UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE ESTUDOS ESTRATÉGICOS
MBA EM ESTUDOS ESTRATÉGICOS
E RELAÇÕES INTERNACIONAIS
TURMA CIASC 2023

A COOPERAÇÃO INTERNACIONAL NA DEFESA CIBERNÉTICA BRASILEIRA NO SÉCULO XXI

FILIPE AMORIM DA SILVA

Niterói - RJ

2023

FILIPE AMORIM DA SILVA

A COOPERAÇÃO INTERNACIONAL NA DEFESA CIBERNÉTICA DO SÉCULO XXI

Trabalho de Conclusão de Curso de MBA apresentado ao Instituto de Estudos Estratégicos da Universidade Federal Fluminense com parceria ao Centro de Instrução Sylvio de Camargo (Marinho do Brasil) como requisito parcial para a obtenção do título de MBA em Relações Internacionais.

Orientadora: Profa. Dra. Raquel dos Santos Missagia

Niterói – RJ
2023

Folha de Aprovação de Trabalho de Conclusão de Curso em Relações Internacionais (Monografia)

Título do Trabalho: A cooperação internacional na defesa cibernética do século xxi

Aluno: Filipe Amorim da Silva

Avaliadores

_____

Avaliador 01: Profa. Dra. Erika Kubik

_____

Avaliador 02: Profa. Dra. Raquel dos Santos Missagia (orientadora)

Notas dos Avaliadores	
Nota 1	
Nota 2	

RESUMO

No contexto do século XXI, a defesa cibernética do Brasil enfrenta desafios únicos impostos pela evolução do ciberespaço. Este trabalho investiga a crescente complexidade das ameaças cibernéticas e a imperativa cooperação internacional como meios para fortalecer a resiliência nacional. Os fundamentos da defesa cibernética são explorados, destacando a importância de uma compreensão abrangente do espaço cibernético e das estratégias defensivas. O TCC discute as iniciativas de cooperação e compartilhamento de informações, ressaltando a necessidade de uma abordagem colaborativa frente à natureza transnacional das ameaças digitais. As políticas cibernéticas são examinadas à luz dos princípios liberais das Relações Internacionais, argumentando que a cooperação é vital para o desenvolvimento de uma infraestrutura robusta e segura. Casos recentes de cibercrime são analisados, enfatizando como o Brasil pode aprender com experiências internacionais para melhorar sua postura de defesa. O papel do compartilhamento de inteligência e as parcerias estratégicas são destacadas como fundamentais para antecipar e neutralizar risco cibernético em um mundo interconectado.

Palavras-chave: Defesa cibernética; Segurança cibernética; ameaças cibernéticas; cooperação internacional; espaço cibernético.

ABSTRACT

In the 21st century, Brazil's cyber defense is challenged by the evolving complexities of cyberspace. This study delves into the intricate nature of cyber threats and the imperative of international cooperation to bolster national resilience. It examines the foundations of cyber defense, emphasizing the significance of comprehensively understanding cyberspace and defensive strategies. The thesis discusses cooperation initiatives and information sharing, highlighting the necessity of collaborative approaches to the transnational nature of digital threats. Cybersecurity policies are scrutinized through the lens of liberal International Relations principles, arguing for cooperation as essential in building robust and secure infrastructure. Recent cybercrime incidents are analyzed, underscoring how Brazil can leverage international experiences to enhance its defense posture. The roles of intelligence sharing and strategic partnerships are underscored as crucial for anticipating and mitigating cyber risk in an interconnected world.

Keywords: Cyber Defense; Cybersecurity; cyber threats; international cooperation; cyberspace.

SUMÁRIO

INTRODUÇÃO 6

1 FUNDAMENTOS DA DEFESA CIBERNÉTICA 10

1.1 Introdução 10

1.2 A Natureza Transfronteiriça do Espaço Cibernético 10

1.3 Distinção entre Segurança e Defesa Cibernética 12

1.4 Tipos de Ameaças Cibernéticas 13

1.5 Motivações por Trás dos Ataques Cibernéticos 14

1.6 Infraestruturas críticas e Ataques cibernéticos 16

1.7 O que é governança de cibersegurança? 17

1.8 Estruturação do setor de cyber defesa e estabelecimento da política de segurança da informação 19

2 COOPERAÇÃO INTERNACIONAL EM DEFESA CIBERNÉTICA 28

2.1 Cyber Security for National Defense Summit 2009 30

2.2 Intercâmbio de informações sobre cibernética nos EUA 31

2.3 I Seminário Internacional de Defesa Cibernética 32

2.4 Visita de comitiva à República Popular da China 33

2.5 Operação Amazônia (2011) 34

2.6 Jornadas de Trabalho de Defesa Cibernética 35

2.7 Caso Snowden em 2013 e seus impactos na cooperação Brasil Estados Unidos em matéria de segurança e defesa cibernética 36

2.8 A cooperação entre o Brasil e os Estados Unidos no campo da segurança cibernética pós o caso Snowden 38

2.9 Participação brasileira no Locked Shields 2022 39

3 O TRATAMENTO DE OPERAÇÕES CIBERNÉTICAS NO CONTEXTO DO DIREITO INTERNACIONAL 44

3.1 Jurisdição e Soberania 44

3.1.1 Abordagem da soberania cibernética 44

3.1.2 Dilemas da jurisdição 45

3.2 Aplicação do Direito Internacional nas Operações Cibernéticas Estatais e as Perspectivas dos Estados Membros da Organização dos Estados Americanos (OEA) 46

CONCLUSÃO 48

REFERÊNCIAS 49

INTRODUÇÃO

No século XXI, a rápida expansão da interconexão digital e a popularização da tecnologia mudaram o cenário da estratégia de defesa e geraram um novo espaço geográfico: o ciberespaço. Nesse ecossistema digital, de acordo com Portela (2018, p. 142), a busca por mais espaço não é o principal fator de disputas, mas as informações, com isso o controle da informação se tornou um elemento essencial nas estratégias de poder, moldando as relações entre Estados e influenciando a defesa estratégica. O ciberespaço está em constante transformação, com uma crescente complexidade e vulnerabilidades sistêmicas cada vez mais sofisticadas, diante disso a cooperação internacional emerge como uma ferramenta indispensável para fortalecer as defesas cibernéticas do Brasil.

Esse cenário é agravado pelo fato de que mais da metade da população mundial está atualmente conectada à internet[1], sendo que grande parte das atividades online ocorre por meio de smartphones. No contexto brasileiro, essa realidade é evidente, com 90% dos lares brasileiros tendo acesso à internet[2].

A pergunta que deve ser considerada é: como o Estado brasileiro respondeu aos desafios de cibersegurança? O Brasil ocupa a 18ª posição no mundo no Índice Global de Cibersegurança[3] da União Internacional de Telecomunicações e o 3º lugar nas Américas, atrás apenas dos Estados Unidos e do Canadá.

Nos últimos anos, o cenário de segurança cibernética no Brasil tem sido marcado por avanços tecnológicos significativos, como a implementação do PIX em 2020 e o desenvolvimento da nova moeda digital brasileira, o DREX com o seu teste na plataforma-piloto pronto para operações a partir de março de 2023 até o final de 2024[4]. Essas inovações financeiras prometem agilizar transações, simplificar pagamentos e fomentar a inclusão financeira, mas também introduzem uma série de desafios complexos na área de defesa cibernética.

---

1 INSPER. "Mundo se Aproxima da Marca de 5 Bilhões de Usuários de Internet, 63% da População." Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao. Acesso em: 12 ago. 2023.

2CASA CIVIL. "90% dos lares brasileiros já têm acesso à internet no Brasil, aponta pesquisa." Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acesso em: 12 ago. 2023.

3 UIT (União Internacional de Telecomunicações). "Global Cybersecurity Index 2021." Disponível em: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E. Acesso em: 12 ago. 2023.

4 Banco Central do Brasil. "DREX - Moeda Digital Brasileira." Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/drex. Acesso em: 12 ago. 2023.

De acordo com o Relatório de Riscos Globais 2023[5] do Fórum Econômico Mundial, o cibercrime generalizado e a insegurança cibernética estão entre os 10 maiores riscos globais em termos de impacto social, econômico e político. O aumento do trabalho remoto e/ou a falta de conhecimento sobre boas práticas de segurança podem resultar na criação de vulnerabilidades em sistemas públicos e privados, expondo-os a novos tipos de ataques. Esse foi o caso do ataque ao Superior Tribunal de Justiça do Brasil (STJ) em novembro de 2020[6]. O ransomware criptografou todos os arquivos no segundo tribunal mais importante do sistema judicial brasileiro, evidenciando as deficiências dos sistemas e a falta de preparo da Administração Pública Federal para responder a esses ataques.

Outro incidente significativo recente veio à tona no depoimento do dia de Walter Delgatti Neto na CPMI dos Atos de 8 de janeiro 2023, relacionado ao ataque hacker ao Conselho Nacional de Justiça (CNJ), nesse ataque ele supostamente inseriu de forma ilegal alvarás de soltura e um falso mandado de prisão contra o ministro Alexandre de Moraes no sistema do CNJ[7].

No enfrentamento desses desafios, a cooperação internacional na defesa cibernética desempenha um papel crítico para o Brasil. A natureza transnacional das ameaças cibernéticas exige uma abordagem colaborativa, uma vez que os atores maliciosos podem operar a partir de qualquer ponto do globo. A troca de informações, compartilhamento de melhores práticas e coordenação de ações conjuntas permitem que o Brasil esteja à altura das ameaças cibernéticas de maneira mais eficaz, aproveitando o conhecimento e a experiência acumulados por outras nações.

Apesar da clara necessidade de cooperação, a colaboração internacional em defesa cibernética não é isenta de desafios. Questões de soberania, desconfiança e diferenças culturais e regulatórias podem dificultar a troca de informações sensíveis. Além disso, a rápida evolução das tecnologias e das ameaças cibernéticas requer uma flexibilidade constante nas estratégias de cooperação.

---

5 WEF. Global Risks Report. World Economic Forum. 2023. Disponível em: https://www.zurich.com.br/-/media/project/zwp/brazil/docs/noticias/2023/relatorio-de-riscos-globais-2023.pdf?rev=c0a0f1b8163f4785bb516ee48074add5&hash=04323AABA2A3FBF398C8DD39A381EA38 . Acesso em: 12 ago. 2023.

6 MARIN, J. “Ataque hacker ao STJ é o pior da história do Brasil”. TecMundo. 2020.Disponível em: https://www.tecmundo.com.br/seguranca/ 206233-ataque-hacker-ter-atingido-stj-pf-investiga.htm. Acesso em: 12 ago. 2023.

7 Agência Câmara de Notícias. "CPMI do 8 de Janeiro ouve hacker que invadiu sistema do Conselho Nacional de Justiça. Disponível em: https://www.camara.leg.br/noticias/984564-comissao-dos-atos-de-8-de-janeiro-ouve-hacker-da-vaza-jato/. Acesso em: 17 ago. 2023.

Este trabalho argumenta que a cooperação internacional é um elemento fundamental para fortalecer a defesa cibernética do Brasil. Através da participação ativa em iniciativas multilaterais, acordos bilaterais e fóruns de compartilhamento de informações, o Brasil pode adotar uma abordagem mais abrangente e eficaz para proteger seus ativos digitais e infraestrutura crítica. Nesse sentido, é possível estabelecer um diálogo próximo com a teoria liberal das Relações Internacionais, que caminha nessa direção de identificar como a cooperação internacional é uma ferramenta importante para os Estados. A metodologia utilizada é exploratória, com revisão de literatura existente sobre o tema.

Para atingir o objetivo de explorar a importância da cooperação internacional na defesa cibernética do Brasil, este TCC será estruturado em três capítulos. No primeiro capítulo são abordados alguns elementos que constituem a defesa cibernética. Nesse espaço objetiva-se caracterizar a defesa cibernética a partir de conceitos basilares. Adicionalmente, é demonstrado como a proteção de sistemas, redes e dados contra ameaças digitais envolve a implementação de medidas estratégicas e técnicas que visam identificar, prevenir e responder a ataques cibernéticos.

O segundo capítulo trata da cooperação internacional em defesa cibernética a partir dos principais acontecimentos que ocorreram no início do século XXI. Nesse tópico são descritas iniciativas que o Brasil promoveu ou aderiu para o fortalecimento do desenvolvimento da cooperação internacional em defesa e segurança cibernética.

Por fim, no terceiro capítulo é caracterizado o debate sobre as operações cibernéticas no contexto do direito internacional e ciberespaço. Nesse sentido, são caracterizados como os dilemas de jurisdição surgem devido à natureza transnacional da internet, desafiando conceitos tradicionais de soberania e jurisdição dos Estados. A soberania cibernética é interpretada de forma variada, com algumas nações adotando abordagens mais restritivas e controladas, enquanto outras defendem um ciberespaço mais aberto. A aplicação do direito internacional nas operações cibernéticas estatais envolve quatro pilares: soberania, uso da força, direito internacional humanitário e direitos humanos, mas a falta de consenso global sobre o que constitui um uso da força no ciberespaço complica a governança cibernética. Além disso, são descritas as perspectivas dos Estados membros da OEA que variam, refletindo suas políticas internas, capacidades cibernéticas e estratégias, embora deem ênfase à cooperação internacional e regional para enfrentar os desafios de segurança cibernética e promover um ciberespaço seguro e estável.

O objetivo deste trabalho é analisar como a cooperação internacional pode fortalecer a defesa cibernética do Brasil, considerando as particularidades do cenário nacional e as

implicações das ameaças cibernéticas transnacionais. As seguintes questões de pesquisa serão abordadas:

Quais são os principais desafios cibernéticos que o Brasil enfrenta no século XXI? Como a cooperação internacional pode contribuir para melhorar a defesa cibernética do Brasil? Quais são os casos de cooperação internacional em defesa cibernética que podem servir de inspiração para as estratégias do Brasil?

Ao responder a essas questões, este estudo visa fornecer subsídios para a formulação de políticas cibernéticas mais robustas e eficazes para o Brasil, em colaboração com a comunidade internacional.

1 FUNDAMENTOS DA DEFESA CIBERNÉTICA

1.1 Introdução

O termo "espaço cibernético," conforme definido por Richard A. Clarke (2010), refere-se ao amplo conjunto de tecnologias que compõem a interconexão global de sistemas computacionais. Este espaço não se limita à infraestrutura da Internet, mas abrange todas as entidades, processos e dados dependentes e controlados por essas redes interconectadas. É crucial não confundir o "espaço cibernético" com a "Internet", pois esta última representa apenas uma parte acessível desse espaço cibernético expandido. Clarke destaca que o conceito de espaço cibernético transcende as fronteiras da Internet, englobando uma complexa rede de sistemas, dispositivos e infraestruturas interdependentes, estabelecendo um cenário vasto e complexo de interações digitais e ameaças potenciais. Partindo desta definição buscaremos neste capítulo caracterizar conceitos básicos que envolvem o espaço cibernético para podermos definir com maior precisão como a defesa cibernética se apresenta no tempo presente.

1.2 A Natureza Transfronteiriça do Espaço Cibernético

A natureza transfronteiriça das atividades cibernéticas e a interdependência das redes de comunicação geram debates intensos sobre como os Estados podem exercer sua autoridade e proteger seus interesses nesse ambiente virtual em constante evolução.

