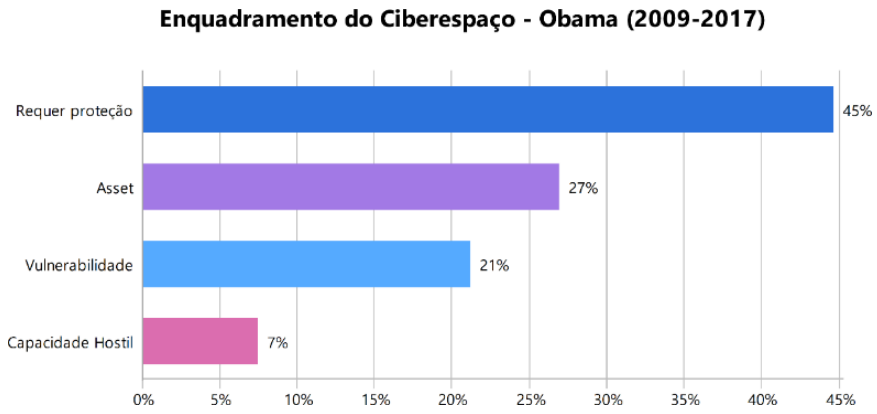
inadimplir, sobretudo em decorrência da elevação das taxas de juros, o sistema financeiro entrou em colapso, conforme apontado por Bresser-Pereira (*et al.,* 2009).

A crise financeira de 2008, por um lado, e a datificação social, por outro, criaram o cenário ideal para que o Vale do Silício se destacasse com produtos, ferramentas e inovações mercadológicas atraentes no enfrentamento da recessão, em um contexto de fragilidade do setor público diante da crise econômica (Morozov, 2018). Esse avanço provocou uma ruptura na lógica da economia capitalista tradicional e impulsionou uma transição para o que alguns autores denominam 'capitalismo digital', 'capitalismo de plataformas' ou 'capitalismo de vigilância' (Srnicek, 2019; Zuboff, 2021). Como destacam Pecequilo e Marzinotto Junior (2022), foi nesse período que surgiram diversos negócios digitais, tais como Uber (2009), WhatsApp (2009), Instagram (2010) e iFood (2011).

Em suma, os fatores supracitados consolidam de fato a ruptura definitiva entre a “Era Industrial” e a “Era da Informação”. Como apontam Couldry e Mejias (2019), se na Era Industrial as matérias-primas convertiam-se em mercadorias, agora os dados produzidos diariamente pelos indivíduos são expropriados pelas empresas para predição comportamental e, consequentemente, para a geração de mais lucro.

Esse novo ciclo de expropriação não se limita ao setor privado, mas também atende aos interesses de segurança nacional. A institucionalização da vigilância promovida no período pós-11 de setembro, durante o governo Bush, estabeleceu as bases para uma relação simbiótica entre grandes empresas de tecnologia — como Google, Microsoft e Apple — e órgãos de segurança, como a NSA, que se consolidou durante o governo Obama. Bauman et al. (2015) destacam que essa parceria permite às empresas extrair capital a partir dos dados coletados, ao mesmo tempo em que repassam essas informações ao Estado, que as utiliza para fortalecer seus mecanismos de vigilância e controle.

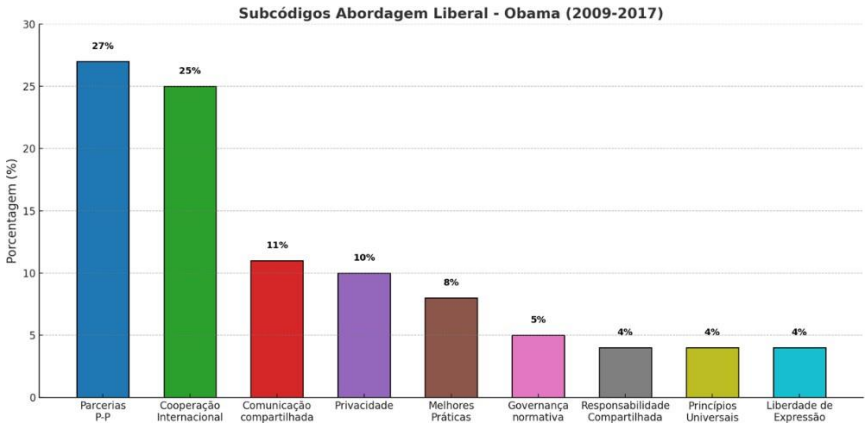
FIGURA 11 - CATEGORIA ENQUADRAMENTO – GOVERNO OBAMA (2009-2017)



Fonte: Elaboração própria

A crescente importância dos dados e, consequentemente, do ciberespaço reflete-se nos documentos analisados da administração Obama. Observa-se na Figura 11 que, das 525 Unidades de Contexto codificadas, aproximadamente 27% enquadram o ciberespaço como um *asset*. Comparativamente, em relação à administração Bush, o enquadramento do ciberespaço como um *asset* cresceu 8%, enquanto sua classificação como vulnerabilidade diminuiu 11%. Sem grandes surpresas, as Unidades de Contexto evidenciaram, de forma majoritária (45%), o ciberespaço como um domínio que demanda proteção. De maneira ilustrativa, a *National Security Strategy* de 2010 destaca-se como o primeiro documento de segurança nacional a conferir ao ciberespaço um protagonismo específico, ao dedicar uma subseção intitulada "*Secure Cyberspace*" dentro da seção "*Advancing Our Interests*".

FIGURA 12 - ABORDAGEM LIBERAL – OBAMA (2009-2017).



Fonte: Elaboração própria

Como ilustrado pela Figura 12, de maneira similar ao governo Bush, a administração Obama continuou a valorizar as parcerias com o setor privado. No entanto, no que diz respeito à cooperação internacional, a postura de Obama diferiu significativamente daquela adotada por seu antecessor. O unilateralismo agressivo característico do período pós-11 de setembro, somado às intervenções no Oriente Médio, provocou uma erosão da liderança estadunidense no Sistema Internacional. Diante desse cenário, a administração Obama passou a defender a cooperação internacional para os temas emergentes da agenda global, o ciberespaço incluso, ao reconhecer que esses temas exigiam respostas multilaterais (Maier, 2019). Sobre esse multilateralismo, uma passagem interessante do documento *International Strategy For Cyberspace* (Estados Unidos, 2011, p. 9, tradução nossa[46]), afirma que:

> Os Estados Unidos trabalharão com Estados que pensam da mesma forma para estabelecer um ambiente de expectativas, ou normas de comportamento, que fundamentem as políticas externas e de defesa e orientem as parcerias internacionais. As duas últimas décadas testemunharam o crescimento rápido e sem precedentes da Internet como meio social; [...] e evidências crescentes de que os governos estão buscando exercer o poder nacional tradicional por meio do ciberespaço. [...] trabalharemos para construir um consenso sobre o que constitui comportamento aceitável [...].

Percebe-se que, de maneira análoga ao período pós-Segunda Guerra Mundial, quando os Estados Unidos lideraram a construção da arquitetura econômica e de segurança global, a administração Obama buscou reafirmar o controle sobre a governança do ciberespaço, ao reivindicar um papel central na definição de normas e práticas que orientassem o comportamento dos Estados no domínio cibernético. Tal reafirmação se justifica pelo fato de o ciberespaço ser indiscutivelmente um domínio moldado pelos valores americanos de liberdade, livre circulação de informações e descentralização. De forma mais enfática, o ciberespaço não pode ser dissociado da ordem internacional construída no pós-Segunda Guerra, uma vez que é um produto direto desse contexto histórico e reflete profundamente seus valores e princípios (Barrinha; Renard, 2020). Nesse sentido, o multilateralismo defendido pelo governo

---

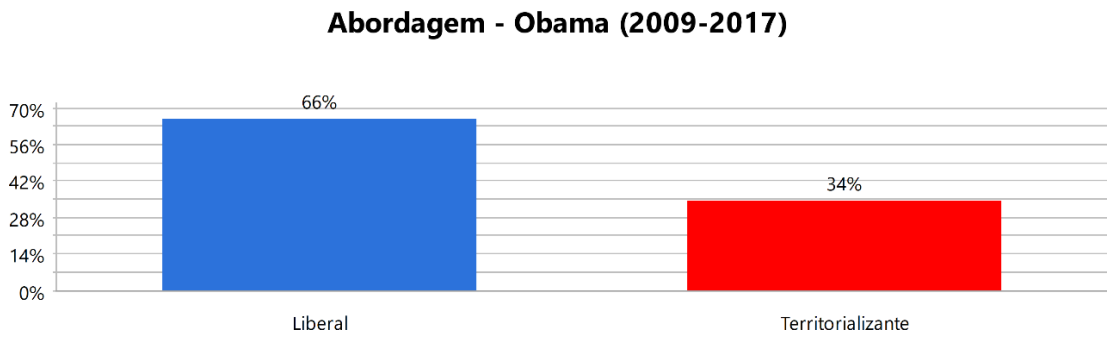
[46] No original: "*The United States will work with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships The last two decades have seen the swift and unprecedented growth of the Internet as a social medium;[...] and increasing evidence that governments are seeking to exercise traditional national power through cyberspace […] we will work to build a consensus on what constitutes acceptable behavior*"

Obama pode ser interpretado muito mais como um movimento de reafirmação da hegemonia estadunidense sobre o ciberespaço, acompanhado de uma tentativa de conter o descontentamento de países como Rússia e China, que passaram a reivindicar alternativas ao modelo ocidental de governança após as revelações de Edward Snowden.

Essa tentativa de manutenção da hegemonia americana no ciberespaço, por meio da construção de consenso e definição de normas, foi comprometida pelas contradições internas da própria administração Obama, especialmente no que diz respeito à espionagem e à privacidade. Embora a Figura 12 demonstre que a questão da privacidade dos indivíduos passou a ocupar um espaço crescente nos documentos produzidos durante essa administração, ironicamente, o governo Obama não apenas deu continuidade às práticas de vigilância institucionalizadas por seu antecessor, como também ampliou esse aparato. As revelações de Edward Snowden, ex-agente da NSA, expuseram a dissonância entre a retórica norte-americana de proteção da privacidade e as práticas de monitoramento em larga escala, ao evidenciar a extensão global do aparato de vigilância dos Estados Unidos.

Somado a isso, sabe-se que os Estados Unidos, em parceria com Israel, foram responsáveis pelo desenvolvimento do malware Stuxnet, descoberto em junho de 2010. Esse ataque cibernético, considerado o primeiro e único a causar danos cinéticos em uma Infraestrutura física, teve como alvo os sistemas de controle das turbinas das instalações de enriquecimento de urânio do Irã. Para atingir tal nível de sofisticação, é provável que o desenvolvimento do Stuxnet tenha se iniciado ainda durante o governo Bush. Entretanto, o uso de uma ferramenta ofensiva dessa magnitude revela uma contradição fundamental na postura adotada pelo governo Obama, que, ao mesmo tempo em que buscava promover normas internacionais de comportamento aceitável no ciberespaço por meio de iniciativas multilaterais, recorria a operações cibernéticas que desafiavam essas mesmas normas. Isso demonstra, mais uma vez, a dissonância entre o discurso nos documentos produzidos e a prática dos Estados Unidos no ciberespaço.

