CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
UNIVERSIDADE FEDERAL DA PARAÍBA
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

MARIA LUIZA ALVES ROCHA GALVÃO

UMA ANÁLISE DA DEFESA CIBERNÉTICA NO BRASIL: O PAPEL DO GUARDIÃO CIBERNÉTICO

JOÃO PESSOA
2025

MARIA LUIZA ALVES ROCHA GALVÃO

UMA ANÁLISE DA DEFESA CIBERNÉTICA NO BRASIL: O PAPEL DO GUARDIÃO CIBERNÉTICO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de bacharel em Relações Internacionais pela Universidade Federal da Paraíba.

Orientador: Prof. Dr. Augusto W. M. Teixeira Júnior.

JOÃO PESSOA

2025

Catalogação na publicação
Seção de Catalogação e Classificação

G182a Galvao, Maria Luiza Alves Rocha.
Uma análise da defesa cibernética no Brasil: o papel do Guardião Cibernético / Maria Luiza Alves Rocha Galvao. - João Pessoa, 2025.
47 f. : il.

Orientação: Augusto Wagner Menezes Teixeira Júnior.
TCC (Graduação) - UFPB/CCSA.

1. Ciberespaço. 2. Guerra cibernética. 3. Defesa cibernética. 4. Brasil. 5. Guardião Cibernético. I. Teixeira Júnior, Augusto Wagner Menezes. II. Título.

UFPB/CCSA CDU 327(043)

Elaborado por ANDRE DOMINGOS DA SILVA FERNANDES - CRB-15/00730

MARIA LUIZA ALVES ROCHA GALVÃO

UMA ANÁLISE DA DEFESA CIBERNÉTICA NO BRASIL: O PAPEL DO GUARDIÃO CIBERNÉTICO

Trabalho de Conclusão de Curdo apresentado ao Curso de Relações Internacionais do Centro de Ciências Sociais Aplicadas (CCSA) da Universidade Federal da Paraíba (UFPB), como requisito parcial para obtenção do grau de bacharel (a) em Relações Internacionais.

Aprovada em 15 de Abril de 2025

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
AUGUSTO WAGNER MENEZES TEIXEIRA JUNIOR
Data: 15/04/2025 12:11:22-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Augusto Wagner Menezes Teixeira Junior – (Orientador)
Universidade Federal da Paraíba - UFPB

Documento assinado digitalmente
gov.br
GILLS VILAR LOPES
Data: 15/04/2025 12:43:21-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Gills Vilar Lopes
Diretoria de Ensino da Aeronáutica -
Divisão de Planejamento de Ensino (DPE)

Documento assinado digitalmente
gov.br
MARIANA GRILLI BELINOTTE
Data: 15/04/2025 12:57:31-0300
Verifique em https://validar.iti.gov.br

Doutoranda Mariana Grilli Belinotte
Escola de Comando e Estado Maior do Exército (RJ)

RESUMO

O presente trabalho busca explorar, a partir de uma análise qualitativa, como o Exercício Guardião Cibernético pode contribuir no desenvolvimento da defesa cibernética brasileira. O exercício, coordenado pelo Comando de Defesa Cibernética, simula ataques cibernéticos a infraestruturas críticas, buscando preparar a defesa brasileira na mitigação ou bloqueio de possíveis ameaças, tais como Hacktivismo, Espionagem, Terrorismo e a própria Guerra Cibernética. Diante do aumento nos ataques cibernéticos no sistema internacional, principalmente ao Brasil, é fundamental compreender como o país se prepara para lidar com essas ameaças no ciberespaço. O projeto utiliza uma abordagem descritiva e exploratória, por meio de um estudo de caso, revisando a literatura sobre a defesa cibernética. Ao investigar a realização do exercício, busca-se explorar como ele contribui para o desenvolvimento das capacidades cibernéticas, fortalecendo a defesa nacional frente aos desafios contemporâneos.

Palavras-chave: Ciberespaço; Guerra Cibernética; Defesa Cibernética; Brasil; Guardião Cibernético.

ABSTRACT

The present work seeks to explore, based on a qualitative analysis, how the Cyber Guardian Exercise can contribute to the development of Brazilian cyber defense. The exercise, coordinated by the Cyber Defense Command, simulates cyberattacks on critical infrastructures, seeking to prepare Brazilian defense in mitigating or blocking possible threats, likewise Hacktivism, Espionage, Terrorism and the Cyberwar itself. Given the increase in cyberattacks in the international system, especially in Brazil, it is essential to understand how the country prepares to deal with these threats in cyberspace. The project uses a descriptive and exploratory approach, through a case study, reviewing the literature on cyber defense. By investigating the exercise, we seek to explore how it contributes to the development of cyber capabilities, strengthening national defense in the face of contemporary challenges.