De acordo com Portela (2018), os Estados desejam preservar sua soberania para gerenciar potenciais ameaças cibernéticas, adquirir informações estratégicas e evitar a obtenção de informações sensíveis por parte de atores, sejam eles estatais ou não. De acordo com a definição clássica westfaliana, a soberania é entendida como a autoridade exclusiva de um Estado sobre seu território físico e população. Escapa à definição clássica a realidade da política internacional em que o alcance e a aplicação da noção de soberania pode variar bastante em um mundo interdependente e globalizado. No espaço cibernético, essa noção é desafiada pela capacidade de atores não estatais e estatais agirem além das fronteiras geográficas sem restrições claras. Ações cibernéticas, como ataques, espionagem e propaganda, podem ocorrer com menos visibilidade e resposta do que ocorreriam em cenários físicos.

Conforme Daniel Ventre (2012), o espaço cibernético apresenta pontos de interseção com outros espaços geográficos, permitindo que suas ramificações alcancem e exerçam

impacto sobre todos esses âmbitos. Simultaneamente, está sujeito a influências provenientes de cada um desses ambientes (Figura 1), formando uma interligação dinâmica e multifacetada.

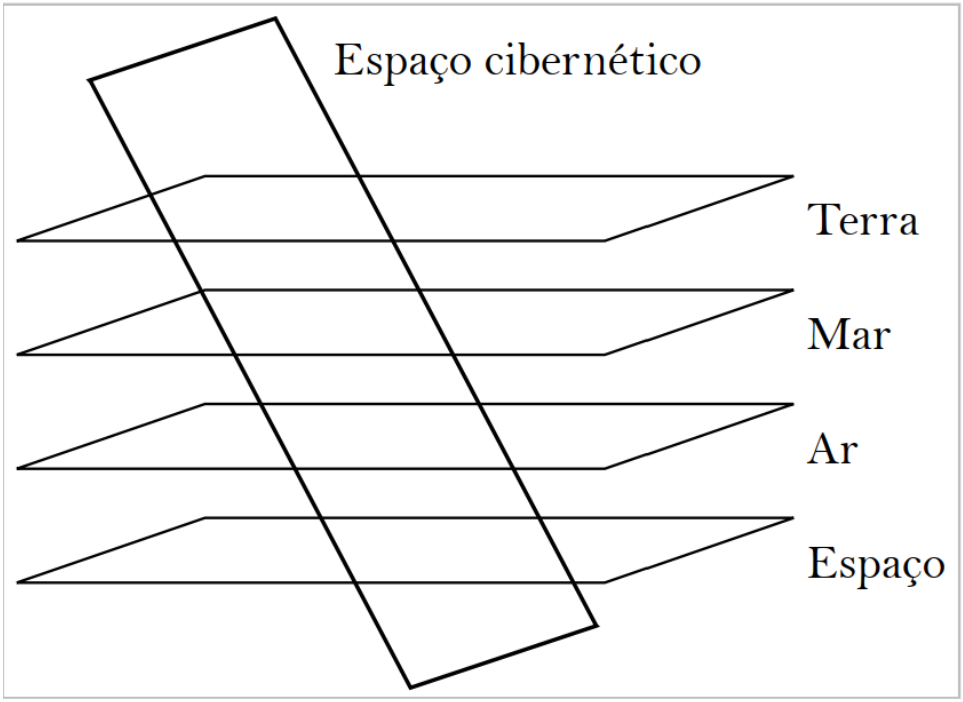

FIGURA 1 – RELAÇÃO DO ESPAÇO CIBERNÉTICO COM OS demais espaços geográficos.
Fonte: Ventre (2012, p. 35).

Portela (2018) destaca que, devido à sua capacidade de transcender os domínios convencionais, o espaço cibernético é uma ferramenta de controle com imenso potencial para os Estados. Ao contrário dos espaços tradicionais, como o terrestre, que frequentemente são almejados pelo Estado para a exploração de recursos, o espaço cibernético atrai o interesse devido ao valor intrínseco da informação gerada internamente e através de suas redes interconectadas.

A geopolítica do espaço cibernético não busca estabelecer uma demarcação territorial cibernética análoga aos espaços físicos convencionais. Em vez disso, concentra-se em delinear os limites e fronteiras desse espaço em relação a outros Estados e em identificar seus pontos de convergência com as esferas terrestre, marítima, aérea e espacial. A construção de um território cibernético, portanto, difere em sua essência, abarcando principalmente os fluxos de informação e as relações interconectadas que permeiam esse ecossistema virtual.

1.3 Distinção entre Segurança e Defesa Cibernética

No contexto cibernético, é importante fazer uma distinção entre segurança e defesa cibernética. Segurança, em termos amplos, pode ser definida como "um estado de equilíbrio, no qual os indivíduos têm a percepção de liberdade para acessar informações, produtos e processos que consideram apropriados para fomentar seu desenvolvimento..." (RAZA, 2005, p. 69)[8]. Na segurança cibernética, esse conceito se traduz em um estado de equilíbrio em que os indivíduos têm a liberdade de acessar informações e processos para seu desenvolvimento. A segurança está associada à estabilidade interna da nação, protegendo fatores estratégicos que garantem o bem-estar da população e o funcionamento das instituições.

A defesa, por outro lado, de acordo com o Plano Nacional de Defesa (PND) (2012) do Ministério da Defesa (MD) do Brasil, envolve "o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantes externas, potenciais ou manifestas." (PND, 2012).

No campo cibernético é possível definir que segurança cibernética protege e garante a "utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais" (CARVALHO, 2011, p. 17). A segurança cibernética também abarca o processo de interação com órgãos públicos e privados que estão envolvidos no das infraestruturas críticas nacionais, com destaque para os órgãos da Administração Pública Federal. (CARVALHO, 2011). De acordo com Carvalho (2011) pode-se definir que a defesa cibernética é o "Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os nossos sistemas de informação" (CARVALHO, 2011, p. 18). No campo da defesa cibernética também são promovidas ações para "obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente." (CARVALHO, 2011, p. 18). A partir desta perspectiva a distinção entre segurança e defesa cibernética é evidente, onde a segurança está ligada à proteção de informações estratégicas e ao funcionamento estável do Estado, enquanto a defesa está mais focada em ameaças externas e na proteção do território e da soberania nacional. A defesa é principalmente uma

[8] Texto original: "state of equilibrium where individuals perceive themselves as having the freedom to access information, products and processes they consider proper for fostering their development."

responsabilidade das Forças Armadas, mas pode envolver vários recursos e instituições. Contudo, não se deve perder de vista a complementariedade desses dois conceitos.

Os conceitos de segurança e defesa cibernética evoluíram para se aplicar ao contexto cibernético. A análise também destaca como esses conceitos se traduzem em políticas e responsabilidades específicas dentro do cenário cibernético. O salvaguardar de sistemas, redes e informações contra ameaças cibernéticas é um imperativo crítico para garantir a segurança, a confidencialidade e a integridade tanto de indivíduos quanto de instituições e nações. Adicionalmente, destaca-se que segurança e defesa cibernética objetivam viabilizar e assegurar, disponibilidade, integridade, confidencialidade e autenticidades dos ativos de informações. (Cruz Júnior, 2013).

1.4 Tipos de Ameaças Cibernéticas

A natureza das ameaças cibernéticas é diversificada e em constante evolução. Os principais tipos de ameaças cibernéticas incluem:

Malware: O malware é uma categoria abrangente que engloba várias ameaças cibernéticas, como vírus, worms, trojans e spyware. Esses programas maliciosos são criados com o propósito de causar danos aos sistemas, roubar informações sensíveis ou fornecer acesso não autorizado(John Aycock, 2006). Um exemplo de calamidade mundial relacionada ao malware foi o worm Stuxnet, que em 2010 atacou sistemas de controle industrial no Irã. Este malware foi projetado para sabotar o programa nuclear iraniano, causando danos significativos a infraestruturas críticas[9].

Ataques de Negação de Serviço (DDoS): Esses ataques sobrecarregam recursos de sistemas ou serviços online, tornando-os inacessíveis para usuários legítimos (Jelena Mirkovic e Sven Dietrich, 2015). Um dos maiores ataques registrados foi o ataque DDoS massivo que afetou a provedora de DNS Dyn em 2016. Esse ataque interrompeu serviços populares, como Twitter, Netflix e Amazon, causando perturbações generalizadas na internet e destacando a vulnerabilidade da infraestrutura digital global[10].

Phishing: Envolve a enganação de usuários para revelar informações pessoais, como senhas e informações financeiras (Christopher Hadnagy e Michele Fincher, 2015). Um exemplo

[9] Disponível em: https://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html. Acesso em [01/09/2023].
[10] Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/#:~:text=O%20ataque%20%C3%A0%20Dyn%20em,o%20Reddit%20e%20o%20GitHub. Acesso em 01 set. 2023.

notável foi o vazamento de dados da Equifax em 2017, onde informações de aproximadamente 147 milhões de consumidores foram expostas, demonstrando o alcance devastador que ataques de phishing podem ter em escala global[11].

Ransomware: Este tipo de ataque criptografa arquivos de vítimas, exigindo um resgate para descriptografá-los (Ronny Richardson, 2017). Um ataque em escala mundial relacionada ao ransomware foi o ataque do WannaCry em 2017, que afetou sistemas de saúde, empresas e órgãos governamentais em todo o mundo. Hospitais foram forçados a desligar seus sistemas, colocando em risco a vida dos pacientes, e empresas enfrentaram grandes prejuízos financeiros, demonstrando a capacidade destrutiva desse tipo de ameaça[12].

1.5 Motivações por Trás dos Ataques Cibernéticos

Existem diferentes causas por trás de ataques cibernético. As motivações são variadas e abrangem uma ampla gama de interesses e intenções. Assim, os ataques cibernéticos podem ser motivados por diversas razões, tais como motivações políticas, econômicas, ideológicas e criminosas. Neste tópico caracterizamos essas motivações.

Questões Políticas: Alguns ataques cibernéticos são motivados por questões políticas, como espionagem entre nações (P.W. Singer e Allan Friedman, 2014). Em 2016, ocorreu um notório ataque cibernético contra o Comitê Nacional Democrata (DNC) dos Estados Unidos. Este incidente exemplifica uma motivação política para ataques cibernéticos. Alegadamente, hackers com ligações ao governo russo comprometeram os sistemas da DNC para obter informações confidenciais e, posteriormente, divulgaram documentos comprometedores durante o período das eleições presidenciais dos EUA. O objetivo era influenciar o processo político e minar a candidatura democrata. Esse evento destacou o uso da cibersegurança como uma ferramenta na guerra cibernética entre nações[13]. Esse ataque levou a tensões diplomáticas entre os EUA e a Rússia, além de questionamentos sobre a integridade das eleições.

Questões Econômicas: Os ataques cibernéticos com motivações econômicas são efetuados por criminosos cibernéticos que frequentemente visam organizações e indivíduos em busca de ganhos financeiros (Jack M. Balkin, et al, 2007). O ataque de ransomware WannaCry em 2017 é um exemplo emblemático de motivação econômica na cibersegurança. Esse malware

[11] Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/22/equifax-faz-acordo-para-pagar-r-26-bi-por-vazamento-de-dados-de-clientes-nos-eua.ghtml. Acesso em: 01 set. 2023
[12] Disponível em: https://olhardigital.com.br/especial/wannacry/. Acesso em: 01 set. 2023.
[13] Disponível em: https://www1.folha.uol.com.br/mundo/2016/12/1841384-hackers-russos-invadiram-as-eleicoes-dos-eua-em-favor-de-trump.shtml. Acesso em: 02 set. 2023.

se espalhou globalmente, criptografando os dados de computadores e exigindo um resgate em Bitcoin para a descriptografia. O objetivo era claramente financeiro, visando extorquir dinheiro das vítimas. O WannaCry afetou hospitais, empresas e órgãos governamentais, causando prejuízos econômicos significativos e evidenciando a importância da proteção contra ameaças cibernéticas para a continuidade dos negócios[14]. Os custos de recuperação, perda de receita e danos à reputação podem ser enormes. Além disso, o cibercrime afeta setores inteiros, como o financeiro e o de saúde.

Questões Ideológicas: Grupos hacktivistas realizam ataques cibernéticos para promover suas causas ou ideologias (Tim Jordan, 2004). O grupo hacktivista Anonymous é conhecido por suas motivações ideológicas e ações online. Eles têm como objetivo defender causas como liberdade de expressão e protestar contra a censura na internet. Durante a Primavera Árabe em 2011, o Anonymous atacou sites do governo egípcio em apoio aos manifestantes pró-democracia. Sua motivação era claramente ideológica, buscando usar habilidades técnicas para promover mudanças políticas e sociais[15].

Motivações Criminosas: Muitos ataques cibernéticos têm motivações criminosas, incluindo roubo de dados, fraudes online e extorsão (Jon Erickson, 2008). O ataque ao banco de dados da Equifax em 2017 exemplifica uma motivação criminosa no ciberespaço. Neste caso, criminosos exploraram vulnerabilidades de segurança para acessar informações pessoais e financeiras de milhões de pessoas. A motivação era o lucro financeiro, uma vez que os dados roubados poderiam ser usados para cometer fraudes financeiras, roubo de identidade e outras atividades criminosas. O impacto foi devastador, levando a enormes perdas financeiras e danos à reputação da empresa[16].

Os ataques cibernéticos têm impactos significativos em vários aspectos da sociedade, desde o cenário político até a economia e a confiança da sociedade na utilização de serviços através da internet. A análise dessas consequências destaca a necessidade de uma abordagem abrangente para a cibersegurança, visando proteger as infraestruturas críticas e os dados pessoais, bem como promover a cooperação internacional na prevenção de ameaças cibernéticas.

---

[14] OLHAR DIGITAL. Especial WannaCry. Disponível em: https://olhardigital.com.br/especial/wannacry/. Acesso em: 02 set. 2023.
[15] Disponível em: https://g1.globo.com/tecnologia/noticia/2011/02/hackers-tiram-do-ar-sites-do-governo-do-egito-diz-jornal.html. Acesso em: 02 set. 2023.
[16] Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/22/equifax-faz-acordo-para-pagar-r-26-bi-por-vazamento-de-dados-de-clientes-nos-eua.ghtml. Acesso em: 02 set. 2023.

1.6 Infraestruturas críticas e Ataques cibernéticos

As infraestruturas críticas, abrangendo setores vitais como energia, transporte e saúde, desempenham um papel essencial em nosso modo de vida contemporâneo. No entanto, essa interdependência com a tecnologia cibernética também as torna altamente suscetíveis a ameaças cibernéticas que podem ter implicações profundas nas esferas política, econômica e social.

Primeiramente, é essencial compreender as dimensões das infraestruturas críticas. Isso inclui sistemas de energia que abastecem nossas casas e indústrias, sistemas de transporte que garantem a mobilidade e o comércio e o setor de saúde, que lida com questões de vida e morte. A dependência dessas infraestruturas em sistemas digitais as torna intrinsecamente vulneráveis a ataques cibernéticos que visam explorar essas fragilidades.

Para ilustrar a gravidade dessas ameaças, é instrutivo analisar estudos de casos bem documentados de ataques cibernéticos bem-sucedidos contra infraestruturas críticas. Um exemplo notável é o ataque à usina nuclear de Natanz em 2010, detalhadamente estudado por Ralph Langner (2013). Neste caso, um ataque cibernético conseguiu comprometer os sistemas de controle industrial, resultando em danos físicos a uma usina nuclear no Irã. Isso destacou de forma alarmante a capacidade dos ataques cibernéticos de causar danos reais e significativos a infraestruturas críticas em todo o mundo.