FIGURA 13 - DISTRIBUIÇÃO DAS ABORDAGENS LIBERAL E TERRITORIALIZANTE – OBAMA (2009-2017)



Fonte: Elaboração própria

À primeira vista, os dados apresentados na Figura 13 sugerem uma predominância da abordagem liberal nos documentos da administração Obama. Dos 346 segmentos analisados, 66% estão associados a essa perspectiva, o que indica uma prevalência do discurso voltado à liberdade, à abertura e à cooperação internacional. No entanto, é importante destacar, além de todas as contradições supracitadas, foi durante o governo Obama que a militarização do espaço cibernético foi institucionalizada, com a criação do USCYBERCOM (Giordano; Bosso, 2021). Como apontam Pecequilo e Marzinotto Jr. (2023), o estabelecimento do comando militar cibernético dos Estados Unidos elevou o ciberespaço ao status de domínio operacional, ao lado dos domínios terrestre, marítimo, aéreo e espacial. De forma semelhante às iniciativas anteriores, como a criação do *United States Indo-Pacific Command* (USINDOPACOM), em 1947, e do *United States Southern Command* (USSOUTHCOM), em 1963, o USCYBERCOM foi instituído com o objetivo de assegurar a ocupação e a proteção desse novo domínio estratégico.

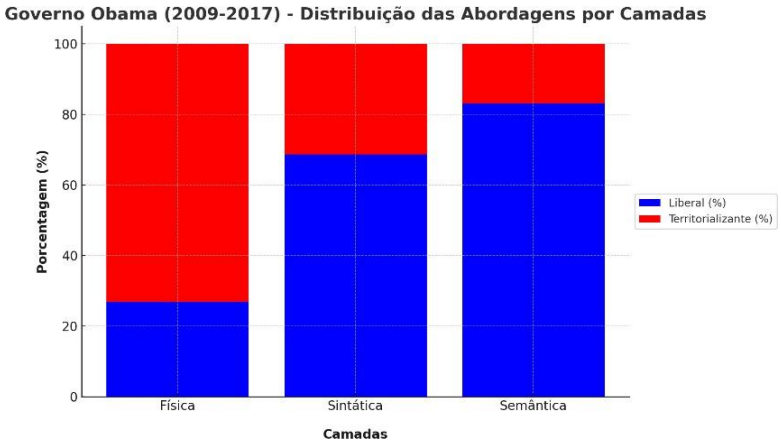
Não obstante, no que diz respeito à militarização do ciberespaço, é pertinente destacar que a *National Security Strategy* de 2015 já sinalizava as raízes das estratégias de *Defend Forward* e *Persistent Engagement* adotadas posteriormente pela administração Trump. Esse indicativo pode ser observado no trecho em que o documento postula:

> Nossas forças armadas permanecerão prontas para deter e derrotar ameaças à pátria, inclusive contra ataques de mísseis, cibernéticos e terroristas [...] As forças dos EUA continuarão a defender a pátria, realizar operações globais de contraterrorismo, assegurar aliados e deter a agressão por meio de

> presença e engajamento avançados (Estados Unidos, 2015, p.4, tradução nossa[47]).

Tal passagem demonstra que, ainda sob a administração Obama, já havia uma preocupação dos Estados Unidos em projetar continuamente sua presença militar no ciberespaço. Percebe-se, nesse contexto, o início da compreensão de que os conceitos tradicionais de segurança e defesa não seriam plenamente aplicáveis a esse domínio. Mais recentemente, Fischerkeller, Goldman e Harknett (2022) dialogam com essa perspectiva ao reconhecer que o ciberespaço demanda um enfoque diferenciado em relação aos paradigmas de segurança adotados ao longo do século XX. A ubiquidade da atividade cibernética desafia a noção de que a segurança pode ser articulada exclusivamente pela lógica de evitar a ação. Em vez disso, as dinâmicas do ciberespaço exigem uma sucessão contínua de engajamentos, na qual controle e vantagem são conceitos fluidos e mutáveis.

FIGURA 14 - DISTRIBUIÇÃO DAS ABORDAGENS POR CAMADAS – OBAMA (2009-2017)



Fonte: Elaboração própria

Quanto à maneira como cada camada foi abordada, a administração Obama apresentou um aumento relativo do discurso liberal tanto na camada física quanto na camada sintática, em comparação ao governo Bush. No entanto, conforme ilustrado pela Figura 14, observa-se que o discurso liberal continua predominantemente

---

[47] No original: *"Our military will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks [...] U.S. forces will continue to defend the homeland, conduct global counterterrorism operations, assure allies, and deter aggression through forward presence and engagement."*

vinculado às camadas semântica e sintática, enquanto a camada física permanece mais associada a abordagens territorializantes.

3.3. O Governo Trump (2017-2021): America First e o Ciberespaço

Desde sua campanha até a presidência, Donald Trump (2017-2021) representou um desafio à Ordem Liberal Internacional, construída e sustentada pelos Estados Unidos desde a década de 1970. Como aponta Ikenberry (2017), a ascensão de Trump rompeu com sete décadas de tradição diplomática americana, ao sinalizar o fim do apoio incondicional à União Europeia, promover o esvaziamento de instituições multilaterais — como os bloqueios à Organização das Nações Unidas (ONU) e à Organização Mundial da Saúde (OMS) — e desfazer importantes compromissos assumidos por seu antecessor, como a suspensão do Acordo de Paris e a retirada dos Estados Unidos da Parceria Transpacífica (TPP) (Marzinotto Jr., 2022).

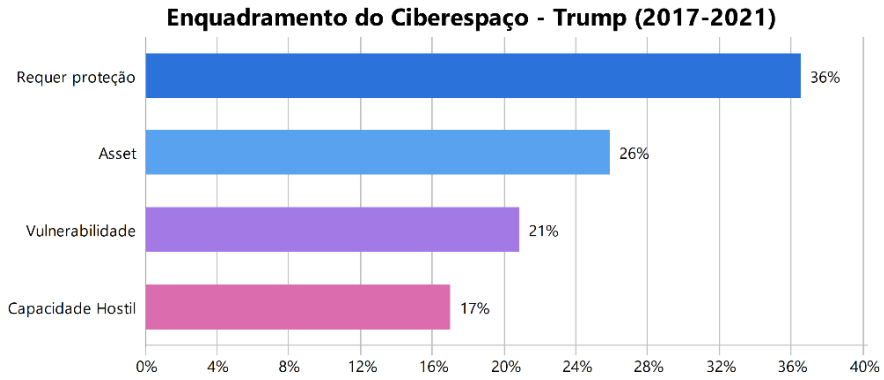
Entretanto, no que se refere ao ciberespaço, a estratégia adotada pelo governo Trump não apresentou uma ruptura tão significativa em relação à administração Obama. O que se observa, de maneira geral, é uma evolução coerente das políticas de cibersegurança norte-americanas ao longo dos últimos anos. De acordo com Devanny (2022), as mudanças de estratégia da era Trump estão muito mais associadas à percepção de que a estratégia implementada durante a era Obama não se mostrou adequada para lidar com o comportamento de adversários no ciberespaço do que a qualquer postura imprevisível ou "irracional" atribuída ao governo Trump.

De forma mais incisiva [48] que os governos anteriores, Trump transportou o discurso de "*America First"*, utilizado em sua campanha eleitoral, para o ciberespaço. Essa visão ficou claramente expressa na *National Security Strategy* de 2017, que afirma: "A internet é uma invenção americana, e deve refletir os nossos valores [...]" (Estados Unidos, 2017, p.13. tradução nossa). Tal discurso revela um viés nacionalista e territorializante que remonta ao conceito do Destino Manifesto e reafirma a "Missão

[48] Observa-se que a ideia de o ciberespaço ser uma invenção americana, que deve refletir os valores norte-americanos, esteve presente em diferentes graus em todas as administrações analisadas ao longo deste capítulo. A principal diferença encontra-se no grau de sutileza com que essa ideia foi apresentada nos documentos oficiais.

Divina" dos Estados Unidos de projetar seus valores para além de suas fronteiras nacionais.

FIGURA 15 - CATEGORIA ENQUADRAMENTO – GOVERNO TRUMP (2017-2021)



Fonte: elaboração própria

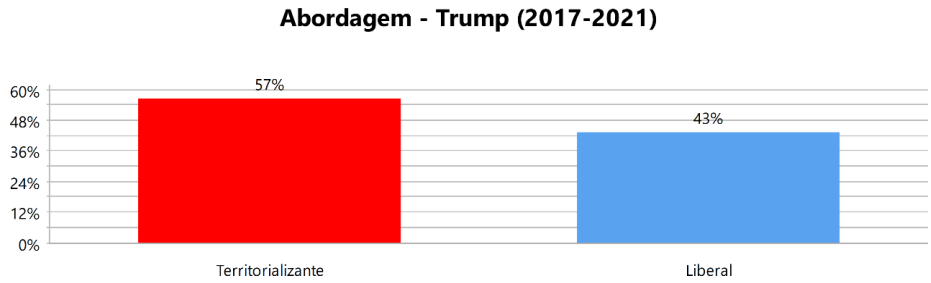
Como ilustra a Figura 15, o enquadramento do ciberespaço pelos Estados Unidos como um Asset estratégico ou como uma vulnerabilidade não sofreu alterações significativas em comparação ao governo Obama. No entanto, observa-se uma mudança relevante na distribuição desses enquadramentos: dos 236 segmentos [49] codificados, houve uma queda relativa de 9% na percepção do ciberespaço como algo a ser protegido. Em contrapartida, verificou-se um aumento de 10% no enquadramento do ciberespaço como uma capacidade hostil, ou seja, como um instrumento que pode ser utilizado contra os Estados Unidos.

Esse deslocamento de abordagem fundamenta-se na percepção norte-americana de que potências revisionistas, como Rússia e China, ascendem em diversas esferas nas quais os Estados Unidos anteriormente detinham primazia. Nesse contexto, a competição entre Grandes Potências torna-se uma questão central na NSS de 2017 (Medeiros, 2024). Essa competição se materializa no ciberespaço por meio da lógica discutida no segundo capítulo, baseada nas reflexões do General Paul Nakasone, ex-Comandante do USCYBERCOM. Segundo sua análise, por terem historicamente obtido sucesso em dissuadir ameaças convencionais, os Estados Unidos passaram a observar que potências revisionistas utilizam o ciberespaço como

[49] Os segmentos relacionados ao governo Trump são numericamente inferiores aos dos demais governos, uma vez que sua administração contou com apenas um mandato e produziu documentos significativamente menores em comparação com as administrações anteriores.

ferramenta assimétrica para comprometer o poder militar, político e econômico americano (Nakasone, 2020).

FIGURA 16 - DISTRIBUIÇÃO DAS ABORDAGENS LIBERAL E TERRITORIALIZANTE – TRUMP (2017-2021)



Fonte: Elaboração própria

Em resposta a esse cenário, os Estados Unidos adotaram uma postura mais assertiva no ciberespaço, fundamentada nos conceitos de *Defending Forward* e *Persistent Engagement*. Como consequência, observa-se uma significativa ampliação da militarização do ciberespaço, que se traduz em uma maior territorialização nos segmentos analisados nos documentos da administração. Como ilustra a Figura 16, de 152 segmentos analisados, 57% foram categorizados como pertencentes à abordagem territorializante. Assim, o governo Trump torna-se a primeira administração a apresentar predominância dessa abordagem em seus documentos analisados.