Keywords: Cyberspace; Cyber-War; Cyber Defense; Brazil; Cyber Guardian.

LISTA DE ILUSTRAÇÕES

FIGURAS

Figura 1 – Sistema Militar de Defesa Cibernética..... 21
Figura 2 – Níveis do Setor Cibernético Brasileiro..... 23
Figura 3 – Os 5 países latino-americanos mais atacados por DDoS por hora..... 26
Figura 4 – Análise do Brasil pelo GCI..... 36

GRÁFICOS

Gráfico 1 – Identificação de *malwares* no período de um mês no Brasil..... 25
Gráfico 2 – Número de Participantes nas edições do EGC..... 34
Gráfico 3 – Porcentagem do nível de cumprimento das categorias do NCSI..... 37

LISTA DE ABREVIATURAS E SIGLAS

APF	Administração Pública Federal
CAC	Centro de Ações Cibernéticas
CCOC	Centro de Coordenação de Operações Cibernéticas
CDCiber	Centro de Defesa Cibernética
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CGE	Centro de Gestão Estratégica
ComDCiber	Comando de Defesa Cibernética
DCT	Departamento de Ciência e Tecnologia
E-Ciber	Estratégia Nacional de Segurança Cibernética
EGC	Exercício Guardião Cibernético
EMCFA	Estado-Maior Conjunto de Forças Armadas
ENaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
ESD	Escola Superior de Defesa
EUA	Estados Unidos da América
FA	Forças Armadas
GCI	Índice Global de Segurança Cibernética
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IC	Infraestruturas Críticas
ITU	União Internacional de Telecomunicações
MD	Ministério da Defesa
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PCD	Política Cibernética de Defesa
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
SIMOC	Simulador de Operações Cibernéticas
SMDC	Sistema Militar de Defesa Cibernética
TI	Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO **8**

2. A TEMÁTICA DA DEFESA CIBERNÉTICA **11**

2.1 O Ciberespaço 11

2.2 Doutrina Cibernética dos Países Não-Agressivos 14

2.3 Metodologia 15

3. A DEFESA CIBERNÉTICA NO BRASIL: O DESENVOLVIMENTO DO COMDCIBER **18**

3.1 A Política Nacional de Defesa e a Estratégia Nacional de Defesa 18

3.2 A Doutrina Militar de Defesa Cibernética Brasileira 19

3.3 O Comando de Defesa Cibernética 22

4. O GUARDIÃO CIBERNÉTICO: UMA ANÁLISE **26**

4.1 Exercícios de Simulação 27

4.2 Estruturação do Exercício Guardião Cibernético 28

4.3 Análise das edições do EGC (2018-2024) 30

5. CONSIDERAÇÕES FINAIS **39**

REFERÊNCIAS **42**

1. INTRODUÇÃO

A guerra, tradicionalmente travada em campos de batalhas físicos, descrita como a continuação da política por outros meios (Clausewitz, 2003), desloca-se cada vez mais para novos ambientes, incluindo o ciberespaço, ambiente no qual nações e grupos hostis utilizam-se das novas tecnologias para realizar ataques tão devastadores quanto os de métodos convencionais[1]. No ciberespaço, as fronteiras são difusas e os conflitos podem ocorrer entre atores de qualquer lugar do mundo, a qualquer momento e sem a necessidade de capacidades militares no mundo físico. Essa nova forma de guerra, muitas vezes denominada "guerra cibernética" não produz necessariamente derramamento de sangue, mas é capaz de desenvolver crises tão problemáticas quanto eventos de violência cinética.

A velocidade e a capacidade de causar danos massivos de maneira furtiva, muitas vezes sem que o autor da ação seja identificado, tornam o ambiente cibernético bastante inseguro. Além disso, estratégias ofensivas partindo desse meio podem incluir desinformação, espionagem e sabotagem, fazendo com que as demais nações sintam-se pressionadas a desenvolver novas doutrinas de defesa, investindo em maneiras de garantir a segurança de seus dados e dos seus cidadãos. Nesse contexto, a capacidade de adaptação e a inovação tecnológica de cada país se tornam essenciais para garantir a defesa nacional (Clarke; Knake, 2010).