Outro caso impactante foi o ataque ao sistema de distribuição de energia na Ucrânia em 2015, segundo a BBC[17], que teve o Departamento de Segurança Interna dos EUA como autor do relatório. Este ataque destrutivo interrompeu o fornecimento de energia elétrica para milhares de pessoas, destacando a vulnerabilidade das redes elétricas e a capacidade dos ataques cibernéticos de afetarem diretamente a vida das pessoas.

Esses casos ilustram a gravidade das ameaças cibernéticas às infraestruturas críticas e suas implicações globais. Os ataques cibernéticos bem-sucedidos não apenas prejudicam as operações e a segurança dessas infraestruturas, mas também afetam a confiança pública, as relações diplomáticas e a economia global. É crucial que sejam tomadas medidas proativas e colaborativas para fortalecer a segurança cibernética das infraestruturas críticas e garantir sua resiliência em face de ameaças em constante evolução.

Nesse sentido, é crucial que governos, empresas e especialistas em segurança cibernética se unam em esforços coordenados, estabelecendo regulamentações adequadas, promovendo a conscientização pública e investindo em tecnologias e práticas de segurança

[17] Disponível em: https://g1.globo.com/tecnologia/blog/seguranca-digital/post/ucrania-tem-segundo-apagao-eletrico-causado-por-hackers.html . Acesso em: 02 set. 2023.

robustas. Somente por meio dessa abordagem abrangente poderemos enfrentar eficazmente os desafios representados pelos ataques cibernéticos às infraestruturas críticas e manter a estabilidade de nossa sociedade moderna.

1.7 O que é governança de cibersegurança?

A governança de cibersegurança a nível nacional refere-se ao conjunto de políticas, diretrizes, regulamentos e estruturas organizacionais que um país estabelece para proteger suas infraestruturas críticas e informações sensíveis contra ameaças cibernéticas. É um componente essencial da estratégia de segurança cibernética de uma nação e envolve a coordenação de esforços entre o governo, o setor privado e outros stakeholders para garantir a proteção adequada contra ataques cibernéticos (Luca Belli, 2023).

No contexto da governança de cibersegurança a nível nacional, os governos desempenham um papel fundamental na formulação de políticas e na criação de regulamentos que incentivem a conformidade com padrões de segurança cibernética. Eles também estabelecem agências ou órgãos responsáveis por supervisionar a implementação dessas políticas e regulamentos. Além disso, promovem a conscientização sobre segurança cibernética e colaboram com empresas e organizações para melhorar a resiliência cibernética em todo o país (Luca Belli, 2023).

Um exemplo de governança de cibersegurança a nível nacional pode ser encontrado nos Estados Unidos, onde a "Estratégia de Segurança Cibernética Nacional" é liderada pelo Departamento de Segurança Interna (DHS) e pela Agência de Segurança Cibernética e Infraestrutura (CISA). Essa estratégia visa fortalecer a segurança cibernética em setores-chave, como energia, transporte e saúde, por meio de colaboração com empresas privadas e desenvolvimento de regulamentos de segurança[18].

Outro exemplo notável é a Estratégia de Segurança Cibernética da União Europeia, que visa melhorar a resiliência cibernética em toda a UE por meio da cooperação entre os Estados membros, a criação de uma Agência Europeia de Segurança Cibernética (ENISA) e a implementação de regulamentos de segurança cibernética, como o Regulamento de Cibersegurança da UE[19].

---

[18] Estratégia de Segurança Cibernética Nacional dos Estados Unidos, Disponível em: https://www.dhs.gov/topics/cybersecurity . Acesso em: 03 set. 2023.

[19] Disponível em: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pt . Acesso em: 03 set. 2023.

No contexto brasileiro, a governança de cibersegurança é uma preocupação crescente, dada a importância das tecnologias da informação e comunicação (TICs) para o funcionamento da sociedade e da economia. O Brasil tem adotado várias medidas e iniciativas para melhorar sua governança de cibersegurança.

Uma dessas medidas é a Estratégia Nacional de Segurança Cibernética (ENSC), lançada em 2018. A ENSC é um plano abrangente que estabelece diretrizes e metas para aprimorar a cibersegurança no Brasil. Ela visa a proteção de infraestruturas críticas, a redução de incidentes cibernéticos e o fortalecimento da capacidade de resposta a ameaças cibernéticas[20]. Além disso, o Brasil promulgou a Lei Geral de Proteção de Dados (LGPD), que não é exclusivamente uma lei de cibersegurança, mas desempenha um papel crucial na proteção de dados pessoais, um componente fundamental da cibersegurança. A LGPD estabelece regras para o tratamento de dados pessoais e impõe penalidades por violações, promovendo a segurança dos dados no ambiente digital[21].

O país também conta com o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), operado pelo NIC.br, que é responsável por monitorar e responder a incidentes de segurança cibernética no Brasil. Ele fornece alertas, orientações e coordenação de resposta a incidentes para proteger a infraestrutura digital do país[22].

Outra iniciativa do Estado foi a criação pelo Gabinete de Segurança Institucional (GSI), a criação do livro verde em 2010 que visa expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, articulando visão de curto (2 - 3 anos), médio (5 – 7 anos), e longo (10 – 15 anos) prazo no tema, abrangendo, como ponto de partida, os seguintes vetores: Político estratégico, Econômico, Social e Ambiental, CT&I, Educação, Legal, Cooperação Internacional, e Segurança das Infraestruturas Críticas. O livro verde também avalia a necessidade de uma macro-coordenação e governança bem estabelecidas, bem como baseados em modelos efetivos e eficazes de colaboração entre governo, setor privado e academia[23].

Os desafios da segurança cibernética são muitos e complexos, demandando uma abordagem holística e uma coordenação internacional eficaz para enfrentá-los de maneira eficiente e eficaz. Nesse contexto, é fundamental desenvolver um conjunto de ações

[20] Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/estrategia-nacional-de-seguranca-cibernetica . Acesso em: 03 set. 2023.
[21] Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd . Acesso em: 03 set. 2023 .
[22] Disponível em: https://www.cert.br/sobre/ . Acesso em:03 set. 2023.
[23] Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf Acesso em:03 set. 2023.

colaborativas que envolvam não apenas o governo, o setor privado, a academia, o terceiro setor e a sociedade, mas também uma coordenação internacional sólida. A natureza transnacional das ameaças cibernéticas, como ataques de hackers e ciberespionagem, transcende as fronteiras nacionais, tornando fundamental que os esforços de defesa cibernética sejam coordenados em nível global.

A cooperação internacional permite o compartilhamento de informações sobre ameaças, a harmonização de normas e regulamentações, a colaboração em investigações transfronteiriças e a criação de estratégias de resposta conjuntas. A coordenação internacional na defesa cibernética não apenas complementa, mas também fortalece a capacidade de todas as partes interessadas em abordar o complexo mosaico de aspectos que envolvem a segurança cibernética em um mundo interconectado.

1.8 Estruturação do setor de cyber defesa e estabelecimento da política de segurança da informação

Em 5 de fevereiro de 2020, o Brasil estabeleceu um marco significativo ao aprovar sua primeira Estratégia de Segurança Cibernética (E-Ciber)[24]. Este documento estratégico delineia as principais ações do governo, tanto em âmbito nacional quanto internacional, para fortalecer a segurança cibernética no país durante o período de 2020 a 2023. No entanto, é crucial observar que essa não foi a primeira incursão do governo brasileiro na definição de competências, princípios e objetivos para a segurança cibernética[25].

Desde meados dos anos 2000, o Brasil vem gradativamente incorporando o conceito de segurança cibernética em seu vocabulário político-estratégico. Isso se reflete na publicação de diversos documentos, como o Livro Verde da Segurança Cibernética em 2010 e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal para o período de 2015 a 2018. Além disso, diferentes órgãos da Administração Pública Federal também se esforçaram para integrar preocupações com a segurança cibernética em seus respectivos planejamentos estratégicos. Um exemplo notável é a E-Digital, iniciativa desenvolvida em conjunto pelo Ministério da Ciência e Tecnologia e o Ministério das Comunicações, que abordou a segurança e defesa cibernética, bem como crimes cibernéticos,

[24] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm Acesso em: 30 set. 2023.
[25] Disponível em https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/estrategia-nacional-de-seguranca-cibernetica Acesso em: 30 set. 2023.

como parte de seus esforços para promover a confiança no ambiente digital. Na Figura 2 mostra um resumo da evolução da segurança cibernética do Brasil[26].

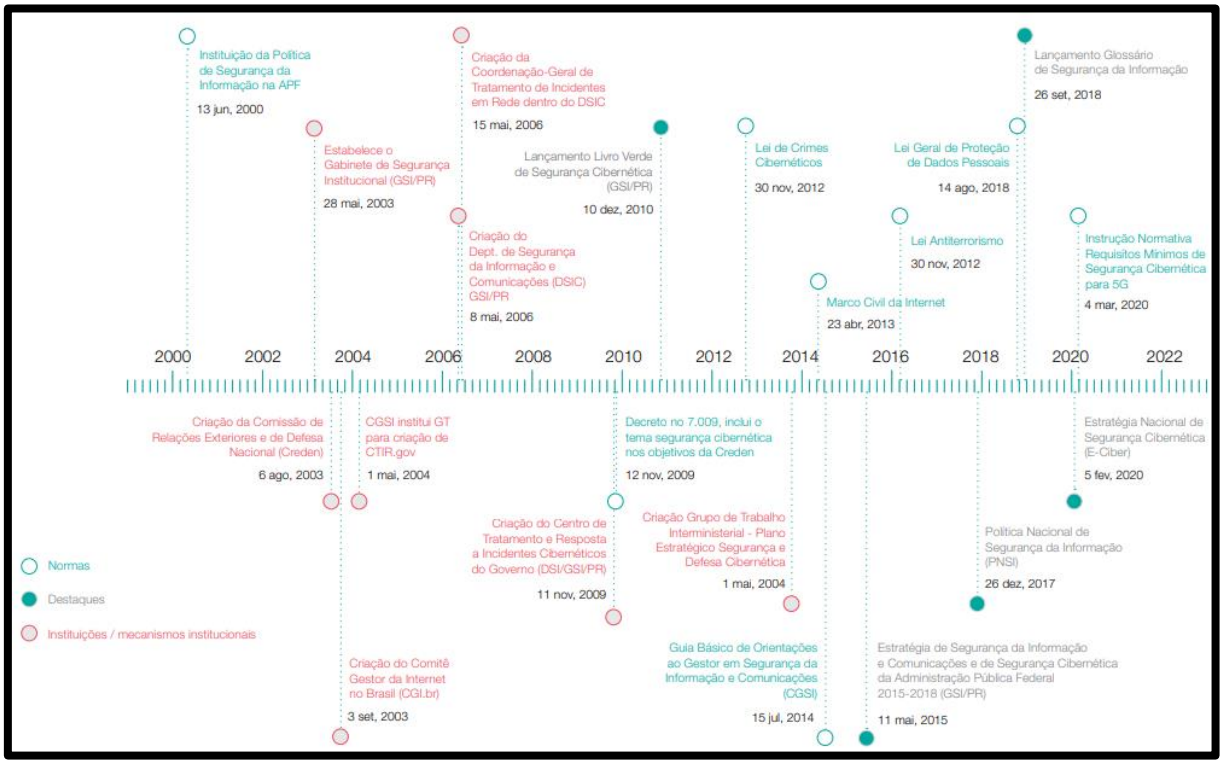

FIGURA 2. LINHA DO TEMPO: SEGURANÇA CIBERNÉTICA NO BRASIL (ADMINISTRAÇÃO PÚBLICA FEDERAL)
Fonte: **INSTITUTO IGARAPÉ, ARTIGO ESTRATÉGICO 54, ABRIL 2021**

A expansão exponencial da internet comercial trouxe consigo uma crescente preocupação em relação aos riscos de segurança cibernética. A necessidade de manter uma infraestrutura resiliente e operacional, o Brasil estabeleceu dois órgãos essenciais no campo da segurança cibernética: o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), criado em 1997, e o Núcleo de Coordenação do Ponto BR (NIC.Br), criado em 2000[27].

O CERT.br surgiu a partir de um estudo encomendado pelo Comitê Gestor da Internet no Brasil (CGI.br), com o propósito de estabelecer uma "coordenadoria de segurança de redes". Este centro desempenha um papel crucial na detecção e mitigação de incidentes de segurança cibernética no cenário nacional[28].

[26] Disponível em https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf Acesso em: 30 set. 2023.
[27] Disponível em https://nic.br/noticia/releases/para-fortalecer-cultura-de-protecao-de-dados-no-pais-nic-br-e-anpd-firmam-acordo-de-cooperacao/ Acesso em: 17 set. 2023.
[28] Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil. Disponível em https://cert.br/sobre/estudo-cgibr-1996.html . Acesso em: 17 set. 2023.

O NIC.br, estabelecido em 2003, tem a responsabilidade de implementar as decisões do CGI.br. Em 2005, o NIC.br assumiu a administração do registro de nomes sob o domínio ".br". Essa iniciativa visava aprimorar a gestão e a segurança dos domínios brasileiros na internet, contribuindo para um ambiente cibernético mais seguro e confiável[29]. A seguir temos na Figura 3 a composição do NIC.br com todas as ramificações.

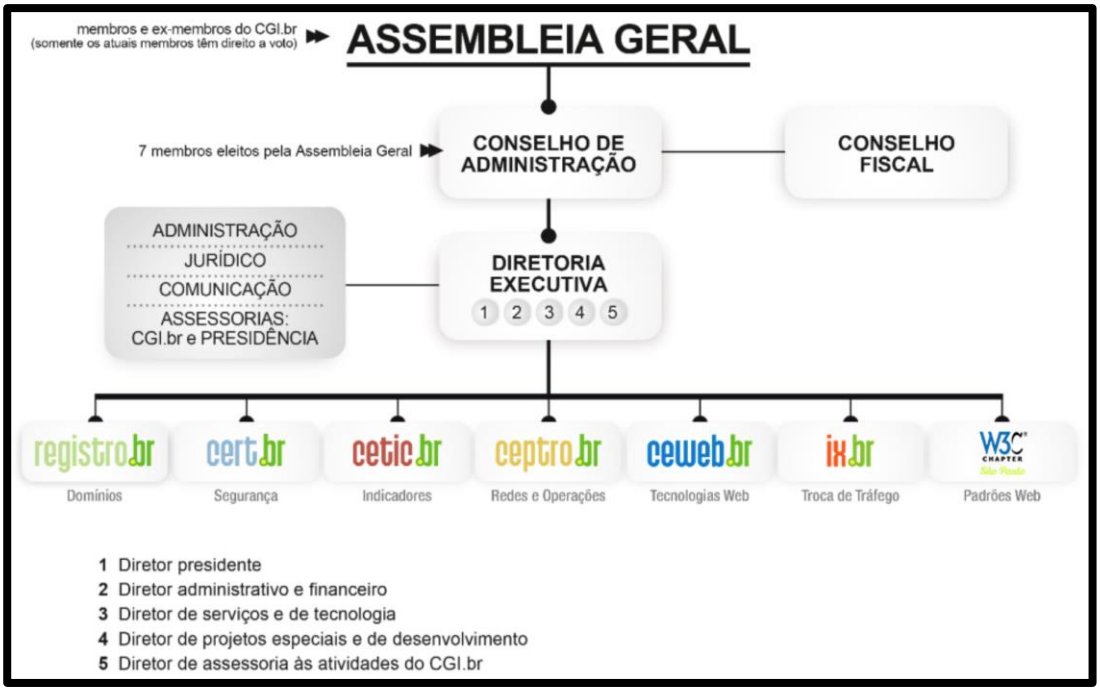

FIGURA 3. COMPOSIÇÃO DO NIC.BR
FONTE: HTTPS://NIC.BR/SOBRE/#COMPOSICAO

Sendo o CERT.br, como ponto focal para notificação e resposta a incidentes no Brasil, desempenha um papel fundamental na segurança cibernética do país. Além de suas atividades de resposta a incidentes, o CERT.br também exerce um papel crucial na promoção da conscientização sobre riscos e ameaças na rede. Isso inclui a realização de treinamentos e a produção e disseminação de recursos educacionais que abordam uma ampla gama de desafios, como botnets, malware, phishing e spam[30].