Esta intensificação da militarização do ciberespaço é explicitamente reconhecida pela própria administração Trump. No documento *Achieve and Maintain Cyberspace Superiority* do USCYBERCOM em 2018, o comando militar não apenas reconhece essa tendência, como também a justifica como uma resposta necessária às ações de seus adversários:

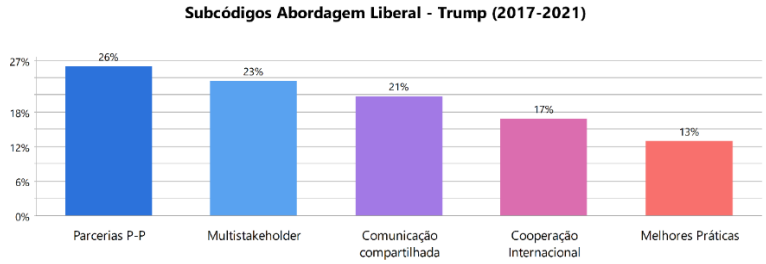
> Reconhecemos que os adversários já condenam os esforços dos EUA para defender nossos interesses e aliados como agressivos, e sabemos que eles também tentarão retratar nossa estratégia como uma "militarização" do domínio do espaço cibernético. O Comando não se desculpa por defender os interesses dos EUA, conforme orientação do Presidente por meio do Secretário de Defesa, em um domínio já militarizado por nossos adversários (Estados Unidos, 2018, p. 10, tradução nossa[50]).

[50] No original: *"We recognize that adversaries already condemn US efforts to defend our interests and allies as aggressive, and we expect they will similarly seek to portray our strategy as "militarizing" the cyberspace domain. The Command makes no apologies for defending US interests as directed by the President through the Secretary of Defense in a domain already militarized by our adversaries."*

No que diz respeito à abordagem liberal presente nos documentos, o governo Trump manteve uma relativa continuidade em relação aos seus antecessores. Dos 77 segmentos analisados, 26% destacam a necessidade e a importância das parcerias público-privadas, o que reafirma o papel central do setor privado na proteção do ciberespaço. Além disso, observa-se um aumento no uso do vocabulário de partes interessadas (*stakeholders*), no âmbito da mitigação de riscos, resposta à incidentes e aumento da resiliência.

No entanto, uma das preocupações apontada nos documentos analisados é a crescente vulnerabilidade dos Estados Unidos decorrente de sua dependência de *software* e *hardware* de produção estrangeira. O problema se agrava devido à priorização, por parte dos produtores globais, de custos e eficiência em detrimento de parâmetros rigorosos de segurança. Assim, por não produzirem internamente a totalidade de componentes essenciais, os Estados Unidos se veem expostos sua cadeia de suprimentos tecnológicos a vulnerabilidades na cadeia global de produção.

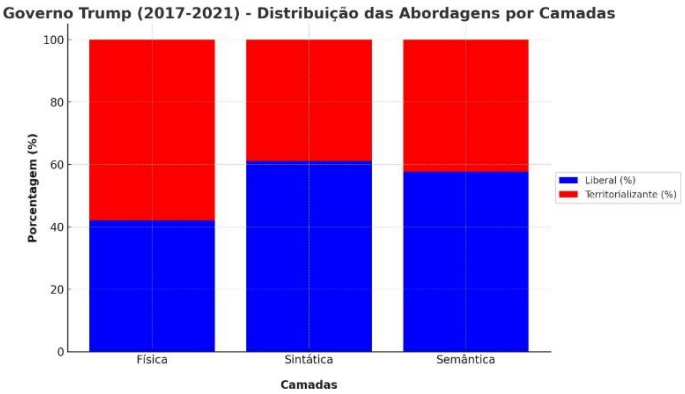
FIGURA 17 - ABORDAGEM LIBERAL – TRUMP (2017-2021)



Fonte: elaboração própria

Assim, mais uma vez, a importância da geografia do ciberespaço se faz presente, evidenciando a constante tensão entre a lógica liberal e territorializante que permeia as políticas de cibersegurança dos Estados Unidos. Por um lado, a globalização contínua da cadeia de suprimentos de tecnologia da informação reforça a lógica liberal, que prioriza o comércio internacional, o compartilhamento de informações, a cooperação multilateral e as parcerias público-privadas. Por outro lado, as vulnerabilidades decorrentes da dependência estrangeira fortalecem a lógica territorializante, na qual os Estados Unidos buscam reduzir essa dependência externa por meio de medidas que privilegiam a produção doméstica.

FIGURA 18 - DISTRIBUIÇÃO DAS ABRDAGENS POR CAMADAS – TRUMP (2017-2021)



Fonte: elaboração própria

No que concerne à distribuição das abordagens entre as camadas, percebe-se que, durante o governo Trump, houve um aumento relativo na territorialização das camadas semântica e sintática. Esse aumento fundamenta-se nas estratégias de *Defend Forward* e *Persistent Engagement* adotadas pelo USCYBERCOM, que deixaram de se restringir a operações reativas nas redes do DoDIN e passaram a adotar uma abordagem proativa e de alcance global.

3.4. O Governo Biden (2021-2025): A Defesa da Ordem Liberal no Ciberespaço

A administração de Joe Biden (2021-2025) herdou um cenário complexo, tanto nos domínios tradicionais quanto no ciberespaço, marcado pela intensificação da competição entre Grandes Potências e pelas instabilidades sistêmicas decorrentes de eventos como a pandemia de COVID-19 e a Guerra na Ucrânia, iniciada em 2022. No campo cibernético, os primeiros anos do governo enfrentaram desafios significativos, com a ocorrência de incidentes de grande escala, como o ataque à SolarWinds, revelado no final de 2020, e o ataque ransomware à Colonial Pipeline, em 2021, que interrompeu o fornecimento de combustível na Costa Leste dos Estados Unidos.

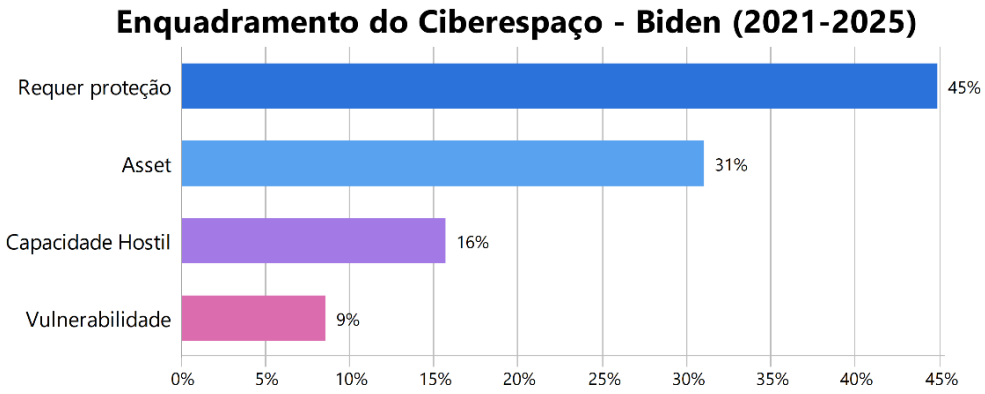
Diante desse cenário, a *National Cybersecurity Strategy* (Estados Unidos, 2023) reflete a percepção crescente de que a ordem cibernética estabelecida desde a criação da Internet encontra-se em processo de erosão, e identifica a República Popular da China como seu principal contestador. De acordo com a estratégia:

> A República Popular da China (RPC) apresenta atualmente a ameaça mais ampla, mais ativa e mais persistente às redes dos setores governamental e privado e é o único país com a intenção de remodelar a ordem internacional e, cada vez mais, com o poder econômico, diplomático, militar e tecnológico

> para fazê-lo [...] Tendo aproveitado com sucesso a Internet como a espinha dorsal de seu estado de vigilância e de suas capacidades de influência, a RPC está exportando sua visão de autoritarismo digital, esforçando-se para moldar a Internet global à sua imagem e colocando em risco os direitos humanos além de suas fronteiras (Estados Unidos, 2023, p.3, tradução nossa[51]).

Douzet e Taillat (2022) afirmam que o retorno da competição interestatal no cenário internacional evidencia uma crise de legitimidade e de recursos dos Estados Unidos no ciberespaço. Diante disso, essa realidade manifesta-se de duas formas nos documentos da administração Biden.

FIGURA 19 - CATEGORIA ENQUADRAMENTO – GOVERNO BIDEN (2021-2025)



Fonte: elaboração propria

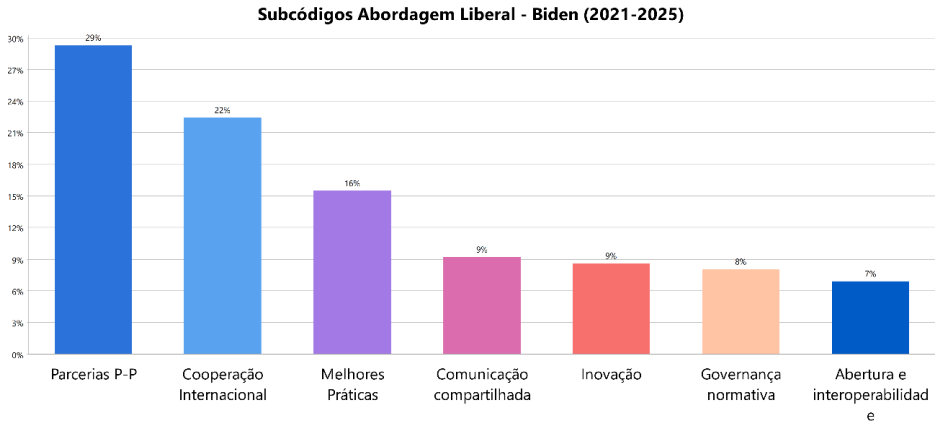
Primeiramente, em continuidade às administrações anteriores, o governo Biden manteve o enquadramento do ciberespaço predominantemente como um domínio que requer proteção. Como demonstra a Figura 19, dos 281 segmentos analisados, 45% foram codificados sob essa perspectiva. Além disso, em 31% dos segmentos, o ciberespaço apareceu como um *asset*, resultado do ressurgimento da dissuasão como principal estratégia diante da nova realidade competitiva. A administração Biden definiu como prioridade conter as ameaças representadas pelo que se pode denominar de 'novo eixo do mal', composto por Rússia, China, Irã e Coreia do Norte, buscando alcançar esse objetivo por meio da integração de diferentes capacidades do poder nacional. Nesse contexto, as capacidades cibernéticas assumiram papel

[51] No original: *"The People's Republic of China (PRC) now presents the broadest, most active, and most persistent threat to both government and private sector networks and is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so […] Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders."*

central nessa estratégia. Observa-se, portanto, a continuidade das estratégias de defesa ativa, engajamento constante e imposição de custos, estabelecidas durante a administração Trump.

No que se refere à abordagem liberal, o governo Biden resgata diversos elementos presentes na administração Obama, adaptando-os às especificidades do cenário atual. Conforme ilustrado na Figura 20, entre os 174 segmentos analisados, a cooperação internacional apareceu em 22% deles, ficando em segundo lugar, atrás apenas das parcerias público-privadas, que representaram 29%. As público-privadas para a proteção de Infraestruturas Críticas mantém-se como um ponto central da estratégia cibernética, e sofreram influência das dinâmicas geopolíticas vigentes.

FIGURA 20 - ABORDAGEM LIBERAL – BIDEN (2021-2025)



Fonte: elaboração própria

Desde o início da Guerra na Ucrânia, em fevereiro de 2022, a Rússia conduziu aproximadamente 240 operações cibernéticas contra alvos civis e militares ucranianos (Souza; Oliveira; de Paula, 2024). Diante desse contexto, como forma de antecipar possíveis ataques, a CISA lançou, em 2022, a campanha de conscientização *Shields Up*, voltada ao setor privado e à população, com o objetivo de mitigar os impactos de potenciais transbordamentos das operações cibernéticas russas sobre os Estados Unidos.

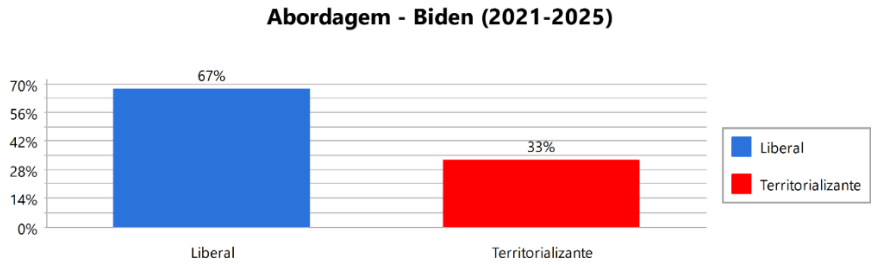
Além do fortalecimento das parcerias público-privadas, a administração Biden resgatou o multilateralismo, abandonado pela gestão anterior, ao recorrer a instituições e fóruns multilaterais, como o *United Nations Group of Governmental Experts* (GGE) e o *Open-Ended Working Group* (OEWG), como demonstram os 8% da categoria de Governança Normativa na Figura 20. Assim como na administração

Obama, Biden busca reafirmar o papel dos Estados Unidos na governança do ciberespaço, fundamentando sua abordagem no antagonismo entre democracias e autocracias. Como demonstra a NCS de 2023:

> À medida que os regimes autocráticos buscam mudar a Internet e sua base multistakeholder para permitir o controle, a censura e a vigilância do governo, os Estados Unidos e seus parceiros estrangeiros e do setor privado implementarão uma estratégia multifacetada para preservar a excelência técnica, proteger nossa segurança, impulsionar a competitividade econômica, promover o comércio digital e garantir que as "regras do caminho" para os padrões de tecnologia favoreçam os princípios de transparência, abertura, consenso, relevância e coerência (Estados Unidos, 2023, p. 24, tradução nossa).

Ironicamente, as práticas de monitoramento em larga escala conduzidas pelas agências de inteligência norte-americanas, detalhadas no capítulo dois e na subseção dedicada ao governo Obama, refletem exatamente as ações que o governo Biden condena nos regimes autoritários. A contradição torna-se ainda mais evidente quando, ao mesmo tempo em que os Estados Unidos promovem uma narrativa de defesa da liberdade de expressão, da privacidade e do combate à censura e ao autoritarismo digital por meio da *Declaration for the Future of the Internet* (DFI) (Estados Unidos, 2022), a própria administração Biden implementa medidas restritivas, como o banimento do aplicativo de vídeos TikTok sob a justificativa de ameaça à segurança nacional (Sherman, 2025).

FIGURA 21 - DISTRIBUIÇÃO DAS ABORDAGENS LIBERAL E TERRITORIALIZANTE – BIDEN (2021-2025)

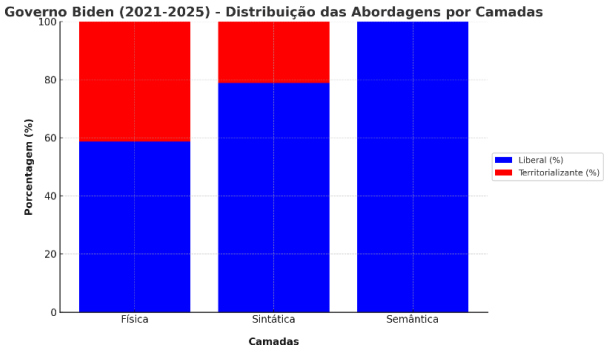


Fonte: elaboração própria

A Figura 21 demonstra que a análise dos documentos da administração Biden indica uma reafirmação dos princípios liberais no ciberespaço: dos 208 segmentos analisados, 67% foram codificados como liberais. No entanto, embora os dados apontem para o retorno da predominância da abordagem liberal em relação à gestão anterior, é fundamental observar que, assim como na era Obama, essa retórica liberal

funciona como um verniz que oculta a contínua territorialização do ciberespaço por meio do controle sobre sua governança. A administração Biden, portanto, resgata esse discurso não apenas como uma reafirmação dos valores liberais, mas como um instrumento estratégico para consolidar sua influência sobre os protocolos e normas que regulam o domínio cibernético.

FIGURA 22 - DISTRIBUIÇÃO DAS ABORDAGENS POR CAMADAS – BIDEN (2021-2025)



Fonte: elaboração própria

Em relação à distribuição das abordagens nas camadas, a Figura 22 revela que a administração Biden foi a que menos territorializou a Camada Física na publicação de seus documentos, em comparação com os governos anteriores. No entanto, é importante ressaltar que esse é o mesmo governo que defende a necessidade de que componentes e sistemas críticos sejam “cada vez mais desenvolvidos internamente ou em estreita coordenação com aliados e parceiros que compartilham nossa visão [...]”(Estados Unidos, 2023, p. 32, tradução nossa). Assim como na administração Trump, há o reconhecimento da dependência norte-americana em relação às cadeias de suprimentos externas e a adoção de estratégias para reduzir essa vulnerabilidade. Nesse sentido, a política de *nearshoring* surge como uma solução para realocar as cadeias produtivas para países aliados.

3.5. Considerações Analíticas

Ao longo deste capítulo, observou-se que, apesar das diferenças ideológicas entre as administrações democratas e republicanas, há uma clara continuidade nas estratégias de cibersegurança adotadas pelos Estados Unidos. A análise dos documentos demonstra que, independentemente da administração, as políticas de

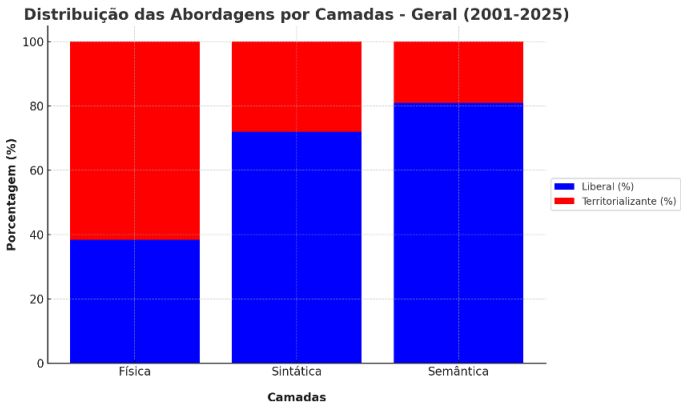
cibersegurança seguem uma trajetória consistente e se ajustam às transformações sociais, econômicas, políticas e tecnológicas. Assim como o ciberespaço da Arpanet difere do atual, as estratégias para a sua operacionalização passam por adaptações naturais à medida que o domínio cibernético evolui e se transforma.

Constata-se que, ao longo dos anos, o ciberespaço, embora frequentemente enquadrado como uma vulnerabilidade e um domínio que exige proteção contínua, passou a ser reconhecido como um ativo estratégico fundamental para os interesses dos Estados Unidos. Inicialmente, sua importância estava amplamente associada ao impulso do crescimento econômico e à inovação tecnológica. Contudo, com o acirramento das pressões sistêmicas, consolidou-se a percepção do ciberespaço como um elemento do poder nacional, indispensável para a dissuasão de atores rivais.

Essa mudança de percepção decorre da própria natureza complexa e dinâmica do ciberespaço, que se configura simultaneamente como objeto de disputa, campo de batalha e ferramenta estratégica. Ele representa o objeto de disputa entre os atores, que buscam estabelecer normas, padrões e exercer influência sobre sua governança de modo a atender a seus interesses nacionais. Ao mesmo tempo, constitui o espaço onde essas disputas ocorrem, sendo o ambiente no qual se realizam ações cibernéticas — ofensivas e defensivas. Além disso, funciona como um mecanismo para a concretização dessa competição, por meio da utilização de *malwares*, ataques de DDoS e campanhas de desinformação, utilizados par alcançar objetivos estratégicos.

No que diz respeito à hipótese inicial desta pesquisa, postulava-se a existência de uma distinção entre as 'camadas superiores' do ciberespaço, nas quais prevalece uma abordagem liberal que enfatiza a livre circulação de informações, e a 'camada inferior', caracterizada por uma postura mais protecionista, voltada à segurança das Infraestruturas Críticas

FIGURA 23 - DISTRIBUIÇÃO DAS ABORDAGENS – GERAL (2001-2025)



Fonte: elaboração própria

A Figura 23 apresenta a distribuição das abordagens por camadas nos documentos das administrações analisadas de forma geral. De certo modo, os resultados obtidos conferem respaldo à hipótese inicial, conforme evidenciado pela análise de conteúdo realizada. No entanto, é fundamental destacar que a territorialização das Infraestruturas Críticas acarreta, inevitavelmente, a territorialização das demais camadas, ou seja, dos sistemas que asseguram seu funcionamento. Dessa forma, constata-se que a separação entre as camadas do ciberespaço revela-se mais conceitual do que prática, em razão da interdependência inerente entre essas diferentes camadas.

Nesse sentido, apesar das diferenças intrínsecas entre as abordagens territorializantes e liberais, observa-se que a abordagem liberal promovida pelos Estados Unidos não escapa a uma lógica de territorialização. De fato, sob o verniz de excepcionalismo que permeia a política externa norte-americana, o discurso liberal serve como um instrumento estratégico para consolidar a influência no ciberespaço e através dele. Isso porque, assim como ocorreu nos domínios tradicionais – terrestre, marítimo, aéreo e espacial – a territorialização do ciberespaço emerge como uma resposta às crescentes pressões por segurança e soberania. Quanto mais as disputas geopolíticas migraram para o domínio cibernético, mais este passou a ser percebido como um espaço em disputa. No entanto, tais disputas vão além das operações cibernéticas militares convencionais, e abrangem a dimensão normativa e diplomática.

Mais relevante do que simplesmente deter capacidades cibernéticas – ou seja, o recurso em si – é exercer controle sobre as regras e padrões que estruturam o ciberespaço. Em resposta a essa necessidade, observa-se o surgimento da *Cyber-*

diplomacy, caracterizada pelo 'uso de recursos diplomáticos e o desempenho de funções diplomáticas para garantir os interesses nacionais em relação ao espaço cibernético' (Barrinha; Renard, 2017, p. 5).