Após a criação do Comitê Gestor da Segurança da Informação em 2000, o Brasil estabeleceu um sistema hierárquico de tomada de decisões federais em matéria de defesa cibernética. Esse sistema se estende desde a Presidência da República, no nível estratégico, até o nível operacional, envolvendo forças-tarefa dentro da Polícia Federal e o Centro de Defesa Institucional da Presidência da República (GSI-PR). Este último tem como missão oferecer

[29] Disponível em: https://nic.br/historia/ .Acesso em; 17 set. 2023.
[30] Disponível em https://www.cert.br/sobre/ .Acesso em: 17 set. 2023.

assistência à presidência em questões de defesa e segurança, além de coordenar as atividades de inteligência federal e segurança da informação, através da Agência Brasileira de Inteligência (ABIN) (LOBATO, 2018).

No contexto do Ministério da Defesa (MD), a Estratégia Nacional de Defesa (END), lançada em 2008 e atualizada em 2012, reconheceu o espaço cibernético como um dos três principais setores estratégicos para a defesa e segurança nacionais, ao lado dos setores nuclear e espacial. A END representa um marco fundamental em um processo político-estratégico de estruturação e desenvolvimento tecnológico no setor militar, com o objetivo de promover uma maior cooperação entre as Forças Armadas. Além disso, ela atribuiu ao Exército a responsabilidade pela coordenação e integração de programas relacionados ao setor cibernético[31].

Em 2016, o Brasil deu mais um passo significativo na direção da defesa cibernética com o estabelecimento do Comando de Defesa Cibernética (ComDCiber), composto por representantes do Exército, da Marinha e da Aeronáutica. Este órgão foi encarregado de planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética. O ComDCiber é um comando operacional conjunto que se insere na estrutura regimental do Exército Brasileiro, trabalhando em estreita colaboração com o Estado-Maior Conjunto, liderado pela Marinha, e o Departamento de Gestão e Estratégia, liderado pela Aeronáutica[32].

A criação do ComDCiber não apenas reforçou a cooperação entre as Forças Armadas, mas também evidenciou um processo contínuo de fortalecimento das capacidades do Centro de Defesa Cibernética (CDCiber). Este fortalecimento está alinhado com as diretrizes estabelecidas na revisão da END em 2012, que reconhece a cibersegurança como um elemento vital na proteção dos interesses nacionais e na garantia da soberania do país. Através dessas medidas, o Brasil demonstra seu compromisso com a defesa cibernética e a proteção das informações e sistemas críticos do Estado (CGCSC,2020).

A Figura 4 apresenta uma visão geral da estrutura de governança da segurança cibernética no Brasil, destacando a participação desses diversos setores. Essa representação visual permite a identificação dos principais grupos e temas que compõem essa estrutura, enfatizando que a segurança cibernética é uma preocupação compartilhada por uma ampla variedade de atores e

[31] Disponível em https://www.gov.br/defesa/pt-br/assuntos/seprod/ciencia-e-tecnologia/setores-estrategicos Acesso em: 17 set. 2023. [17/09/2023].
[32] Disponível em https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/comando-conjunto-na-defesa-cibernetica Acesso em:17 set. 2023.]

ressalta a necessidade de promover uma colaboração mais ampla entre esses atores no que se refere à formulação de políticas integradas de segurança cibernética.

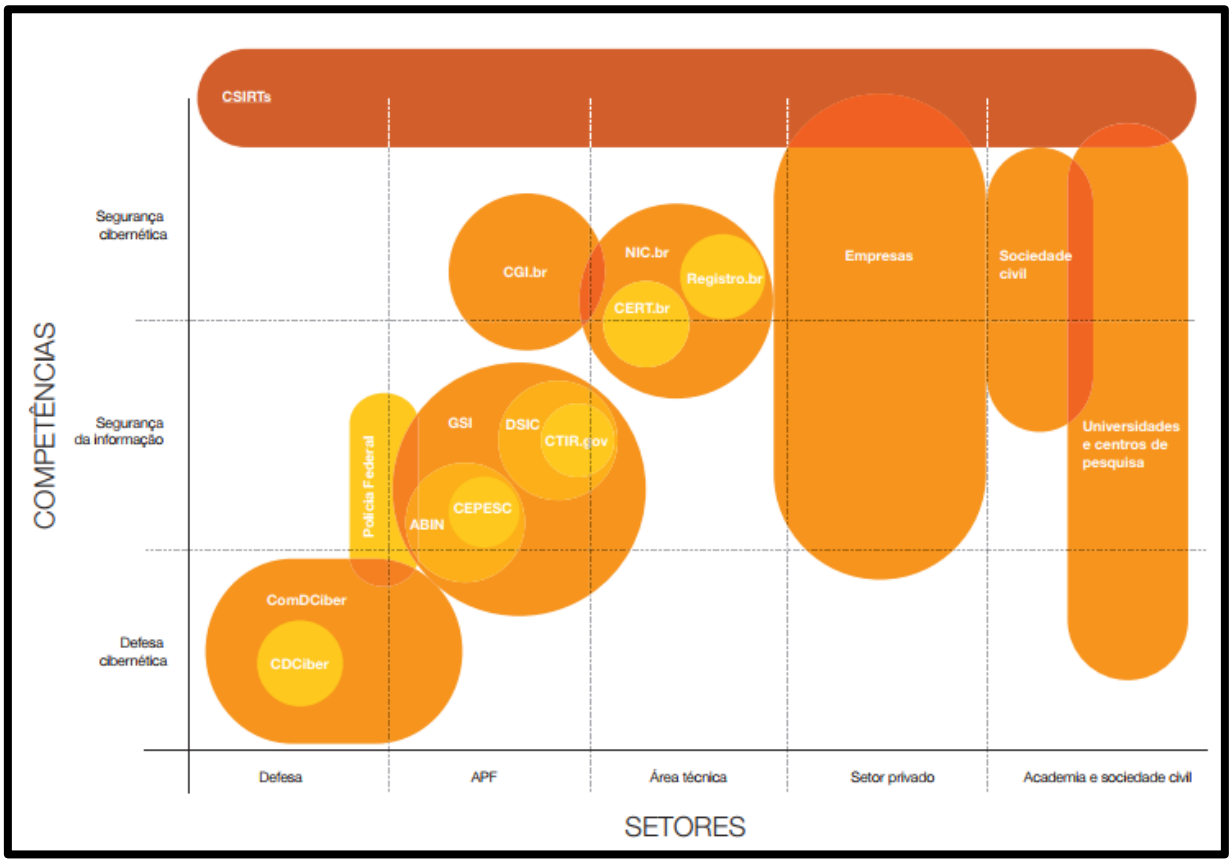

FIGURA 4. ESTRUTURA DA GOVERNANÇA DA SEGURANÇA CIBERNÉTICA NO BRASIL. FONTE: LOBATO, 2018, P. 09.

No contexto da institucionalização da segurança cibernética no país, é importante observar que diversos órgãos técnicos de natureza governamental desempenham papéis cruciais na elaboração de políticas, regulamentações e práticas relacionadas à segurança cibernética. Esses órgãos, embora operando de forma distinta, estão intrinsecamente interligados em seus esforços.

É de extrema relevância destacar que todos os órgãos e servidores da Administração Pública Federal (APF) possuem algum grau de envolvimento com a segurança cibernética. No entanto, neste contexto, estamos direcionando nosso foco para aqueles que desempenham um papel ativo na estratégia de defesa cibernética adotada pelo país, estabelecendo uma ligação direta entre suas atribuições e funções específicas no âmbito deste estudo.

A Figura 5 ilustra o sistema brasileiro de defesa cibernética (Secretaria de assuntos estratégicos, 2011). É importante ressaltar que os temas relacionados à segurança da informação e comunicações, segurança cibernética e proteção das infraestruturas críticas a nível nacional

estão sob a alçada do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN).

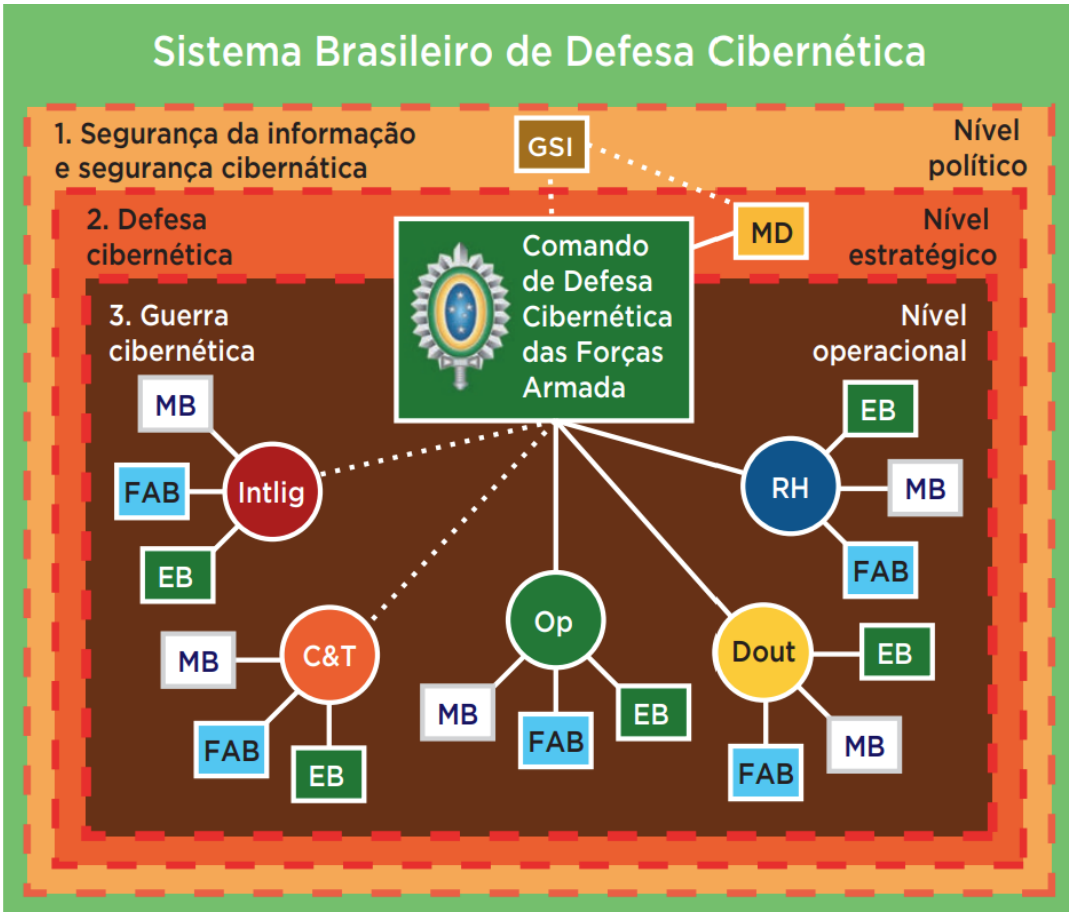

FIGURA 5. SISTEMA BRASILEIRO DE DEFESA CIBERNÉTICA.HIERARQUIA DOS PRINCIPAIS ÓRGÃOS DA APF NA SEGURANÇA E DEFESA CIBERNÉTICA.

O CDN desempenha o papel de um órgão consultivo da Presidência da República em questões relacionadas à soberania nacional e à defesa do Estado democrático. Ele exerce influência em decisões estratégicas, inclusive aquelas relacionadas à esfera da segurança cibernética.

Por sua vez, o CREDEN age como um órgão consultivo da Presidência com foco em questões de relações exteriores e defesa nacional. Entre suas responsabilidades estão incluídas a segurança das informações e comunicações, bem como a segurança cibernética, especialmente no que diz respeito à formulação de diretrizes estratégicas. Ambos os órgãos têm o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) como sua Secretaria-Executiva, o que destaca a integração dessas instâncias no contexto da segurança cibernética.

No âmbito do CREDEN, durante uma de suas reuniões, foi decidida a criação do Comitê Gestor da Informação (CGSI), com o propósito de realizar estudos específicos sobre segurança

da informação e comunicações, além de desenvolver propostas relacionadas à segurança e defesa das infraestruturas críticas da informação. Esse comitê é composto por representantes dos ministérios e também por órgãos públicos e privados com interesses nessa área (MANDARINO JUNIOR, 2010).

Além do CGSI (Canongia, Júnior & Júnior, 2010), o GSI/PR coordena outros grupos e equipes essenciais para a segurança cibernética, tais como:

- Grupos de Trabalho de Segurança das Infraestruturas Críticas, nos setores de energia, telecomunicações, transporte, abastecimento de água e finanças;
- Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação;
- Grupo Técnico de Segurança Cibernética; e
- Grupo Técnico de Criptografia.

Com base na Lei nº 10.683 de 2003, o GSI/PR coordena as atividades de inteligência e segurança da informação, assumindo assim um papel central na coordenação da estratégia de segurança cibernética nacional. O Departamento de Segurança da Informação e Comunicações (DSIC) e a Agência Brasileira de Inteligência (ABIN) são subordinados ao GSI/PR e desempenham um papel fundamental na construção da estratégia de segurança cibernética.

O DSIC (Presidência da República,2014) possui competências que abrangem diversas atividades no processo de operacionalização das questões relacionadas à Segurança da Informação e Comunicações (SIC), incluindo:

- Regulamentação;
- Avaliação de tratados, acordos ou atos internacionais;
- Coordenação do Sistema de Segurança e Credenciamento;
- Definição de requisitos metodológicos;
- Planejamento e coordenação da gestão de assuntos, documentos e tecnologias sigilosas.

A Agência Brasileira de Inteligência (ABIN) desempenha um papel crucial na avaliação de ameaças, tanto internas quanto externas, com o objetivo de fornecer informações oportunas para a implementação de planos de defesa dos sistemas brasileiros.[33] Dentro da estrutura da ABIN, o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC) desempenha um papel fundamental ao promover pesquisa científica e tecnológica voltada para soluções criptográficas e algoritmos de importância estratégica para o governo.