Nesse sentido, a defesa de uma abordagem liberal para o ciberespaço pelos Estados Unidos, paradoxalmente, promove sua territorialização. Por um lado, o discurso liberal enfatiza a livre circulação de informações, a abertura, a interoperabilidade, a descentralização e a cooperação internacional, apresentando o ciberespaço como um bem comum global. Por outro lado, ao estabelecer normas, protocolos e padrões técnicos, os Estados Unidos asseguram que seus valores e interesses sejam internalizados como padrões universais.

4. Considerações Finais

A presente dissertação teve como objetivo analisar como as políticas públicas de cibersegurança dos Estados Unidos refletem uma tensão entre as abordagens territorializantes e liberais do ciberespaço. A partir da Revolução Técnico Científica, ocorrida na década de 1970, o ciberespaço se engendrou na maioria dos processos sociais do século XXI, inclusive no gerenciamento e gestão das Infraestruturas Críticas.

Isto posto, a pergunta que orientou esta dissertação foi: como as políticas de cibersegurança para infraestruturas críticas dos Estados Unidos refletiram uma tensão entre as abordagens territorializantes e liberais do ciberespaço? Como hipótese, postulou-se que, nas políticas de cibersegurança dos Estados Unidos, existia uma distinção fundamental entre a 'camada superior' do ciberespaço, na qual prevalecia uma abordagem liberal que enfatizava a livre circulação de informações, e a 'camada inferior', que adotava uma postura mais protecionista focada na segurança das Infraestruturas Críticas.

No primeiro capítulo, buscou-se estabelecer os fundamentos teóricos essenciais para a compreensão da pesquisa. A partir da revisão de literatura, constatou-se que a dualidade material/imaterial do ciberespaço dificultava sua compreensão, pois muitas vezes este era percebido como algo intangível e imaterial. Portanto, autores como Ventre (2012) e Libicki (2009), que conceituavam o ciberespaço através de uma lógica estratificada, foram utilizados como base para uma melhor compreensão da materialidade do ciberespaço na realidade.

Não obstante, a relação intrínseca entre as infraestruturas críticas (ICs) e o ciberespaço foi analisada com base na Trindade Conceitual Fundamental do Ciberespaço (T.C.F), ferramenta analítica desenvolvida por Medeiros e Goldoni (2020). A T.C.F é composta por três peculiaridades fundamentais do ciberespaço: desterritorialidade, multiplicidade de atores e incerteza, as quais são essenciais para compreender as complexas relações entre o ambiente cibernético e as infraestruturas críticas.

Em primeiro lugar, a multiplicidade de atores, em relação às Infraestruturas Críticas (ICs), ressaltava que a proteção dessas infraestruturas não era uma responsabilidade exclusiva do Estado, mas sim uma tarefa conjunta que exigia uma cooperação eficaz entre o setor público e o privado. Utilizando os Estados Unidos

como exemplo, constatou-se que uma das grandes dificuldades na proteção e mitigação de vulnerabilidades dessas infraestruturas reside na necessidade de parcerias público-privadas robustas, uma vez que a maior parte das ICs do país está sob controle de empresas privadas. Nos EUA, aproximadamente 85% das infraestruturas críticas são de propriedade e operação do setor privado, o que impõe desafios adicionais à implementação de políticas de cibersegurança eficazes.

Não somente, mas a multiplicidade de atores que agora possuem a capacidade de operar no ciberespaço desafia a noção de que o Estado detém o monopólio da força. A simbiose entre as Tecnologias da Informação e Comunicação (TICs) e o ciberespaço, juntamente com a crescente dependência da sociedade dessas tecnologias, abriu uma nova frente de vulnerabilidades que os Estados precisam gerenciar.

Ainda no primeiro capítulo, foi examinada a crescente tendência de equiparar o ciberespaço a um espaço geográfico. Com base na literatura, verificou-se uma significativa inclinação em associar o ciberespaço a noções de território, fronteiras e soberania. Entende-se que o ciberespaço sempre foi um campo onde disputas por poder e soberania se manifestam, fatores intrínsecos à Geografia e Geopolítica. Portanto, através de novas concepções de territorialidade, pode-se compreender que o processo de territorialização do ciberespaço reflete preocupações geopolíticas contemporâneas, nas quais Estados buscam controlar ativos essenciais para a sua segurança e riqueza.

Portanto, longe de representar o fim do território, o advento do ciberespaço e sua concomitante desterritorialização não representaram uma ruptura com o modelo estatal tradicional, mas sim uma complexificação do modelo westfaliano. Isso ocorre porque todo movimento de desterritorialização é inevitavelmente seguido por um processo de reterritorialização, no qual os Estados buscam reafirmar sua soberania e controle sobre esse domínio. No entanto, a natureza desmaterializada do ciberespaço — caracterizada pelo espectro eletromagnético — apresenta desafios significativos para a imposição de fronteiras, fator que não impede Estados de tentar impor formas de controle. Constatou-se, portanto, que a cibersegurança em si se tornou um dos principais mecanismos pelos quais os Estados justificam a ampliação de sua soberania em nome da “segurança nacional”.

No segundo capítulo teve como objetivo mapear e analisar a estrutura organizacional de cibersegurança dos Estados Unidos, mais especificamente: o

Department of Homeland Security (DHS), a *Cybersecurity and Infrastructure Security Agency* (CISA), o *Department of Defense* (DoD), o *United States Cyber Command* (USCYBERCOM), o *Department of* Justice (DOJ), o *Federal Bureal of Investigation* (FBI), o *United States Secret Service* (USS) e o *Office of National Cyber Director.*

Para fundamentar o capítulo, foi realizada uma discussão aprofundada sobre os conceitos de Segurança e Defesa. Constatou-se que, devido às peculiaridades inerentes ao domínio cibernético, existem dificuldades em estabelecer distinções claras entre Segurança e Defesa (Interno x Externo) no ciberespaço. Além disso, observa-se uma extrapolação de competências de órgãos tradicionalmente voltados à segurança para funções relacionadas à defesa, e vice-versa.

No caso do DoD, observa-se que, por meio do USCYBERCOM, há uma clara tentativa de territorialização do espaço cibernético, fundamentada nas doutrinas de *Defend Forward* e *Persistent Engagement*. Essas estratégias visam projetar a soberania dos Estados Unidos para além de suas fronteiras físicas, através de uma postura mais proativa no espaço cibernético. Além disso, a vinculação estreita entre o USCYBERCOM e a NSA, por meio da liderança compartilhada, extrapola o escopo da atuação do DoD como um órgão de Defesa. Um exemplo é o envolvimento recente do departamento na proteção e integridade dos processos eleitorais.

Por outro lado, a NSA, tradicionalmente ligada à segurança interna e inteligência, tornou-se controversa por escândalos de espionagem e vigilância em massa. Revelações de Edward Snowden mostraram que a agência extrapolou suas funções e usou o ciberespaço para expandir a jurisdição dos Estados Unidos em nome da segurança nacional ao coletar dados de cidadãos e líderes estrangeiros.

Outra constatação relevante foi observar que o DHS inclui a cibersegurança e a proteção de infraestruturas críticas como uma de suas principais missões institucionais. Essa abordagem chama a atenção, considerando que o DHS é, por definição, um departamento voltado à segurança interna, o que levanta questionamentos. Tal inclusão pode ser compreendida como a tentativa do DHS de enquadrar o ciberespaço dentro das fronteiras estatais, tratando-o como uma extensão do território nacional a ser protegido.

Por fim, no último capítulo foi utilizada a Análise de Conteúdo (A.C.) como ferramenta metodológica para examinar as estratégias de cibersegurança publicadas pelos Estados Unidos ao longo do século XXI com o objetivo de testar a hipótese formulada. A aplicação da A.C. permitiu uma abordagem sistemática dos documentos

selecionados e possibilitou a identificação de padrões. Combinada com uma análise conjuntural, foi possível obter uma visão de como os governos recentes enquadraram o ciberespaço.

Algumas percepções importantes emergiram da A.C. aplicada. Primeiramente, há uma certa continuidade na política aplicada para o ciberespaço entre os governos. Embora cada administração tenha ajustado suas estratégias para atender determinadas prioridades específicas do contexto geopolítico e interno vigentes, não houve rupturas significativas.

A análise dos documentos revela que, ao longo do tempo, houve uma ampliação da percepção americana sobre o ciberespaço. Inicialmente concebido principalmente como uma vulnerabilidade—um espaço suscetível a ataques e intrusões—, embora reconhecido como essencial para a economia, a inovação e a conectividade global, aos poucos passou a ser considerado uma capacidade estratégica essencial para a dissuasão de atores rivais.

Quanto à hipótese formulada, a Figura 23, apresentada no capítulo 3, confirma a distinção entre as abordagens adotadas para as diferentes camadas do ciberespaço. Os resultados obtidos demonstram que as camadas superiores—sintática e semântica—são predominantemente tratadas sob uma perspectiva liberal, enfatizando a livre circulação de informações, a inovação tecnológica e a interoperabilidade global. Em contrapartida, a camada inferior, camada física, é abordada de maneira mais territorializante, refletindo preocupações com a soberania nacional, o controle estatal e a proteção das infraestruturas críticas.

Entre os achados desta pesquisa, observa-se que, embora as abordagens territorializantes e liberais possam ser contrastantes, a abordagem liberal adotada pelos Estados Unidos no ciberespaço não está isenta de uma lógica de territorialização. Esse fato é claramente evidenciado em documentos recentes, que evocam princípios liberais de um ciberespaço livre e aberto para conter a influência de grandes potências como China e Rússia. Conclui-se, portanto, que o grande palco da disputa política pelo controle do ciberespaço se dá cada vez mais nos Fóruns de Governança, foco da agenda de pesquisas futuras.

REFERÊNCIAS

16th AIR FORCE (AIR FORCES CYBER). **About Us**. Disponível em: https://www.16af.af.mil/About-Us/. Acesso em: 9 jul. 2024.

ALBUQUERQUE, F. L. Relações Internacionais: o estado da disciplina. **Conjuntura internacional**, v. 18, n. 1, p. 6–15, 10 dez. 2021.

ALBUQUERQUE, F. L. Relações Internacionais: o estado da disciplina. **Conjuntura internacional**, v. 18, n. 1, p. 6–15, 10 dez. 2021.

ARMY CYBER COMMAND (ARCYBER). **About Army Cyber**. Disponível em: https://www.arcyber.army.mil/About/About-Army-Cyber/. Acesso em: 9 jul. 2024.
BADIE, Bertrand. La fin des territoires westphaliens**. Géographie et cultures**, v. 20, p. 113-118, 1996.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARLOW, J. P. A declaration of the independence of Cyberspace. **Eletronic Frontier Foundation**, 1996. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: 27 29 fev. 2024.

BARRETT, Brian. **Russia's SolarWinds Hack Is a Historic Mess**. *Wired*, 2020. Disponível em: https://www.wired.com/story/russia-solarwinds-hack-roundup/. Acesso em: 12 set. 2024.

BARRINHA, A.; RENARD, T. Cyber-diplomacy: the making of an international society in the digital age. **Global Affairs**, v. 3, n. 4–5, p. 353–364, 20 out. 2017.