Outro órgão de extrema importância vinculado à Presidência da República é a Casa Civil, que desempenha um papel significativo no contexto da defesa cibernética e segurança da

[33] Disponível em: https://www.gov.br/abin/pt-br/institucional/a-abin . Acesso em [30/09/2023].

informação. Isso ocorre por meio de uma autarquia federal que está sob sua jurisdição, conhecida como Instituto Nacional de Tecnologia da Informação (ITI). O ITI é responsável por manter a Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil) e atua como a primeira autoridade na cadeia de certificação. Sua missão consiste em fornecer um ambiente seguro para autenticação digital e a assinatura eletrônica, garantindo a confiabilidade e a integridade das transações eletrônicas no âmbito do governo brasileiro.[34]

Uma vez que a preservação da soberania nacional está intrinsecamente ligada à manutenção da defesa cibernética, torna-se evidente a responsabilidade do Ministério da Defesa, por meio das Forças Armadas, em desempenhar um papel fundamental nesse contexto. A Marinha do Brasil, o Exército Brasileiro e a Força Aérea Brasileira, componentes integrantes da estrutura do Ministério da Defesa (MD), aplicam suas tecnologias e conhecimentos para atuar no mais recente campo de batalha, o espaço cibernético.

FIGURA 6. COMPOSIÇÃO DA DEFESA CIBERNÉTICA DO MINISTÉRIO DA DEFESA.

No contexto das atividades cibernéticas do MD, merece destaque especial o Exército Brasileiro (EB), que opera o Centro de Defesa Cibernética (CDCiber). O CDCiber tem, em linhas gerais, os seguintes objetivos, conforme destacado por Oliveira (2011):

- Expansão e aprimoramento da infraestrutura de segurança cibernética já existente.

[34] Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/o-iti. Acesso em:[30/09/2023].

- Expansão e aprimoramento da infraestrutura de capacitação, treinamento e emprego operacional existente, a fim de atender às necessidades do Setor Cibernético, incluindo a integração de tópicos relacionados ao tema nos currículos dos estabelecimentos de ensino da Força.
- Estabelecimento de uma infraestrutura de apoio tecnológico e pesquisa cibernética.
- Estabelecimento de uma estrutura de gestão de pessoal e desenvolvimento de doutrina.
- Estabelecimento de uma estrutura voltada para atender às necessidades de inteligência no setor cibernético.

Definição da estrutura e missões do Centro de Defesa Cibernética do Exército, com base em seu Núcleo já ativo.

O Ministério da Justiça (MJ), (Amin,2016) em virtude de suas atribuições, também pode desempenhar um papel relevante no contexto da segurança de defesa cibernética, especialmente por meio do Departamento de Polícia Federal (DPF). Um exemplo concreto dessa atuação é a repressão aos crimes cometidos no espaço cibernético.

Outra instituição de grande relevância no contexto da segurança cibernética é o Tribunal de Contas da União (TCU), que dedica especial atenção à gestão pública relacionada à segurança da informação e à qualidade dos sistemas de informação disponibilizados ao público. O TCU mantém a Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), uma entidade especializada na área que tem como objetivo fiscalizar a gestão e o uso dos recursos de Tecnologia da Informação (TI) na Administração Pública Federal (APF). A SEFTI desempenha um papel crucial ao desenvolver metodologias, manuais, notas técnicas e procedimentos para o planejamento e a execução de auditorias em TI. Além disso, ela promove um Diálogo Público de TI com a sociedade, o Congresso Nacional e os Gestores Públicos, demonstrando seu compromisso em garantir a integridade e eficiência dos sistemas de informação governamentais (TCU, 2008).

2. COOPERAÇÃO INTERNACIONAL EM DEFESA CIBERNÉTICA

O conceito de cooperação internacional é central nas teorias realista e liberal das relações internacionais, mas essas abordagens oferecem perspectivas distintas sobre como a cooperação se desenvolve e é sustentada. De acordo com a teoria realista, as relações internacionais são caracterizadas pela competição e pela busca de interesses nacionais próprios. A cooperação é vista como uma estratégia de curto prazo, muitas vezes baseada na balança de poder e no equilíbrio de forças. Para os realistas, a cooperação internacional é frequentemente frágil e efêmera, pois os Estados estão sempre preocupados com a segurança e a maximização de seu poder relativo. Por outro lado, o liberalismo destaca a capacidade de os Estados cooperarem em uma base mais duradoura e mutuamente benéfica. Os liberais argumentam que a cooperação internacional pode ser alcançada por meio de instituições internacionais, acordos e regimes que promovam normas compartilhadas e valores comuns. A ênfase está na interdependência econômica, na diplomacia e na resolução pacífica de conflitos. Os liberais veem a cooperação como um meio eficaz de promover a paz e a prosperidade global, pois acreditam que os Estados podem encontrar maneiras de superar os obstáculos que os realistas consideram intransponíveis. (Jackson; Sorensen, 2007)

As teorias realista e liberal oferecem perspectivas contrastantes sobre o conceito de cooperação internacional. Enquanto os realistas veem a cooperação como um fenômeno frágil e muitas vezes limitado pela busca de interesses nacionais, os liberais enfatizam a capacidade de os Estados cooperarem de forma mais sustentável, graças a instituições e mecanismos que promovem a interdependência e a diplomacia. A realidade das relações internacionais muitas vezes envolve uma combinação de ambas as abordagens, com períodos de competição e cooperação, refletindo a complexidade das dinâmicas globais. (Jackson; Sorensen, 2007)

No setor cibernético é possível verificar que a dinâmica de interação entre os Estados pode oscilar bastante entre competição e cooperação. Contudo, a cooperação internacional em defesa cibernética desempenha um papel fundamental na proteção das infraestruturas críticas e na garantia da segurança digital em um mundo cada vez mais interconectado. Em primeiro lugar, a natureza transnacional das ameaças cibernéticas exige uma abordagem colaborativa entre nações. Ataques cibernéticos podem originar-se em qualquer lugar do mundo e atingir alvos em diferentes países, tornando imperativo o compartilhamento de informações e a coordenação entre governos, organizações internacionais e empresas privadas.

Além disso, a cooperação internacional em defesa cibernética envolve o desenvolvimento de normas e acordos comuns que estabelecem as regras do jogo no

ciberespaço. Acordos como o Tratado de Budapeste sobre Crimes Cibernéticos e a Convenção de Haia sobre o Cibercrime promovem a cooperação em investigações e processos judiciais relacionados a crimes cibernéticos, criando um ambiente jurídico global mais coeso.

A troca de melhores práticas e a capacitação mútua também são elementos-chave da cooperação em defesa cibernética. Países mais avançados em termos de segurança cibernética podem ajudar na formação e no fortalecimento das capacidades de nações em desenvolvimento, reduzindo assim a lacuna global em matéria de segurança digital.

A cooperação em defesa cibernética não se limita apenas a governos e organizações internacionais. Empresas do setor privado desempenham um papel significativo na defesa cibernética, uma vez que muitas infraestruturas críticas estão em mãos privadas. Parcerias público-privadas são essenciais para garantir a resiliência cibernética em âmbito global. A cooperação internacional em defesa cibernética é relevante para enfrentar as ameaças em constante evolução no ciberespaço. Ela abrange compartilhamento de informações, desenvolvimento de normas, capacitação, e colaboração entre governos e empresas privadas, criando um ambiente mais seguro e resiliente no mundo digital.

O período compreendido entre os anos de 2009 a 2011 representou uma fase de atividades de notável importância para o desenvolvimento do setor cibernético brasileiro, marcada por colaborações internacionais com diversos países. Esses eventos desempenharam um papel fundamental na construção das capacidades e estratégias de segurança cibernética do Brasil, contribuindo para a sua postura no cenário global de cibersegurança.(Vianna; Camelo, 2020)

Durante esse período, o Brasil estabeleceu vínculos de cooperação com nações parceiras em questões relacionadas à segurança cibernética. Essas parcerias ajudaram a promover o compartilhamento de melhores práticas, troca de informações e capacitação no campo da cibersegurança. Além disso, essas colaborações fortaleceram a posição do Brasil no contexto internacional, permitindo que o país desempenhasse um papel mais ativo em fóruns e discussões globais relacionadas à cibersegurança. Na Figura 7 estão representados os marcos de cooperação internacional no setor de defesa cibernética entre os anos 2009 e 2011.

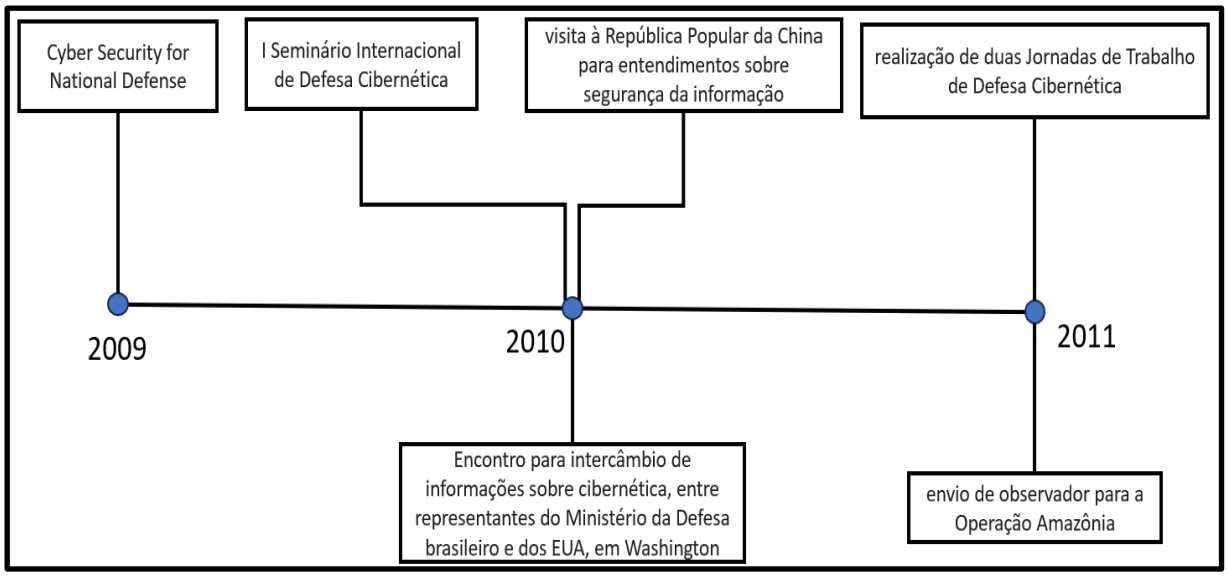

FIGURA 7. MARCOS DE COOPERAÇÃO INTERNACIONAL DE DEFESA CIBERNÉTICA ENTRE OS ANOS 2009 E 2011.
Fonte: Elaboração própria com base em Vianna; Camelo, 2020.

A identificação destes eventos como marcos da cooperação internacional em defesa cibernética foi identificada por Vianna e Camelo (2020). Nesse sentido, esses marcos ressaltam como o Brasil buscou estabelecer políticas que estiveram pautadas no fortalecimento da cooperação com outros Estados. Nos próximos tópicos serão detalhados os seguintes eventos: Cyber security for National Defense Summit, realizado em 2009; o Encontro para intercâmbio de informações sobre cibernética entre representantes do Ministério da Defesa brasileiro e do Departamento de Defesa dos Estados Unidos (DOD, sigla em inglês), ocorrido nos EUA, em 2010; I Seminário Internacional de Defesa Cibernética; a visita da Comitiva brasileira à República Popular da China para entendimentos sobre segurança da informação, ocorrida em 2010; por fim, a Operação Amazônia, em 2011.

2.1 Cyber Security for National Defense Summit 2009

Este simpósio, embora inicialmente pudesse parecer mais um evento técnico comum, destacou-se por duas características cruciais que moldaram a abordagem e a visão do Brasil em relação à segurança cibernética. A primeira característica notável foi a composição predominantemente norte-americana do público presente, composto por representantes de diversos setores do governo dos EUA. Isso proporcionou uma oportunidade rara para que os palestrantes e participantes abordassem abertamente questões sensíveis relacionadas a ataques

cibernéticos à infraestrutura crítica, desenvolvimentos científicos delicados e a necessidade de capacitação de pessoal. Essa transparência nas discussões sobre os desafios enfrentados pelos Estados Unidos na construção de seu próprio setor cibernético serviu como uma valiosa referência para a equipe brasileira. (Vianna; Camelo, 2020).

A segunda característica crucial do SUMMIT 2009 foi a notável semelhança entre as áreas prioritárias discutidas durante as palestras nos EUA e as escolhas estratégicas já estabelecidas no escopo de projeto enviado pelo Brasil ao Ministério da Defesa. Essa convergência de prioridades entre os dois países, desde o desenvolvimento de um arcabouço documental até a criação de uma estrutura de defesa cibernética, foi fundamental para alinhar as metas nacionais do Brasil com as melhores práticas internacionais.(Vianna; Camelo, 2023)

Essa experiência demonstrou a importância da cooperação internacional e da troca de conhecimento no campo da segurança cibernética. Ao aprender com os desafios e soluções enfrentados pelos Estados Unidos, o Brasil conseguiu modelar seu próprio desenvolvimento no setor cibernético de forma mais eficaz. Para a defesa cibernética do Brasil, essa colaboração global e a identificação de áreas de convergência com nações parceiras são cruciais para fortalecer suas capacidades e enfrentar as crescentes ameaças cibernéticas.

2.2 Intercâmbio de informações sobre cibernética nos EUA

Em 2010, o encontro de intercâmbio de informações sobre cibernética entre o Ministério da Defesa brasileiro e o Department of Defense dos Estados Unidos (US DoD) desempenhou um papel crucial na compreensão dos elementos não classificados da estratégia do DoD para a cibernética. A estratégia do DoD destacou cinco pilares essenciais que influenciaram diretamente a abordagem brasileira para a defesa cibernética:

- Ciberespaço como um Domínio: O reconhecimento do ciberespaço como um domínio estratégico ressaltou a importância de garantir a segurança nesse ambiente digital, equiparando-o aos domínios tradicionais de terra, mar, ar e espaço.
- Combate no Espaço Cibernético: A ênfase em conceitos operacionais no campo da defesa cibernética revelou a necessidade de desenvolver capacidades para combater ameaças cibernéticas de maneira eficaz e proativa.
- Extensão da Defesa Cibernética: A ampliação da defesa cibernética para órgãos governamentais e parte do setor privado, especialmente infraestruturas críticas, demonstrou a importância de proteger não apenas as instituições governamentais, mas também os sistemas vitais para o funcionamento do país.

- Parcerias Internacionais, Tecnologia e Inovação: O reconhecimento da necessidade de colaboração internacional, adoção de tecnologias avançadas e incentivo à inovação destacou a importância de estar atualizado com as melhores práticas globais em segurança cibernética.
- Prioridade em Pesquisa, Desenvolvimento e Inovação (P, D&I): O foco em P, D&I na área de ciência e tecnologia evidenciou a necessidade de investimentos contínuos em pesquisa e desenvolvimento para manter e aprimorar as capacidades cibernéticas.

Outro aspecto crucial da missão foi a visita ao Department of Homeland Security (US DHS), onde a interação com a equipe do US-Cert (United States Computer Emergency Response Team) permitiu à delegação brasileira entender as complexidades de implementar um programa abrangente de conscientização em cibersegurança nas áreas governamentais civis. Além disso, a videoconferência com o CCIRC (Canadian Cyber Incident Response Centre), principal Computer Security Incident Response Teams (CSIRT) canadense, proporcionou valiosas lições aprendidas nos Jogos de Inverno de Vancouver, destacando a importância da colaboração internacional.