BARRINHA, A.; RENARD, T. Power and diplomacy in the post-liberal cyberspace. **International Affairs**, v. 96, n. 3, p. 749–766, 1 maio 2020.

BAUMAN, Z. et al. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, v. 8, n. 2, p. 121–144, jun. 2014.

BIGO, Didier. The Möbius Ribbon of Internal and External Security(ies). In: ALBERT, Mathias; JACOBSON, David; LAPID, Yosef (Ed.). ***Identities, Borders, Orders: Rethinking International Relations Theory.*** NED-New edition, v. 18. University of Minnesota Press, 2001. p. 91–116

BLACK, Jeremy. The revolution in military affairs: the historian's perspective. **The RUSI Journal,** v. 154, n. 2, p. 98 102, 2009.

BORJA, Elizabeth C. *Brief documentary history of the Department of Homeland Security, 2001-2008*. [Washington, D.C.]: U.S. Department of Homeland Security, History Office, 2008. Disponível em: <https://www.govinfo.gov/content/pkg/GOVPUB-HS-PURL-LPS118010/pdf/GOVPUB-HS-PURL-LPS118010.pdf>. Acesso em: 8 jul. 2024.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Diário Oficial da União, Brasília, DF, 27 dez. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 25 de mar, 2024.

BRESSER-PEREIRA, Luiz CarLos *et al*. A crise financeira de 2008. **Brazilian Journal of Political Economy**, v. 29, n. 1, p. 133-149, 2009.

BRESSER-PEREIRA, Luiz CarLos *et al*. A crise financeira de 2008. **Brazilian Journal of Political Economy**, v. 29, n. 1, p. 133-149, 2009.

BRODIE, B. **National security policy and economic stability**. Yale Institute of International Studies, 1950.

BURGESS, M. WikiLeaks drops “Grasshopper” documents, part four of its CIA Vault 7 files. **Wired**, 2017. Disponível em: <https://www.wired.co.uk/article/cia-files-wikileaks-vault-7>. Acesso em: 20 fev. 2024.

BUSH, George W. **Address to a Joint Session of Congress and the American People**. The White House, Washington, D.C., 20 set. 2001. Disponível em: https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html. Acesso em: 2 jul. 2024.

CASSINO, J.; SOUZA, J.; SILVEIRA, S. A. DA (EDS.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra liberal**. São Paulo, SP: Autonomia Literária, 2021.

CAVELTY, M. D. Cyber-Security. *In*: BURGESS, P. **The Routledge Handbook of New Security Studies.** Nova York: Routledge, 2010.

CAVELTY, M.D. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. **International Studies Review**, v. 15, n. 1, p. 105–122, mar. 2013.

CEPIK, M. **Espionagem e democracia**. 1. Ed ed. Rio de Janeiro: Ed. FGV, 2003.

CEPIK, M.; CANABARRO, D.; BORNE, T. Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica. In: SOUZA, A.; NASSER, R. M.; MORAES, R. F. (Eds.). **Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI**. Brasília: IPEA, 2014. p. 161–186.

CIMPANU, C.**Trump signs bill that creates the Cybersecurity and Infrastructure Security Agency**. ZDNET, 2018. Disponível em: <https://www.zdnet.com/article/trump-signs-bill-that-creates-the-cybersecurity-and-infrastructure-security-agency/>. Acesso em: 11 jul. 2024.

COELHO NETO, A. S. networks and territories. **Mercator**, v. 12, n. 28, p. 19–34, 30 ago. 2013.

COMPUTER SECURITY RESOURCE CENTER (CSRC) . **Malware**. Disponível em: <https://csrc.nist.gov/glossary/term/malware>. Acesso em: 27 mar. 2024.

CONNELL, Michael; VOGLER, Sarah. **Russia's approach to cyber warfare**. Arlington, VA: CNA, 2017.

COSTA, D. Segurança e defesa: uma única visão abaixo do Equador. **Revista Brasileira de Política Internacional,** v. 42, n. 1, p. 127-156, 1999.
COSTELLO, John; MONTGOMERY, Mark. How the National Cyber Director Position Is Going to Work: Frequently Asked Questions. **LAWFARE**, 2021. Disponível em: https://www.lawfaremedia.org/article/how-national-cyber-director-position-going-work-frequently-asked-questions. Acesso em: 12 set. 2024.

CUKIER, Kenneth Neil; MAYER-SCHÖNBERGER, Viktor. The rise of big data. ***Foreign Affairs***, 1 abr. 2013. Disponível em: https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data. Acesso em: 15 dez. 2024.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Vocabulary**. 2024. Disponível em: <https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary>. Acesso em: 20 fev. 2024.

CYBERSPACE SOLARIUM COMMISSION. **About**. 2024. Disponível em: https://www.solarium.gov/about. Acesso em: 12 set. 2024.

DE LESPINOIS, J. La territorialisation du cyberespace: la fin de la mondialisation? **Prospective et stratégie**, v. 1, n. 8, p. 47-56, 2017.

DEIBERT, R. Cyber-Security. *In*: CAVELTY, Myriam Dunn; BALZACQ, Thierry. (edit). **Routledge Handbook of Security Studies**. 2. ed. Nova York: Routledge, 2016.

DEIBERT, R. Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. **Journal of Military and Strategic Studies**. 29 out. 2018.

DEIBERT, R. The geopolitics of cyberspace after Snowden. **Current History**, v. 114, n. 768, 2015.

Department of Commerce. **Computer and Internet Use in the United States**: 2003. Disponível em: < https://www.census.gov/content/dam/Census/library/publications/2005/demo/p23-208.pdf> . Acesso em: 15 de dez. 2024.

DEPARTMENT OF DEFENSE. Cybercom's Partneship With NSA Helped Secure U.S. Elections, General Says. 2021. Disponível em: < https://www.defense.gov/News/News-Stories/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/>. Acesso em: 05 de dez. 2024.

DEPARTMENT OF DEFENSE. **Quadrennial Defense Review Report**. Washington, D.C.: U.S. Department of Defense, 2010. Disponível em:

<https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf>. Acesso em: 11 de jul, 2024.

DEPARTMENT OF HOMELAND SECURITY. **Budget-in-Brief: Fiscal Year 2023**. Washington, D.C.: Department of Homeland Security, 2023. Disponível em: https://www.dhs.gov. Acesso em: 12 de set. 2024.

DEPARTMENT OF HOMELAND SECURITY. **Budget-in-Brief: Fiscal Year 2022**. Washington, D.C.: Department of Homeland Security, 2023. Disponível em: https://www.dhs.gov. Acesso em: 12 de set. 2024.

DEPARTMENT OF HOMELAND SECURITY. **Budget-in-Brief: Fiscal Year 2021**. Washington, D.C.: Department of Homeland Security, 2023. Disponível em: https://www.dhs.gov. Acesso em: 12 de set. 2024.

DEPARTMENT OF HOMELAND SECURITY. ***Organizational Chart***. 2023. Disponível em: https://www.dhs.gov/organizational-chart. Acesso em: 9 jul. 2024.

DEPARTMENT OF HOMELAND SECURITY. Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector. 2017. Disponível em: < https://www.dhs.gov/archive/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>. Acesso em: 05 de dez. 2024.

DEPARTMENT OF JUSTICE (DOJ). **About CCIPS**. 2024a. Disponível em: https://www.justice.gov/criminal/criminal-ccips/about-ccips. Acesso em: 9 jul. 2024.

DEPARTMENT OF JUSTICE (DOJ). **Agencies Chart Map**. 2023. Disponível em: https://www.justice.gov/agencies/chart/map. Acesso em: 9 jul. 2024.

DEPARTMENT OF JUSTICE (DOJ). **Cybersecurity Unit**. 2024b. Disponível em: https://www.justice.gov/criminal/criminal-ccips/cybersecurity-unit. Acesso em: 6 ago. 2024.

DEPPA, Catherine S. U.S. Cyber Command: An Overview. **American Intelligence Journal**, v. 34, n. 1, p. 12-15, 2017. Disponível em: https://www.jstor.org/stable/26497111. Acesso em: 22 jul. 2024.

DEPPISH, Breanne. **DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump.** Politico, 2019. Disponível em: <https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149>. Acesso em: 10 jul. 2024.

DEVANNY, J. 'Madman Theory' or 'Persistent Engagement'? The Coherence of US Cyber Strategy under Trump. **Journal of Applied Security Research**, v. 17, n. 3, p. 282–309, 3 jul. 2022.

DEVANNY, J.; GOLDONI, L. R. F.; MEDEIROS, B. P. The rise of cyber power in Brazil. **Revista Brasileira de Política Internacional**, v. 65, n. 1, p. e013, 2022.

DEVANNY, J.; GOLDONI, L.; MEDEIROS, B. Strategy in an Uncertain Domain: Threat and Response in Cyberspace. **Journal of Strategic Security**, v. 15, n. 2, p. 34–47, jul. 2022.

DOUZET, F.; TAILLAT, S**.** Prepping for long-term competition? U.S. leadership in cyberspace from Trump to Biden. In: STRICOF, M.; VAGNOUX, I. (org.). ***U.S. leadership in a world of uncertainties***. Cham: Palgrave Macmillan, 2022. p. 213-234. (Studies of the Americas). Disponível em: https://doi.org/10.1007/978-3-031-10260-8_12. Acesso em: 13 jan. 2025.

DOUZET, Frédérick; DESFORGES, Alix; LIMONIER, Kevin**. Géopolitique du cyberespace : « territoire », frontières et conflits.** In: CIST2014 - Fronts et frontières des sciences du territoire. Paris, França: Collège international des sciences du territoire (CIST), mar. 2014. p. 173-178. Disponível em<https://hal.science/hal-01353455>. Acesso em: 20 de fev. 2024

ELIASON, William T. An interview with Michael S. Rogers. **Joint Force Quarterly**, n. 80, 2016. Disponível em: https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643105/an-interview-with-michael-s-rogers/. Acesso em: 9 jul. 2024.

ESTADOS UNIDOS. *A Declaration for the Future of the Internet.* Washington, D.C.: U.S. Department of State, 2022. Disponível em: < https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf>. Acesso em: 27 de dez. 2024.

ESTADOS UNIDOS. A *National Cybersecurity Strategy*. White house. Washington, 2023. Acesso em: 27 de dez. 2024.

ESTADOS UNIDOS. Cyber Command. **History**. 2024. Disponível em: https://www.cybercom.mil/About/History/. Acesso em: 9 jul. 2024.

ESTADOS UNIDOS. **Cybersecurity and Infrastructure Security Agency Act of 2018**. Washington, D.C.: U.S. Government Publishing Office, 2018. Disponível em: https://www.govinfo.gov/content/pkg/COMPS-15296/pdf/COMPS-15296.pdf. Acesso em: 9 jul. 2024.

ESTADOS UNIDOS. **DOD Dictionary of Military and Associated Terms.** 2021. Disponível em: < https://irp.fas.org/doddir/dod/dictionary.pdf>. Acesso em: 13 de mar. 2024

ESTADOS UNIDOS. **Executive Order 13228 of October 8, 2001: Establishing the Office of Homeland Security and the Homeland Security Council**. Federal Register, v. 66, n. 196, p. 51812-51817, 10 out. 2001a. Disponível em: https://www.govinfo.gov/content/pkg/FR-2001-10-10/pdf/01-25677.pdf. Acesso em: 2 jul. 2024.