A visita ao Department of Cyber Crime Center (DC3), onde foram observados trabalhos de perícia forense e capacitação técnica de pessoal, bem como a ida à National Defense University (NDU), onde laboratórios e programas acadêmicos relacionados à defesa cibernética foram apresentados, acrescentaram perspectivas importantes ao entendimento do Brasil sobre como fortalecer suas capacidades nesse campo.(Vianna; Camelo, 2020)

2.3 I Seminário Internacional de Defesa Cibernética

Realizado entre 21 e 24 de junho de 2010, representou um marco fundamental na construção da estratégia de defesa cibernética do Brasil. Este evento foi dividido em dois momentos essenciais para o desenvolvimento dessa estratégia.

No primeiro momento, de caráter político-estratégico, o seminário reuniu palestrantes e participantes dos setores público e privado, bem como membros da comunidade acadêmica, todos eles ligados principalmente às infraestruturas críticas. Essa abordagem multidisciplinar demonstrou a compreensão de que a defesa cibernética não é apenas uma preocupação militar, mas uma questão que envolve todo o tecido social e econômico do país. A participação do Ministério da Defesa (MD) nesse contexto enfatizou a importância que o governo brasileiro atribuía à segurança cibernética.

No segundo momento, o foco se voltou para a esfera militar, abordando a situação do setor cibernético dentro das Forças Armadas. Esse segmento específico do seminário permitiu uma análise aprofundada das questões relacionadas a pessoal, doutrina, estruturas e tecnologia nas Forças Armadas brasileiras. Esses debates desempenharam um papel crucial na formulação de estratégias e políticas direcionadas ao desenvolvimento das capacidades cibernéticas militares do país.

A partir dessas discussões, foi elaborada uma "nota de coordenação doutrinária" interna ao Exército. Este documento serviu como um dos pilares de referência para a implantação do setor cibernético no Brasil. Ele consolidou os princípios e diretrizes necessários para a construção das capacidades de defesa cibernética das Forças Armadas, bem como sua integração com os esforços globais de segurança cibernética. (Vianna; Camelo, 2020).

2.4 Visita de comitiva à República Popular da China

A visita à República Popular da China em 2010 fortaleceu o intercâmbio bilateral entre o Brasil e a China no campo da segurança do espaço informacional. Essa iniciativa teve como destaque a participação de um membro da equipe original que desempenhou um papel fundamental na especificação do setor cibernético brasileiro e na supervisão de um de seus projetos-chave.

Uma das contribuições mais significativas dessa visita foi a oportunidade de adquirir conhecimento sobre a forma de gestão da segurança da informação pelo governo chinês. Embora a interação tenha ocorrido sob certas restrições, as áreas abrangidas durante a visita foram abrangentes e abordaram aspectos cruciais da segurança cibernética. Isso incluiu:

- Gestão de Nível Governamental: A visita permitiu ao Brasil entender como o governo chinês estrutura e gerencia a segurança da informação em nível governamental. Esse conhecimento é vital para o desenvolvimento de políticas e estratégias eficazes de segurança cibernética no país.
- Pesquisa e Desenvolvimento: O intercâmbio abrangeu as atividades de pesquisa e desenvolvimento em segurança cibernética. Isso ofereceu ao Brasil insights sobre as áreas de pesquisa prioritárias e as iniciativas que poderiam ser replicadas ou adaptadas para atender às necessidades nacionais.
- Infraestrutura de TI: A compreensão da infraestrutura de tecnologia da informação na China permitiu ao Brasil avaliar as melhores práticas em termos de proteção de sistemas e redes críticas.

- Indústria de Segurança da Informação: A visita também abordou a indústria de segurança da informação na China, destacando oportunidades de colaboração com empresas do setor e identificando soluções inovadoras em segurança cibernética.
- Formação de Especialistas: Conhecer os programas de formação de especialistas em segurança cibernética na China ofereceu ao Brasil insights valiosos sobre como desenvolver sua própria força de trabalho altamente qualificada nesse campo.

A visita à China em 2010 desempenhou um papel crucial na capacitação do Brasil para fortalecer suas defesas cibernéticas e promover a cooperação internacional nessa área vital. Essa troca de conhecimento e experiência contribuiu para o aprimoramento das políticas e estratégias de segurança cibernética no Brasil, preparando o país para enfrentar ameaças cada vez mais complexas no ciberespaço. A colaboração contínua com nações parceiras, como a China, continua sendo uma parte essencial da defesa cibernética do Brasil, à medida que o país se esforça para proteger sua infraestrutura crítica e garantir a segurança de suas operações no mundo digital.(Vianna; Camelo, 2020)

2.5 Operação Amazônia (2011)

Em 2011, durante os estágios iniciais da criação do Centro de Defesa Cibernética (CDCiber), o Núcleo do Centro de Defesa Cibernética (NuCDCiber) do Exército adotou uma abordagem proativa ao enviar um observador para analisar e avaliar como as equipes de defesa cibernética poderiam contribuir significativamente para as operações de combate simulado e, ao mesmo tempo, estar preparadas para enfrentar situações reais.

O objetivo era entender como as capacidades de defesa cibernética poderiam ser integradas de maneira eficaz nos exercícios de adestramento conduzidos pelo Ministério da Defesa (MD). Esses exercícios, realizados a partir de 2012, desempenharam um papel vital no aprimoramento das habilidades das Forças Armadas brasileiras, seguindo uma metodologia que visava testar tanto a capacidade do Estado-Maior Conjunto em tomar decisões diante de cenários simulados de conflito quanto a capacidade da tropa no terreno de executar operações que se assemelhassem o máximo possível a situações reais.

Essa integração permanente de exercícios de defesa cibernética nos programas de treinamento do MD representou um avanço significativo na preparação das Forças Armadas para enfrentar ameaças cibernéticas. Essas simulações proporcionaram às equipes de defesa cibernética uma compreensão prática das complexidades envolvidas na proteção das

infraestruturas críticas e na garantia da segurança das operações militares no ambiente digital.(Vianna; Camelo, 2020)

2.6 Jornadas de Trabalho de Defesa Cibernética

No segundo semestre de 2011, marcam-se dois eventos cruciais que tiveram um impacto significativo no desenvolvimento da defesa cibernética no Brasil. Estas jornadas de trabalho, realizadas em julho e setembro de 2011, foram organizadas pelo Exército Brasileiro/Ministério da Defesa em colaboração com a Secretaria de Política de Informática do Ministério da Ciência, Tecnologia e Inovação. Elas contaram com uma ampla participação de órgãos do governo federal, comunidade acadêmica e empresas envolvidas em segurança da informação digital.

A primeira jornada teve uma importância tão grande que contou com a presença do então Ministro da Ciência, Tecnologia e Inovação, que não apenas elogiou o evento, mas também destacou o compromisso do Ministério em investir recursos na área. Essas jornadas tinham como premissas orientadoras: abordar a multidisciplinaridade e as diversas aplicações da cibersegurança, estimular a indústria nacional de defesa, incentivar a produção de sistemas inovadores no país e desenvolver componentes críticos de forma nacional.

Como resultado dessas jornadas, quatro programas de trabalho foram estruturados para fortalecer a defesa cibernética no Brasil: (i) Desenvolvimento de um Sistema Modular de Soluções de Tecnologia da Informação; (ii) Investimento em Supercomputação (computação de alto desempenho - CAD); (iii) Criação da Escola Nacional de Defesa Cibernética (ENaDCiber); e (iv) Implementação de um Sistema de Proteção para ambientes computacionais.

Paralelamente a essas atividades, o Núcleo de Centro de Defesa Cibernética começou a preparar as equipes de defesa cibernética das Forças Armadas para participarem da segurança cibernética da Rio+20 em junho de 2012. Esse novo desafio envolveu reuniões preparatórias com o Comitê Nacional de Organização da Rio+20 e outros parceiros externos para configurar a Central de Monitoramento Cibernético do CDCiber.

Esses esforços demonstram o compromisso do Brasil em fortalecer sua capacidade de defesa cibernética, abordando não apenas questões militares, mas também a necessidade de desenvolver uma infraestrutura de segurança digital sólida para proteger seus interesses nacionais e garantir a segurança no ciberespaço. O investimento em pesquisa, inovação e treinamento, bem como a colaboração entre diferentes setores, desempenham um papel fundamental na construção de uma estratégia de defesa cibernética eficaz e resiliente. É

essencial continuar aprimorando essas iniciativas para enfrentar as ameaças cibernéticas em constante evolução. (Vianna; Camelo, 2020).

2.7 Caso Snowden em 2013 e seus impactos na cooperação Brasil Estados Unidos em matéria de segurança e defesa cibernética

Edward Snowden, um ex-analista de sistemas que trabalhou como administrador de sistemas na Central de Inteligência Americana (CIA) e posteriormente como contratado da Agência de Segurança Nacional (NSA), desempenhou um papel significativo na exposição pública do projeto PRISM. Este projeto era um programa de espionagem global e sistemática dos meios de comunicação, orquestrado pela NSA dos Estados Unidos. Em 2013, Snowden revelou detalhes alarmantes, acusando a NSA de desenvolver uma infraestrutura tecnológica capaz de interceptar virtualmente qualquer tipo de informação. Tal aparato possibilitaria o rastreamento automático das comunicações de qualquer pessoa, sem nenhum controle prévio.

Após a divulgação dessas informações, o governo norte-americano acusou Snowden de espionagem e revogou seu passaporte. Isso o forçou a buscar refúgio em Moscou, na Rússia, onde vive desde então. Durante entrevistas, Snowden apresentou evidências de que a NSA estava monitorando milhões de telefones e dados de usuários online nos Estados Unidos e em outros países. Além disso, alegou que a NSA tinha acesso aos servidores de grandes empresas, como Google, Skype, Facebook e Apple, como parte do programa de espionagem PRISM, permitindo aos agentes coletar uma ampla gama de informações, incluindo histórico de navegação na internet, conteúdo de e-mails, conversas de chat e transferências de arquivos. Como resultado dessas revelações, ficou evidente que o Brasil teve 2.3 bilhões de telefonemas e mensagens de e-mails espionados (Pilati; Olivo, 2014).

O que se tornou claro com a liberação dos documentos que comprovaram a existência do PRISM foi que os alvos do programa eram muito mais diversificados do que inicialmente havia sido imaginado, incluindo figuras de alto escalão, como a Chanceler da Alemanha, Angela Merkel, e a então Presidente do Brasil, Dilma Rousseff, cujas comunicações telefônicas e eletrônicas foram alvo direto da espionagem (Teixeira; Datysgeld, 2016).

Após o incidente de espionagem, a então Presidente da República do Brasil, Dilma Rousseff, cancelou sua visita planejada a Washington em outubro de 2013. A princípio, as relações bilaterais entre o Brasil e os Estados Unidos esfriaram, já que a presidente não solicitou desculpas ao governo norte-americano e não recebeu explicações substanciais. No entanto, esse episódio não resultou em uma ruptura permanente, e as relações entre os dois países foram

gradualmente restauradas, abrindo caminho para a cooperação em várias áreas, incluindo economia, energia e defesa.

De acordo com o Ministério da Defesa do Brasil (2015), houve um esforço por parte do setor político brasileiro e do então Ministro da Defesa, Jaques Wagner, para buscar cooperação em segurança e defesa antes da visita da Presidente Dilma Rousseff a Washington. O Senado e a Câmara brasileira aprovaram dois acordos em 25 de junho de 2015: um relacionado às medidas de segurança para a proteção de informações militares sigilosas e outro sobre a cooperação em defesa entre os dois países. Esses acordos haviam sido assinados em 2010, mas precisaram de ajustes devido à Lei de Acesso à Informação (LAI), que entrou em vigor no Brasil em 2011.

O primeiro acordo diz respeito ao sigilo de informações militares e visa impulsionar parcerias comerciais e industriais, garantindo a proteção das informações militares abrangidas em contratos, sem prejudicar a legislação nacional das partes em relação ao acesso público a documentos e informações públicas, à proteção de dados pessoais e às informações classificadas.

O segundo acordo, o Projeto de Decreto Legislativo nº 256, trata da cooperação em matéria de defesa. Seu principal objetivo é promover a cooperação, troca de informações e experiências, em conformidade com as leis e regulamentos nacionais e as obrigações internacionais das partes. Isso inclui a participação em treinamento militar conjunto, exercícios militares conjuntos e intercâmbio de informações, bem como a colaboração em áreas militares de interesse mútuo. Esses acordos aprofundaram a parceria Brasil-EUA na área de defesa.

Em 2017, o Ministério da Defesa do Brasil e o Departamento de Defesa dos Estados Unidos concluíram os termos do Convênio para Intercâmbio de Informações em Pesquisa e Desenvolvimento (MIEA), um acordo fundamental para permitir que os dois países conduzam projetos conjuntos de desenvolvimento tecnológico. Esses avanços nas relações de cooperação militar incluíram também o Acordo de Apoio Logístico e Serviços de 2018.

Após o caso de espionagem, Brasil e Estados Unidos encontraram maneiras de fortalecer sua cooperação em diversas áreas, incluindo segurança cibernética e defesa, restabelecendo relações diplomáticas e buscando um entendimento mútuo sobre governança global da Internet. Esses acordos e cooperações visam proteger os interesses de ambos os países em um mundo cada vez mais conectado e dependente da tecnologia (DEFESANET, 2018).

2.8 A cooperação entre o Brasil e os Estados Unidos no campo da segurança cibernética pós o caso Snowden

A cooperação entre o Brasil e os Estados Unidos no campo da segurança cibernética tem se desenvolvido de forma significativa nos últimos anos, especialmente por meio da parceria entre a Rede Nacional de Pesquisa (RNP) brasileira e a Directorate for Computer & Information Science & Engineering (CISE) da US National Science Foundation (NSF). Essa colaboração, que começou em 2016, tem como objetivo principal promover a pesquisa e o desenvolvimento conjunto em segurança cibernética, abrangendo áreas como segurança de rede, internet das coisas (IoT), sistemas ciber-humanos, ciber-físicos e detecção de malware.

O projeto "HealthSense: Assessing and Protecting Privacy in Wireless Wearable Sensor-generated Medical Data" visa garantir a privacidade e a confidencialidade dos dados médicos gerados por dispositivos vestíveis (wearables) e transmitidos para repositórios de dados centralizados. Isso não apenas protege a privacidade dos indivíduos, mas também evita que informações médicas críticas de figuras públicas, como o Presidente, sejam acessadas por terceiros não autorizados, minimizando riscos à sua segurança pessoal.

O projeto "Lightweight Policy Enforcement of Information Flows in IoT Infrastructures" tem o objetivo de fortalecer a segurança dos sistemas IoT, incluindo a detecção de dispositivos comprometidos e a caracterização de seu comportamento. Isso é fundamental para evitar que dispositivos conectados sejam explorados por atores maliciosos que possam usá-los para ataques ou para coletar informações sensíveis.

O projeto "Researching Internet Routing Security in the Wild" visa melhorar a segurança do roteamento na Internet, identificando redes vulneráveis a ataques DDoS e interceptação de dados. Essa iniciativa tem implicações diretas na capacidade do Estado de proteger sua infraestrutura crítica e coordenar operações militares de forma segura.

O projeto "Securing Networks in the Programmable Data Plane Era" busca criar técnicas de verificação de rede e serviços de segurança que garantam a integridade das redes de próxima geração. Isso é crucial para a segurança nacional, pois redes vulneráveis podem ser exploradas para interromper a comunicação e a coordenação de políticas e movimentos militares.

Embora esses projetos não tenham como objetivo primário a defesa nacional, eles desempenham um papel fundamental na proteção dos dados dos indivíduos e, por extensão, na segurança do Estado brasileiro. Investir em pesquisa e desenvolvimento nessa área é essencial para enfrentar ameaças cibernéticas em constante evolução e garantir a soberania digital do

país. É importante continuar a promover a colaboração internacional para fortalecer ainda mais a defesa cibernética do Brasil.