ESTADOS UNIDOS. **Executive Order 13231 of October 16, 2001 - Critical Infrastructure Protection in the Information Age**. Federal Register, v. 66, n. 202, p. 53063-53071, 18 out. 2001b. Disponível em: https://www.federalregister.gov/documents/2001/10/18/01-26509/critical-infrastructure-protection-in-the-information-age. Acesso em: 03 jul. 2024.

ESTADOS UNIDOS. **Homeland Security Act of 2002**. Public Law 107-296, 25 nov. 2002. Disponível em: https://www.congress.gov/107/plaws/publ296/PLAW-107publ296.pdf. Acesso em: 2 de dez. 2024

ESTADOS UNIDOS. ***International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World***. White House. Washington, 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 20 dez. 2024.

ESTADOS UNIDOS. ***International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World***. White House. Washington, 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 20 dez. 2024.

ESTADOS UNIDOS. **National Cyber Strategy of the United States of America**. Washington, D.C. 2018. Disponível em: < https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf >. Acesso em: 15 de fev, 2024.

ESTADOS UNIDOS. *National Security Strategy of the United States of America*. White House. Washington, 2017. Disponível em: < https://history.defense.gov/Portals/70/Documents/nss/NSS2017.pdf?ver=CnFwURrw09pJ0q5EogFpwg%3d%3d>. Acesso em: 20 de dez. 2024.

ESTADOS UNIDOS. ***National security Strategy***. White House. Washington, 2015. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf. Acesso em: 20 dez. 2024.

ESTADOS UNIDOS. **National Strategy For Homeland Security**. Washington, D.C. 2002. Disponível em: < https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf>. Acesso em: 15 de fev, 2024.

ESTADOS UNIDOS. Presidente (2009 – 2017: Barack Obama). **Remarks by the President on Cybersecurity and Consumer Protection Summit**. Stanford, 13 fev. 2015. Disponível em: <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks president-cybersecurity-and-consumer-protection-summit.>. Acesso em: 15 de fev, 2024.

ESTADOS UNIDOS. *Remarks at the Simon Wiesenthal Center in Los Angeles*. Santa Barbara: The American Presidency Project, 06 mar. 2000. Disponível em: https://www.presidency.ucsb.edu/documents/remarks-the-simon-wiesenthal-center-los-angeles. Acesso em: 20 dez. 2024.

ESTADOS UNIDOS. Statement from President Biden on Addressing National Security Risks to the U.S. Auto Industry. 2024. Disponível em: <https://www.whitehouse.gov/briefing-room/statements-

releases/2024/02/29/statement-from-president-biden-on-addressing-national-security-risks-to-the-u-s-auto-industry/>. Acesso em: 06 de mar. 2024

ESTADOS UNIDOS. The National Defense Strategy of the United States of America. 2005. DIsponível em: <http://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=2014-06-25-124535143.> Acesos em: 13 de mar, 2024.

ESTADOS UNIDOS. The National Strategy to Secure Cyberspace. Washington, D.C. 2003. Disponível em: < https://nsarchive.gwu.edu/document/21412-document-16>. Acesso em: 15 de dez. 2024.

ESTADOS UNIDOS. The National Strategy to Secure Cyberspace. Washington, D.C. 2003. Disponível em: < https://nsarchive.gwu.edu/document/21412-document-16>. Acesso em: 15 de dez. 2024.

ESTADOS UNIDOS. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001**. Public Law no. 107-56, 26 out. 2001. Disponível em: </https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em: 13 mar. 2024.

FEDERAL BUREAL OF INVESTIGATION (FBI). **Internet Crime Report.** 2023. Disponível em: < https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf>. Acesso em: 9 jul. 2024.

FEDERAL BUREAL OF INVESTIGATION (FBI). Meet the Cyber Action Team. 2023b. Disponível em: < https://www.fbi.gov/news/stories/meet-the-cyber-action-team>. Acesso em: 05 de dez. 2024.

FEDERAL BUREAU OF INVESTIGATION (FBI). **Cyber Crime**. 2024b. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 9 jul. 2024.

FEDERAL BUREAU OF INVESTIGATION (FBI). **What is the FBI**. 2024a. Disponível em: <https://www.fbi.gov/about/faqs/what-is-the-fbi>. Acesso em: 9 jul. 2024.

FERREIRA NETO ,W.B. Territorializando o “novo” e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder. **Revista Brasileira de Estudos Estratégicos**, v. 1, n. 4, 12 de dez 2012.

FERREIRA NETO, W. B. Território: da dimensão terrestre ao ciberespaço - espaço, poder, segurança e oportunidades econômicas. **Revista Agulhas Negras**, v. 2, n. 2, p. 88-99, 3 dez. 2018.

FERREIRA NETO, Walfredo Bento. **Uma Estratégia Nacional de Defesa para Além da Guerra: Geopolítica Cibernética e Seu Transbordamento Econômico-Tecnológico no Brasil (2008-2018)**. 2020. Tese (Doutorado em Economia Política Internacional) – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020.

FIREEYE. Evasive Attacker Leverages SolarWinds Supply Chain Compromises with SUNBURST Backdoor. 2020. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor/. Acesso em: 12 set. 2024.

FISCHERKELLER, M. P.; GOLDMAN, E. O.; HARKNETT, R. J. **Cyber persistence theory: redefining national security in cyberspace**. New York: Oxford University Press, 2022.

FLEET CYBER COMMAND (FCC). **Mission and Vision**. Disponível em: https://www.fcc.navy.mil/ABOUT-US/MISSION-VISION/. Acesso em: 9 jul. 2024.

GIORDANO, Vitória Rangel; BOSSO, João Paulo Cavazzani. A Estruturação da Defesa e da Segurança Cibernética a partir do mapeamento documental dos Estados Unidos da América. *In*: Ayres Pinto, DJ et al. **A geopolítica das estratégias em defesa cibernética: como EUA, China, Rússia e Israel protegem seu ciberespaço**. Rio de Janeiro: Editora Alpheratz, p. 15-46, 2021.

GOTTMANN, J. A evolução do conceito de território. **Boletim Campineiro de Geografia**, v. 2, n. 3, p. 523–545, 31 dez. 2012.

Government Accountability Office. **Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure**. Washington, D.C.: GAO, 2008. Disponível em: <https://www.gao.gov/assets/gao-08-1157t.pdf>. Acesso em: 9 jul. 2024.

GREENWALD, Gleen. **Sem lugar para se esconder.** Rio de Janeiro: Editora Primeira Pessoa, 2014.

HAESBAERT, R. **O mito da desterritorialização: do "fim dos territórias" à multiterritorialidade**. Rio de Janeiro: Bertrand Brasil, 2004.

HARRIS, S. **@war: the rise of cyber warfare**. London: Headline, 2014.

HOFMANOVÁ, Lucie. **Cyber Security in the United States of America: Assessing the Role of the Department of Homeland Security**. 2019. Dissertação (Mestrado) – Charles University, Faculty of Social Sciences, Institute of Political Studies, Department of International Relations, Praha, 2019.

HOLLIS, D. Cyberwarfare Case Study: Georgia 2008. Small Wars Journal, 6 de janeiro, 2011.

IKENBERRY, G. John. The plot against American foreign policy: Can the liberal order survive. **Foreign Aff.**, v. 96, p. 2, 2017.

INGLIS, J. Chris. **Testimony of the National Cyber Director**. Committee on Homeland Security, United States House of Representatives, 03 nov. 2021. Disponível em: <https://democrats-homeland.house.gov/imo/media/doc/inglis_testimony_full_110321.pdf>. Acesso em: 12 set. 2024.

INTERNET CRIME COMPLAINT CENTER (IC3). **2021 Internet Crime Report**. 2021. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. Acesso em: 9 jul. 2024.

INTERNET CRIME COMPLAINT CENTER (IC3). **2023 Internet Crime Report**. 2023. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. Acesso em: 9 jul. 2024.

ISRAEL, C. B. Território, Jurisdição e Ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet. **GEOUSP Espaço e Tempo (Online)**, v. 24, n. 1, p. 69–82, 18 nov. 2019.

JAPARIDZE, T. Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? *In*: BERGHOFER, J. et al. (Eds.). **The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network**. Cham: Springer International Publishing, 2023. p. 209–225.

JESUS, D. S. V. D. O baile do monstro: o mito da paz de vestfália na história das relações internacionais modernas. **História (São Paulo)**, v. 29, n. 2, p. 221–232, dez. 2010.

KELLNER, Douglas. Como mapear o presente a partir do futuro: de Baudrillard ao cyberpunk. In: Kellner, D. **A cultura da mídia**. Bauru: EDUSC, 2001. p.377-419.

KRAFT, M.; MARKS, E. **U.S. government counterterrorism: a guide to who does what**. Boca Raton, Fla.: CRC Press, 2012.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. **Cyberpower and National Security**, v.30,2009.

LALLIE, H. S. et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. **Computers & Security**, v. 105, p. 102248, jun. 2021.

LAMBACH, D. The Territorialization of Cyberspace*. **International Studies Review**, v. 22, n. 3, p. 482–506, 1 set. 2020.

Lasswell, H. The theory of political propaganda. ***The American Political Science Review***, v. 21, n. 3, p. 627-631, 1927

LIBICKI, M. C. **Cyberdeterrence and cyberwar**. Rand Corporation, 2009

LINDSAY, J. R. Stuxnet and the Limits of Cyber Warfare. **Security Studies**, v. 22, n. 3, p. 365–404, jul. 2013.

MABEE, B. Re-imagining the Borders of US Security after 9/11: Securitisation, Risk, and the Creation of the Department of Homeland Security. **Globalizations**, v. 4, n. 3, p. 385–397, set. 2007.

MACRI, Kate. SolarWinds Hack Shows Why We Need a National Cyber Director. **GovCIO Media & Research**, 2021. Disponível em: https://govciomedia.com/solarwinds-hack-shows-why-we-need-a-national-cyber-director/. Acesso em: 05 set. 2024.

MAIER**, F.** *De Obama a Trump: o contínuo da política cibernética estadunidense*. **Caderno de Relações Internacionais**, [S. l.], v. 10, n. 18, 2019. DOI: 10.22293/2179-1376.v10i18.1034. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/relacoesinternacionais/article/view/1034. Acesso em: 13 dez. 2024.

MARINE FORCES CYBER COMMAND (MARFORCYBER). **About**. Disponível em: https://www.marforcyber.marines.mil/About/. Acesso em: 9 jul. 2024.

MARTELLE, Michael. Preparing for Computer Network Operations: USCYBERCOM Documents Trace the Path to an Operational Cyber Force. **National Security Archive**, 3 maio 2019. Disponível em: https://nsarchive.gwu.edu/news/cyber-vault/2019-05-03/preparing-computer-network-operations-uscybercom-documents-trace-path-operational-cyber-force. Acesso em: 9 jul. 2024.

MATTOS, Carlos de Meira. **Geopolítica e Teoria de Fronteiras: fronteiras do Brasil.** Rio de Janeiro: Biblioteca do Exército, 1990.

Medeiros, B. P**. Ciberespaço e relações internacionais: rumo a construção de um novo paradigma?** 2019. Dissertação (Mestrado em Ciências Militares) – Instituto Meira Mattos, Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024. MEDEIROS, B. P. et al. O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidades. **Revista de Administração Pública**, v. 54, n. 4, p. 650–662, ago. 2020.

MEDEIROS, B. P.; GOLDONI, L. R. F. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, v. 42, n. 1, p. 31–54, abr. 2020.

MEDEIROS, Breno Pauli**. Cyber Power: Challenges (and Opportunities) for Military Power**. 2024. Tese (Doutorado em Ciências Militares) – Instituto Meira Mattos, Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024.

MOROZOV, Evgeny**. Big Tech: a ascensão dos dados e a morte da política**. Tradução de Claudio Marcondes. São Paulo: Editora Ubu, 2018.

MUSSO, P. A filosofia da Rede. In: PARENTE, A**. Tramas da rede: novas dimensões filosóficas, estéticas e políticas da comunicação**. Porto Alegre: Sulina, 2004

NAKASONE, Paul M. A cyber force for persistent operations.**Joint force quarterly**, v. 92, n. 1, p. 10-4, 2019.

NATIONAL SECURITY AGENCY. ST-09-002 Working Draft. Office of the Inspector General. 24 de março 2009. Disponível em União Americana de Liberdades Civis, em: https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf Acesso: 05 dez. 2024.

NAUGHTON, J. The evolution of the Internet: from military experiment to General Purpose Technology. **Journal of Cyber Policy**, v. 1, n. 1, p. 5–28, 2 jan. 2016.
NIC.BR. **O que é defacement?** Disponível em: <https://www.nic.br/noticia/na-midia/o-que-e-defacement/>. Acesso em: 20 de fev. 2024.

NIELSEN, S. The Role of the U.S. Military in Cyberspace. **Journal of Information Warfare**, v. 15, n. 2, p. 27–38, 2016.

NING, H. **A brief history of cyberspace**. First edition ed. Place of publication not identified: Auerbach Publications, 2022.

NISSENBAUM, H. Where Computer Security Meets National Security. **Ethics and Information Technology**, v. 7, n. 2, p. 61–73, jun. 2005.

NYE, J. S. **The future of power**. 1st ed ed. New York: Public Affairs, 2011.

O'NEIL, W. D. Cyberspace and Infrastructure. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L, K. **Cyberpower and National Security**, p. 113-146, 2009.

OTHON, Adriano. Da revolução behaviorista ao contributo de David Easton: Breve ensaio epistêmico-biográfico. **Observatório Político**, v. 103, 2021.

PECEQUILO, C. S. **Os Estados Unidos e o século XXI**. Rio de Janeiro. Elsevier, 2016.

PECEQUILO, Cristina Soreanu; JUNIOR, Franciso Luiz Marzinotto. Os Estados Unidos e a projeção de poder multidimensional: a Guerra Fria e o papel da Defensa Advanced Research Project Aency (1958-1989). **Oikos,** v. 21, n. 1, 2022.
PECEQUILO, Cristina; MARZINOTTO JR., Francisco Luiz. O poder dos Estados Unidos e as multinacionais tecnológicas na era digital: uma análise da oligopolização nos governos Obama e Trump (2009/2021). ***AUSTRAL: Brazilian Journal of Strategy & International Relations***, v. 11, n. 21, 2022.

PETROSYAN, Ani. *United States internet penetration 2000-2024*. **Statista**, 20 set. 2024. Disponível em: https://www.statista.com/statistics/209117/us-internet-penetration/#:~:text=As%20of%202024%2C%20approximately%2097.1,in%20the%20country%20went%20online. Acesso em: 20 dez. 2024.

PORTELA, L. S. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. **Revista Brasileira de Estudos de Defesa**, v. 5, n. 1, 2 abr. 2018.

RAFFESTIN, C. **Por Uma Geografia do poder**. Brasilia: Atica, 1993.

RATTRAY, G. J. An environmental approach to understanding cyberpower. **Cyberpower and National Security**, p. 253-274, 2009.

RID, T. Cyber War Will Not Take Place. **Journal of Strategic Studies**, v. 35, n. 1, p. 5–32, fev. 2012.

ROBERTS, J. **Transatlantic Tech Bridge: Digital Infrastructure and Subsea Cables, a US Perspective.** Istituto Affari Internazionali, 2024. Disponível em: <https://policycommons.net/artifacts/11754212/transatlantic-techbridge/12645436/>. Acesso em: 21 mar. 2024. CID: 20.500.12592/h189866.

ROCHA, Henrique Ribeiro da. **Governança Securitária do Ciberespaço: questões sobre Segurança e Defesa**. Dissertação (Mestrado em Ciências Militares) - Instituto Meira Mattos, Escola de Comando e Estado Maior do Exército, Rio de Janeiro, 2022

ROSENZWEIG, P. Turns out it is not 85 percent. **LawFare,** 2022. Disponível em: <https://www.lawfaremedia.org/article/turns-out-it-not-85-percent>. Acesso em: 15 de mar. 2024.

SACK, R. D. **Human territoriality: its theory and history**. Cambridge London New York New Rochelle Melbourne Sydney: Cambridge University Press, 1986.

SAINT-PIERRE, H. L.; GONÇALVES, L. J. C. Nem Revolução Militar (RM) nem Revolução em Assuntos Militares (RAM) apenas mudanças de longa duração condensadas na guerra pelo gênio militar. **Revista Brasileira de Estudos de Defesa**, v. 5, n. 2, 2 nov. 2018.

SAMPAIO, R. C. **Análise de conteúdo categorial: manual de aplicação**. Brasília, DF: Escola Nacional de Administração Pública - Enap, 2021.

Santos, S.M. Um povo eleito em uma terra prometida: o mito do destino manifesto e as raízes do nacionalismo norte-americano. ***Aedos***, v. 14, n. 32, p. 140-155, jul.–dez., 2022.

SCHMITT, M. N. (Ed.). **Tallinn manual 2.0 on the international law applicable to cyber operations.** Cambridge University Press, 2017.
SCHMITT, Michael N.; VIHUL, Liis. Proxy wars in cyberspace: the evolving international law of attribution. **Fletcher Sec. Rev**., v. 1, p. 53, 2014.

SCHREIER, M. **Qualitative content analysis in practice**. Los Angeles London New Dehli Singapore Washington DC: SAGE, 2012.

SHELDON, J. B. Deciphering cyberpower: Strategic purpose in peace and war. **Strategic Studies Quarterly**, v. 5, n. 2, p. 95-112, 2011.
SHERMAN, Mark. TikTok says it will ‘go dark’ unless it gets clarity from Biden following Supreme Court ruling. AP News, 18 jan. 2025. Disponível em: <https://apnews.com/article/supreme-court-tiktok-china-security-speech-166f7c794ee587d3385190f893e52777>. Acesso em: 18 jan. 2025.

SHERMAN, Mark. TikTok says it will ‘go dark’ unless it gets clarity from Biden following Supreme Court ruling. AP News, 18 jan. 2025. Disponível em: <https://apnews.com/article/supreme-court-tiktok-china-security-speech-166f7c794ee587d3385190f893e52777>. Acesso em: 18 jan. 2025

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

SOUZA, R. C. S. D.; OLIVEIRA, T. F. D. D.; PAULA, M. G. D. A Guerra Cibernética Russo-Ucraniana: os ataques russos às Infraestruturas Críticas ucranianas e possíveis lições para o Exército Brasileiro. **Coleção Meira Mattos**, v. 18, n. 61, p. 143–158, 2024.

SRNICEK, N. **Platform capitalism**. Reprinted ed. Cambridge Malden, MA: Polity, 2019.

STARKS, Tim. Biden's cybersecurity legacy: A big shift to private sector responsibility. **CyberScoop**, 2023. Disponível em: https://cyberscoop.com/bidens-cybersecurity-legacy-a-big-shift-to-private-sector-responsibility/. Acesso em: 12 set. 2024.

TANGREDI, S.J. From Global Commons to Territorial Seas: A Naval Analogy for the Nationalization of Cyberspace. **Military Cyber Affairs**, v. 3, n. 1, jun. 2018.

TARRY, Sarah. Deepening and Widening: An Analysis of Security Definitions in the 1990s. **Journal of military and strategic studies**, v. 2, n. 1, 1999.

TEN, C.-W.; MANIMARAN, G.; LIU, C.-C. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. **IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans**, v. 40, n. 4, p. 853–865, jul. 2010.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**, 2017. Disponível em: < https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 22 de fev. 2024

TIKK-RINGAS, E.; KASKA, K.; VIHUL, L. **International cyber incidents: legal considerations**. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.

TURTON, William; MANSON, Katrina. Joe Biden's Cybersecurity Dream Team Roiled as Chris Inglis Resigns. **Bloomberg**, 03 abr. 2023. Disponível em: https://www.bloomberg.com/news/articles/2023-04-03/joe-biden-s-cybersecurity-dream-team-roiled-as-chris-inglis-resigns. Acesso em: 12 set. 2024.

UNITED STATES NAVAL INSTITUTE. **Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks.** Disponível em: < https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks>. Acesso em: 05 de dez, 2024.

UNITED STATES SECRET SERVICE. **150 Years**. 2024. Disponível em: https://www.secretservice.gov/about/history/150-years. Acesso em: 12 jul. 2024

UNITED STATES SECRET SERVICE. About us. 2024a. Disponível em: https://www.secretservice.gov/about/overview. Acesso em: 5 de dez. 2024.

UNITED STATES SECRET SERVICE. **Secret Service Announces the Creation of the Cyber Fraud Task Force**. 2020. Disponível em: https://www.secretservice.gov/newsroom/releases/2020/07/secret-service-announces-creation-cyber-fraud-task-force. Acesso em: 12 jul. 2024.

VENTRE, D. 2012. **Ciberguerra.** In: Academia General Militar. Seguridad global y potências emergentes em um mundo multipolar. XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza.

VENTRE, Daniel. O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras. **Dilemas-Revista de Estudos de Conflito e Controle Social**, n. Esp. 3, p. 75-96, 2019.

VIOTTI, P. R.; KAUPPI, M. V. **International relations theory**. 5th ed ed. Boston: Longman, 2012.

WALT, S. M. The Renaissance of Security Studies. **International Studies Quarterly**, v. 35, n. 2, p. 211–239, 1 jun. 1991.

WARBURTON, D. **2020 phishing and Fraud Report**. Disponível em: <https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report>. Acesso em: 12 ago. 2024.

WARNER, M. Cybersecurity: A Pre-history. **Intelligence and National Security**, v. 27, n. 5, p. 781–799, out. 2012.

WOODCOCK, BILL. On Internet, Brazil is beating US at its own game. Aljazeera America, 2013. Disponível em: <http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html>. Acesso em: 22 de fev. 2024

ZHANG, X. A geography of the internet in China. *In*: **Geographies of the Internet**. London; New York: Routledge, Taylor & Francis Group, 2021. p. 214 238.

ZUBOFF, Shoshana. ***A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder***. Tradução de George Schlesinger. Rio de Janeiro: Editora Intrínseca, 2021.