2.9 Participação brasileira no Locked Shields 2022

Locked Sields é o maior exercício de defesa cibernética do mundo[35], a participação brasileira foi um marco importante para a segurança cibernética do Brasil e trouxe visibilidade internacional das capacidades tecnológicas do país. O Locked Shields é um evento desafiador que simula ataques cibernéticos a sistemas militares e civis, oferecendo um ambiente realista. Abaixo é possível ver a foto do evento do ano de 2023(Figura 8), para que equipes de defesa testem suas habilidades.

FIGURA 8. FOTO DO LOCKED SHIELDS REALIZADO NO ANO DE 2023 NA ESTÔNIA.
FONTE: HTTPS://WWW.NATO.INT/CPS/EN/NATOHQ/NEWS_194902.HTM?SELECTEDLOCALE=EN .

As atividades de simulação de ataques e defesa se desenrolam em um cenário fictício denominado Berylia, divisão das cores do LS de 2022 está representado na Figura 9. Nesse ambiente simulado, Berylia é alvo de ataques cibernéticos em larga escala, apresentando todos os desafios e consequências associados a essa situação. Sob a liderança do CCDCOE, as equipes participantes têm a missão de auxiliar Berylia a enfrentar essa crise cibernética.

[35] Disponível em https://www.defesanet.com.br/cyberwar/noticia/44330/locked-shields-2022-participacao-brasileira-no-maior-exercicio-cibernetico-do-mundo/ . Acesso em [03/10/2023].

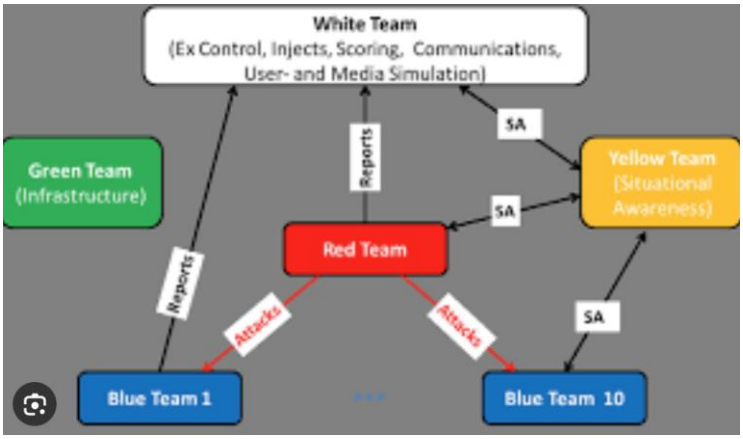

FIGURA 9. DIVISÃO DAS CORES DOS TIMES DO LOCKED SHIELDS 2022.
FONTE: HTTPS://WWW.DEFESANET.COM.BR/ .

A simulação abrange a proteção dos sistemas de tecnologia da informação e as infraestruturas críticas de Berylia (Figura 10).As equipes envolvidas devem demonstrar eficácia na identificação, relato e resolução de incidentes. Isso inclui a elaboração de estratégias para conter os ataques, exemplificado na Figura 11 e na Figura 12, conduzir investigações forenses, abordar questões legais, políticas e também comunicar efetivamente com a sociedade para lidar com os desafios decorrentes da situação de crise cibernética.

FIGURA 10. FOTO DA REPRESENTAÇÃO DAS INFRAESTRUTURA CRÍTICAS DE BERYLIA.
FONTE: HTTPS://WWW.DEFESANET.COM.BR/ .

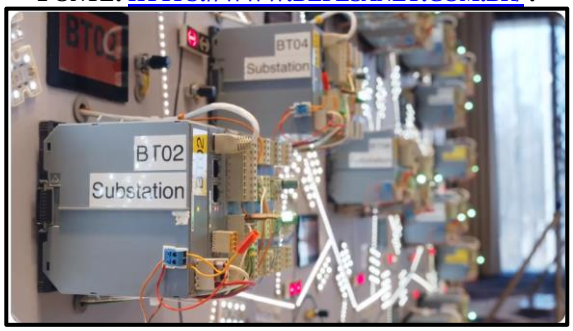

FIGURA 11. SIMULAÇÃO DE UMA SUBESTAÇÃO DE ENERGIA DE BERYLIA.
FONTE: HTTPS://WWW.DEFESANET.COM.BR/ .

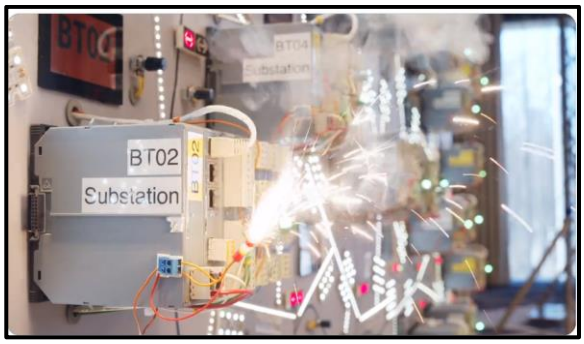

FIGURA 12. ÊXITO DO ATAQUE DO TIME VERMELHO À SUBESTAÇÃO DE ENERGIA DE BERYLIA.
FONTE: HTTPS://WWW.DEFESANET.COM.BR/ .

A ATECH[36], como única representante brasileira no evento, destacou-se ao fornecer um sistema de Comando e Controle para defesa antiaérea, como mostrado na Figura 13, que permite o processamento de informações de sensores e a tomada de decisões em vários níveis operacionais. Esse tipo de tecnologia não apenas contribui para a segurança cibernética global, mas também pode ser aplicado no âmbito militar e civil, fortalecendo a infraestrutura de defesa do Brasil.

A participação da ATECH, no Locked Shields demonstra não apenas sua excelência tecnológica, mas também sua capacidade de colaborar em um ambiente internacional de segurança cibernética. O exercício oferece à empresa a oportunidade de trocar conhecimentos e experiências com especialistas em segurança cibernética de todo o mundo, enriquecendo suas habilidades e conhecimentos. Essa troca de experiências é crucial para o aprimoramento das capacidades de segurança cibernética do Brasil.

[36] A ATECH é uma empresa do grupo EMBRAER, reconhecida com “System house” da Base Industrial de Defesa, possui expertise em engenharia de sistemas e tecnologias de consciência situacional e apoio a tomada de decisão, a ATECH trabalha no setor de soluções inovadoras com aplicações nas áreas de tráfego aéreo, gestão de ativos, segurança cibernética, conexões inteligentes, logística, sistemas de comando e controle, de instrumentação e controle, embarcados e simuladores. (ATECH, 2023).

FIGURA 13. A FOTO MOSTRA MEMBRO DO GREEN TEAM EM FRENTE A PAINEL DO ADS (AIR DEFENCE SYSTEM), DESENVOLVIDO PELA ATECH E AVIBRAS PARA O LS DE 2021
CRÉDITO: DIVULGAÇÃO / CCDCOE.
FONTE: HTTPS://WWW.DEFESANET.COM.BR/ .

A expertise da ATECH, na Figura 14 mostra detalhe do painel da ATECH, em sistemas de comando e controle, segurança cibernética e tecnologias de consciência situacional desempenha um papel fundamental na modernização das Forças Armadas e na gestão de infraestruturas críticas do país.

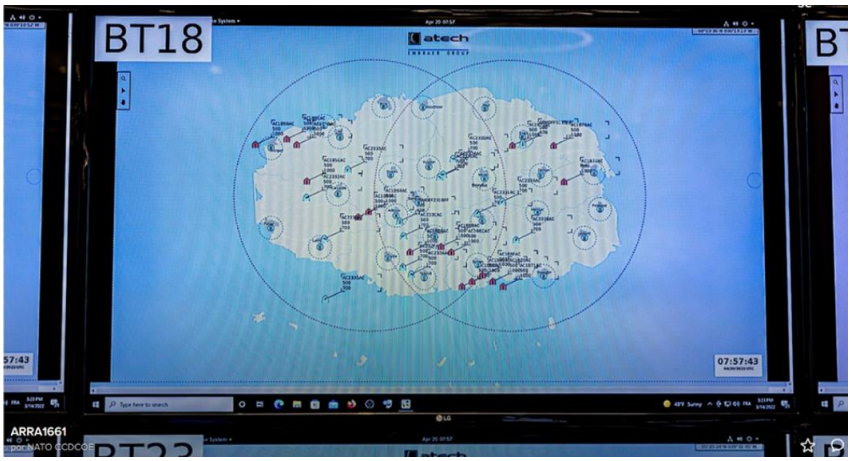

FIGURA 14. DETALHE DO PAINEL PAINEL DO ADS (AIR DEFENCE SYSTEM)
FONTE: HTTPS://WWW.DEFESANET.COM.BR/ .

De acordo com Kohl, representante da ATECH,

> Trocamos experiências com empresas e especialistas em segurança cibernética do mundo todo, enriquecendo nossas capacidades e habilidades. Aqui no Brasil, compartilhamos esse conhecimento com outros parceiros deste ecossistema. Por exemplo, no ano passado, quando participamos do Guardião Cibernético, exercício realizado pelo COMDCIBER (Comando de Defesa Cibernética), aplicamos toda a

> nova tecnologia que desenvolvemos no Locked Shields, claro que adaptada para este novo ambiente do exercício brasileiro.[37]

A participação da ATECH no Locked Shields não apenas promove a reputação do Brasil no cenário internacional de segurança cibernética, mas também contribui para o fortalecimento da defesa cibernética do país. É importante continuar incentivando e apoiando essas iniciativas para garantir a soberania digital do Brasil em um mundo cada vez mais conectado e digitalmente dependente.

[37] Disponível em https://www.defesanet.com.br/cyberwar/noticia/44330/locked-shields-2022-participacao-brasileira-no-maior-exercicio-cibernetico-do-mundo/ . Acesso em [03/10/2023].

3 O TRATAMENTO DE OPERAÇÕES CIBERNÉTICAS NO CONTEXTO DO DIREITO INTERNACIONAL

O ciberespaço tornou-se um domínio de operações vitais, moldando interações globais e gerando novos desafios e dinâmicas no cenário internacional. A integração da tecnologia nas tarefas diárias do Estado, suas agências e departamentos, especialmente no domínio cibernético, eleva questões de aplicabilidade do direito internacional e à soberania dos estados, pois a natureza sem fronteira da internet contrasta com conceitos tradicionais de jurisdição e território.

3.1 Jurisdição e Soberania

No domínio digital que é o ciberespaço, os princípios fundamentais de jurisdição e soberania, originados em um contexto geográfico e territorial, são confrontados com dilemas notáveis, como jurisdição transfronteiriça, soberania e controle, defesa e ataques cibernéticos regulamentação da informação proteção de dados e privacidade. Além disso, os princípios fundamentais clássicos são confrontados com dilemas multidimensionais como político, social, legal, econômico em diferentes escalas (NYE, 2014). A ausência de barreiras físicas e a natureza intrinsecamente global da internet precipitam uma série de questões relacionadas à jurisdição sobre crimes cibernéticos e à aplicação da soberania no ciberespaço (CONSELHO DA EUROPA, 2001).

3.1.1 Abordagem da soberania cibernética

A soberania no ciberespaço é objeto de interpretações variadas entre as nações, com algumas adotando uma postura mais restritiva e controlada, enquanto outras advogam por um ciberespaço mais aberto e menos regulamentado (ZHENG, 2017).

O episódio do Stuxnet, notório por ser o primeiro malware descoberto que foi projetado não apenas para espionar, mas para causar dano físico a infraestruturas críticas, no caso, o malware em questão causou danos significativos às instalações nucleares iranianas, alterando secretamente as velocidades dos centrífugos para causar danos físicos, enquanto enviava leituras normais aos operadores. O que evidencia como o ciberespaço pode ser utilizado para operações que têm profundas implicações na soberania e segurança nacional dos Estados (ZETTER, 2014; KASPERSKY, 2015).

O Brasil tem sido um ator proeminente nas discussões sobre governança da internet e soberania cibernética. A implementação do Marco Civil da Internet em 2014 destacou a posição do Brasil em favorecer um ciberespaço que respeita os direitos fundamentais, como a liberdade de expressão e a privacidade (BRASIL, 2014). O Marco Civil, muitas vezes referido como a "Constituição da Internet" do Brasil, defende princípios como a neutralidade da rede e estabelece um quadro legal para a proteção de dados e a privacidade dos usuários na internet. Por outro lado, a soberania cibernética no Brasil também envolve estratégias para proteger infraestruturas críticas e manter a integridade do ciberespaço nacional frente a ameaças cibernéticas (SANTOS, 2017).

A China adota uma perspectiva de soberania cibernética bastante distinta, enfatizando o controle estatal sobre o ciberespaço. A Lei de Cibersegurança da China, implementada em 2017, reflete essa postura, permitindo ao governo uma influência significativa sobre as operações da internet no país e reforçando a censura online (CHINA, 2016). A estratégia chinesa enfatiza a importância da governança da internet sob uma ótica nacionalista, vendo o controle do ciberespaço como uma extensão da soberania estatal (SEGAL, 2018).

Nos Estados Unidos, a abordagem à soberania cibernética é frequentemente pautada pela promoção de um ciberespaço aberto e seguro, onde a liberdade de expressão é um valor central. Contudo, essa visão também é complementada por uma estratégia robusta de ciberdefesa e ofensiva cibernética, como visto na Estratégia Nacional de Ciberespaço dos EUA (ESTADOS UNIDOS, 2018).

3.1.2 Dilemas da jurisdição

A questão da jurisdição é especialmente premente em crimes cibernéticos, onde um ato malicioso pode envolver diversas jurisdições nacionais e internacionais. A Convenção de Budapeste sobre Cibercrime, um tratado internacional, objetiva proporcionar uma resposta coesa e colaborativa para tais desafios, promovendo a cooperação internacional em resposta a crimes cibernéticos (CONSELHO DA EUROPA, 2001). Essa colaboração mútua para combater os crimes cibernéticos faz com que seja possível a troca de informação de forma muito mais rápida, podendo um país solicitar alguma informação de dados que esteja navegando em uma rede de outro país de forma muito mais rápida, o que antes era feito através de carta rogatória que as vezes o país nem cumpria a determinação da carta pois dependia de questões de soberania para o país aceitar ou não. Um exemplo prático da aplicação deste tratado pode ser observado na investigação de sites maliciosos que, embora estejam em português (br),

estão hospedados em servidores localizados em outros países. Antes da implementação do tratado, a localização física dos servidores em uma nação diferente poderia significativamente obstruir ou retardar investigações legais e esforços de responsabilização devido à necessidade de navegar por diversas legislações e processos judiciais internacionais.

A jurisdição cibernética tem implicações diretas na privacidade e nos direitos humanos. Os casos "Schrems I", em 2015 e "Schrems II", em 2020, que culminaram na invalidação respectivamente do Safe Harbor e do Privacy Shield entre a UE e os EUA. Ambos os casos foram fundamentados na premissa de que os mecanismos existentes para transferência de dados pessoais da UE para os EUA (primeiro o "Safe Harbor" e depois o "Privacy Shield") eram inadequados e ineficazes para proteger os direitos de privacidade dos cidadãos da UE, em grande parte devido às leis de vigilância dos EUA e à falta de recurso legal adequado para os indivíduos da UE em caso de má utilização dos dados, Schrems argumentou também que a legislação dos Estados Unidos permitia a ampla vigilância dos dados dos usuários por agências governamentais, como a NSA, violando os direitos de privacidade dos cidadãos da UE. Schrems baseou suas alegações na Carta dos Direitos Fundamentais da União Europeia, que protege o direito dos cidadãos à privacidade e à proteção de dados pessoais. Esse caso exemplifica como a jurisdição pode influenciar nas operações de transferência de dados e afetar a privacidade dos cidadãos (CJUE, 2020). Em ambos os casos a CJUE invalidou o acordo do “Safe Harbor” e “Privacy shield” mas no segundo caso manteve as Cláusulas Contratuais Padrão (CCPs).

3.2 Aplicação do Direito Internacional nas Operações Cibernéticas Estatais e as Perspectivas dos Estados Membros da Organização dos Estados Americanos (OEA)

Os parâmetros para a aplicação do direito internacional ao ciberespaço no contexto das operações cibernéticas estatais, destacando-se quatro pilares fundamentais: soberania e jurisdição, uso da força, direito internacional humanitário e direitos humanos (HOLLIS, 2020).

A soberania, manifestada no controle sobre o ciberespaço dentro das fronteiras nacionais, enfrenta desafios frente à natureza global da internet e à necessidade de cooperação internacional para a governança e segurança cibernética (HOLLIS, 2020).

Dada a amplitude e complexidade do ciberespaço, a definição de quando uma operação cibernética constitui um uso da força e quais são as respostas permitidas sob a Carta das Nações Unidas torna-se crucial para evitar escaladas conflituosas (OEA, 2020). A Carta, embora forneça uma estrutura para a manutenção da paz e da segurança internacionais, foi redigida em

uma era pré-digital, desafiando os juristas contemporâneos a interpretar seus princípios à luz das realidades cibernéticas contemporâneas. Operações cibernéticas, como ataques a infraestruturas críticas, podem ter impactos tangíveis e devastadores sem o uso da força militar convencional, lançando dúvidas sobre como tais ações se enquadram nas provisões tradicionais da Carta referentes ao uso da força (UNITED NATIONS, 1945).

A falta de consenso internacional sobre o que constitui um uso da força no ciberespaço e as respostas permitidas a essas ações adicionam uma camada de complexidade à governança global cibernética. Além disso, o anonimato potencial e as capacidades assimétricas inerentes ao ciberespaço desafiam as normas e práticas tradicionais de atribuição e resposta em cenários de conflito. Discussões e debates em foros internacionais sobre a necessidade de desenvolver normas específicas, ou até mesmo um tratado internacional dedicado para regular o comportamento dos Estados no ciberespaço, refletem a urgência e a importância desta questão no cenário geopolítico contemporâneo (HOLLIS, 2020).

A aplicação do direito internacional humanitário e a proteção dos direitos humanos no ciberespaço são imperativos para garantir que as operações cibernéticas estatais respeitem os princípios fundamentais do direito internacional (OEA, 2020).

As perspectivas dos estados membros da OEA são diversas e refletem suas políticas internas, capacidades cibernéticas e posicionamentos estratégicos. Os Estados Unidos, por exemplo, têm enfatizado a aplicabilidade do direito internacional ao ciberespaço, reservando o direito de responder a ataques cibernéticos significativos por todos os meios necessários (OEA, 2020). O Brasil tem focado na governança multilateral do ciberespaço, priorizando a inclusão digital e a proteção dos direitos humanos online (BRASIL, 2021). O México, por sua vez, busca uma abordagem cooperativa e coletiva para a segurança cibernética internacional, promovendo a paz e a segurança internacionais no ciberespaço (MÉXICO, 2021). Adicionalmente, nações como a Argentina e o Canadá têm enfatizado a necessidade de fortalecer a cooperação internacional e regional para enfrentar os desafios de segurança cibernética e promover um ciberespaço seguro e estável (OEA, 2020).

CONCLUSÃO

No entrelaçamento da era digital com a geopolítica contemporânea, a defesa cibernética surge como um pilar essencial na salvaguarda das nações contra ameaças multidimensionais no ciberespaço. Este trabalho explorou os diferentes aspectos e dinâmicas da defesa cibernética, desde seus fundamentos, exercícios conjuntos que promovem a transferência de conhecimento até as complexidades das operações cibernéticas no cenário internacional.

O primeiro capítulo lançou luz sobre os fundamentos da defesa cibernética, proporcionando uma base sólida para entender a natureza do espaço cibernético, esclarecer o significado de expressões utilizadas, as motivações por trás dos ataques cibernéticos, os desafios e estratégias inerentes à proteção dos ativos de informação e infraestruturas críticas. As nuances da defesa cibernética brasileira foram dissecadas, oferecendo uma visão das variáveis que sobre a governança brasileira e as políticas de defesa do Estado contra uma possível ameaça e a necessidade de um aparato de defesa robusto e resiliente.

O segundo capítulo abordou a cooperação internacional, a participação em fóruns e eventos globais, a aprendizagem com outros países e a aplicação prática de estratégias e tecnologias em exercícios nacionais e internacionais têm sido vitais para o desenvolvimento e fortalecimento da postura cibernética do Brasil. A trajetória ilustra o compromisso do Brasil com o desenvolvimento de capacidades cibernéticas robustas e resilientes, preparando o país para enfrentar as complexas ameaças cibernéticas do cenário global. Outra conclusão do capítulo é a necessidade de uma frente unificada contra ameaças cibernéticas transfronteiriças e a partilha de informações e recursos entre nações podem ter sido discutidos para destacar o valor da cooperação internacional.

O terceiro capítulo esclareceu sobre o tratamento de operações cibernéticas sob o escopo do direito internacional, trazendo à tona as complexidades e desafios associados à regulamentação e ao gerenciamento de atividades cibernéticas em uma arena global. O capítulo explorou os mecanismos legais, mostrando a visão de alguns países sobre normas e políticas que orientam as operações cibernéticas, o papel do direito internacional em estabelecer limites e como promover a justiça em um domínio tão volátil e não demarcado quanto o ciberespaço.

À medida que adentramos uma era onde o ciberespaço se tornará cada vez mais entrelaçado com a realidade geopolítica e social, os insights e análises derivados deste estudo servirão como um recurso valioso para pesquisadores, formuladores de políticas e profissionais de segurança cibernética, na busca constante por estratégias inovadoras e soluções pragmáticas para a defesa cibernética em um mundo progressivamente interconectado e digitalizado.

REFERÊNCIAS

AMIN, Esperidião. Comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país. **Relatório final.** [Online] 30 de março de 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125.

AYCOCK, John.. **Computer Viruses and Malware**. 2006.

BALKIN, Jack M., et al.. **Cybercrime:** Digital Cops in a Networked Environment (Ex Machina: Law, Technology, and Society, *4*. NY,United States : New York University Press, 2007.

BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B.. **Cibersegurança:** uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil digitalmente soberano. *FGV Direito Rio.* [Online] 2023. Disponível em: https://cyberbrics.info/wp-content/uploads/2023/03/Agenda-de-politicas-publicas-em-ciberseguranca-consolidado-primeira-final.pdf.

BRASIL. **Lei Nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [Online] 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. **Estratégia Nacional de Segurança Cibernética**. [Online] 2021. https://www.gov.br/gsi/pt-br/dsic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf.

CANONGIA, Claudia; GONÇALVES JÚNIOR, Admilson Gonçalves; MANDARINO JÚNIOR, Raphael. **Guia de referência para a segurança das infraestruturas críticas da informação.** [Online] 10 nov. 2010. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Brazil_2010_Orig_2_Guia_SICI.pdf.

CARVALHO, Paulo Sérgio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. **Coleção Meira Mattos-Revista das Ciências Militares**, 2011.

CGCSC, Centro Global de Capacidade de Segurança Cibernética. **Revisão Da Capacidade De Cibersegurança da Republica Federativa do Brasil.** [Online] 05 de Jun de 2020. Disponível em: https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf.

CHINA. **Cybersecurity Law of the People's Republic of China.** [Online] 2016. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

CJUE – CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. **Caso C-311/18:** Data Protection Commissioner v Facebook Ireland e Maximillian Schrems.Luxemburgo. [Online] 16 de Jul de

2020. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=8253507.

CLARKE, Richard A. **Cyber War:** the next threat to national security and what to do about it. New York : HarperCollins Publishers, 2010.

CONSELHO DA EUROPA. **Convenção sobre Cibercrime.** Budapeste. [Online] 23 de Nov de 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

DAI, Xinyuan; SNIDAL, Duncan; SAMPSON, Michael. International cooperation theory and international institutions. In: **Oxford Research Encyclopedia of International Studies**. 2010.

DEFESANET. **Brasil e EUA avançam em acordos bilaterais no setor espacial.** 2018. Disponível em: https://www.defesanet.com.br/br_usa/noticia/30218/brasil-e-eua-avancam-em-acordos-bilaterais-no-setor-espacial/.

DIETRICH, Jelena Mirkovic e Sven. **Internet Denial of Service:** Attack and Defense Mechanisms. s.l. : Prentice hall, 2015.

ERICKSON, Jon. 2008. **Hacking:** The Art of Exploitation, 2nd Edition. San Francisco : NO STARCH PRESS, 2008.

ESTADOS UNIDOS. **National Cyber Strategy of the United States of America.** [Online] 2018. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

HADNAGY, Christopher; Fincher, Michele. **Phishing Dark Waters:** The Offensive and Defensive Sides of Malicious Emails. s.l. : WILEY, 2015.

HOLLIS, Duncan B. **Derecho Internacional y Operaciones Cibernéticas del Estado:** Mejora de la Transparencia – Quinto Informe. *documento CJI/doc.615/20.* [Online] 7 ago. 2020. Disponível em: https://www.oas.org/es/sla/cji/docs/temas_culminados_recientemente_derecho_internacional_operaciones_ciberneticas_estado_INFORME_FINAL.pdf.

HUREL, Louise Marie; LOBATO, Luisa Cruz. Uma Estratégia para a Governança da Segurança Cibernética no Brasil. **Instituto Igarapé. Nota Estratégica**, v. 30, p. 1-32, 2018.

JACKSON, Robert; SORENSEN, Georg. **Introdução às relações internacionais.** Rio de Janeiro: Jorge Zahar, 2007.

JORDAN, Tim e TAYLOR, Paul. **Hacktivism and Cyberwars:** Rebels with a Cause? . 2004.

KASPERSKY. **A história do Stuxnet**. [Online] 2015. Disponível Em: https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/.

LANGNER, Ralph. **To Kill a Centrifuge:** A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Arlington : The Langner Group, 2013.

MEXICO. **La Estrategia Nacional de Ciberseguridad en México tiene más motivos económicos que de protección de datos.** OEA. [Online] 2021. Disponível em: https://www.eleconomista.com.mx/tecnologia/La-Estrategia-Nacional-de-Ciberseguridad-en-Mexico-tiene-mas-motivos-economicos-que-de-proteccion-de-datos-OEA-20220703-0001.html.

MINISTÉRIO DA DEFESA. **Política Nacional de Defesa e Estratégia Nacional de Defesa.** [Online] 31 de 08 de 2023. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf/view.

MANDERINO Jr.,Raphael **Segurança e Defesa do Espaço Cibernético Brasileiro**. Recife : CUBZAC, 2010.

NYE, S. J. **O futuro do poder.** São Paulo : Benvirá, 2014.

OLIVEIRA, João Roberto de. 2011. **Sistema de Segurança e Defesa Cibernética Nacional**. s.l. : Desafios Estratégicos, 2011.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Direito internacional e operações cibernéticas do estado.** OEA, Organização dos Estados Americanos. 2020. 2020, CJI/RES. 260 (XCVII-O/20).

PARTICIPAÇÃO brasileira no maior exervício cibernético do mundo. **Defesanet,** 26 abr. 2022. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/44330/locked-shields-2022-participacao-brasileira-no-maior-exercicio-cibernetico-do-mundo/.

PILATI, José; OLIVO, Isaac. **Um novo olhar sobre o Direito à Privacidade:** caso Snowden e pós-modernidade jurídica. *scielo.br.* [Online] 2014. Disponível em: https://www.scielo.br/j/seq/a/BKdjxJFTbXNPwJnnP4hk8kF/?lang=pt.

PORTELA, Lucas Soares. Geopolítica do espaço cibernético e o poder: o exercicio da soberania por meio do controle. Rio de Janeiro: s.n., 2018, **Revista Brasileira de Estudos de Defesa**, p. 141-165.

PRESIDÊNCIA DA REPÚBLICA, GABINETE DE SEGURANÇA INSTITUCIONAL. Comissão de Ciência e Tecnologia,Comunicação e Informática. **O Plano de Ação de Políticas de Segurança da Informação do Governo Federal.** [Online] 03 de Dez de 2014 Disponível em:. https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/apresentacoes-em-eventos/2014/2014-12-03-ap-plano-de-acao-de-politicas-de-seguranca-da-informacao-do-governo-federal/marconi-bezerra-gsi-pr.

RAZA, Salvador. Concepts matter in defense analysis? s.l. : **Defense and Security Analysis**, 2005, vol. 21, p. 67-78.

RICHARDSON, Ronny. Ransomware: Evolution, Mitigation and Prevention. **Faculty Publications**. 1 jan. 2017, p. 10-21.

SANTOS, Henrique F. A cibersegurança no Brasil: desafios e estratégias. **Conjuntura Global,** v. 6, n. 1, p. 163-180. [Online] jan/abr de 2017. https://revistas.ufpr.br/revistaconjuntura/article/view/52315.

SECRETARIA DE ASSUNTOS ESTRATÉGICOS. **Desafios estratégicos para a segurança e defesa cibernética.** [Online] 2011. Disponível em: https://livroaberto.ibict.br/bitstream/1/612/2/Desafios%20estrat%C3%A9gicos%20para%20seguran%C3%A7a%20e%20defesa%20cibern%C3%A9tica.pdf.

SEGAL, Adam. 2018. **The Code War:** America's Battle Against Russia, China, and the Rising Global Cyber Threat. New York : PublicAffairs, 2018.

SINGER, P.W. e Friedman, Allan. **Cybersecurity and Cyberwar:** What Everyone Needs to Know. s.l. : Oxford University Press, 2014.

TCU. **Boas práticas em Segurança da Informação**. Brasília : Tribunal de Contas da União, 2008.

TEIXEIRA, Carlos Gustavo Poggio; DATYSGELD, Mark William. **Os clientes diplomáticos e econômicos da espionagem digital estadunidense:** análise das ações contra o Conselho de Segurança da ONU e a Petrobras. 2016. Disponível em: . https://periodicos.pucminas.br/index.php/estudosinternacionais/article/view/P.2317-773X.2016v4n1p71/11021.

UNITED NATIONS. **Charter of the United Nations.** [Online] 1945. Disponível em: https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

VIANNA, Eduardo Wallier; CAMELO, José Ricardo Souza. DEFESA CIBERNÉTICA NO BRASIL: primícias de uma história de sucesso. **Revista da Escola Superior de Guerra**, v. 35, n. 75, p. 127-154, 2020.

ZETTER, K. **Countdown to Zero Day:** Stuxnet and the Launch of the World's First Digital Weapon. New York : Crown, 2014.

ZHENG, Y. 2017. **Governança da Internet na China:** conteúdo controlado. New York : Palgrave Macmillan, 2017.