Diante disso, percebe-se que, nas últimas décadas, o atual cenário que compõe o sistema internacional está cada vez mais atrelado às novas tecnologias e a maneira em que elas podem ser empregadas a conflitos em iminência, especialmente no que tange à inserção do ambiente cibernético em novas formas de se fazer a guerra. Somados a isso, os ataques cibernéticos realizados nas últimas décadas, tornam o problema mais tangível, sendo agora uma questão inserida nas agendas internacionais relacionadas à defesa e segurança nacional e internacional, e não mais sob uma roupagem meramente técnica. Exemplos notáveis incluem os ataques sofridos pela Estônia e pela Geórgia, causados pela Rússia em 2007 e 2008, respectivamente (Clarke; Knake, 2012).

O Brasil, sendo o país que mais sofre com ataques cibernéticos na América Latina (Netscout, 2024), também enfrenta uma realidade na qual a crescente digitalização de serviços e a dependência de tecnologias conectadas tornam as Infraestruturas Críticas (IC)[2] alvos

[1]Refere-se aos meios tradicionais de guerra, os quais envolvem combate físico e uso de armas convencionais (Andress; Winterfeld, 2014).
[2]Setores de transporte, energia, financeiros, serviços e telecomunicações (Vieira, 2023).

estratégicos para ciberataques. Essas ameaças têm o potencial de causar impactos significativos na economia, na segurança nacional e no bem-estar da população, destacando a necessidade de estratégias de defesa cibernética eficientes. Nesse contexto, torna-se fundamental avaliar as medidas que o Brasil tem adotado para aprimorar sua capacidade de resposta a essas ameaças, elevando sua segurança frente a esses desafios contemporâneos.

Nesse mesmo sentido, o Brasil detém a Política Cibernética de Defesa (PCD), aprovada em 2012, que estabelece diretrizes para a defesa cibernética do país, e foi desenhada para orientar a atuação das Forças Armadas e de outras instituições governamentais na proteção do espaço cibernético. Em 2014, um passo importante foi dado com a aprovação, pelo Ministério da Defesa, da implantação do Sistema Militar de Defesa Cibernética (SMDC). Esse sistema, sob a responsabilidade do Estado-Maior Conjunto das Forças Armadas (EMCFA), tem como órgão central o Comando de Defesa Cibernética (ComDCiber), e seu objetivo principal é assegurar o funcionamento seguro e eficaz do ambiente cibernético brasileiro, especialmente no que tange às IC do país. Para isso, são enfatizadas questões estratégicas e técnicas, como a execução de exercícios simuladores que permitem testar e aperfeiçoar as respostas às ameaças cibernéticas em um ambiente controlado.

A partir do ano de 2018, o ComDCiber passa a realizar, anualmente, exercícios do Guardião Cibernético (EGC), que se caracteriza por um estilo de jogo de simulação, que busca analisar e, posteriormente, avaliar, as capacidades de defesa das unidades responsáveis pelas IC do país (Vieira, 2023). Assim, em todas as suas realizações, são simulados diferentes cenários de adversidades dentro do ambiente cibernético que envolvam as principais IC brasileiras, e que, divididos em equipes, buscarão resoluções, por meio de cooperação interagências, por exemplo, que possam mitigar/bloquear as possíveis ameaças.

Nesse sentido, entende-se a importância de analisar de maneira mais aprofundada sobre o assunto em questão, uma vez que, a realização desse exercício reúne a atenção de diversos setores do país (públicos e privados), com a justificativa de aprimorar a defesa nacional. Assim, é fundamental que os esforços reunidos para o acontecimento das edições do exercício sejam aproveitados de maneira eficiente, a fim de garantir que haja um real desenvolvimento no fortalecimento das capacidades de defesa brasileira.

Dessa maneira, o presente trabalho tem por objetivo principal compreender a maneira em que o exercício “Guardião Cibernético” contribui na preparação da defesa brasileira no âmbito cibernético. Nesse prisma, busca-se responder a seguinte pergunta: qual o papel do exercício “Guardião Cibernético” no desenvolvimento da defesa cibernética do Brasil? Por conseguinte, os objetivos específicos a serem alcançados são os seguintes: (1) a realização de

uma revisão teórica e de literatura acerca da defesa cibernética; (2) descrição do EGC de maneira histórica e contextual na defesa brasileira; e (3) fazer uma análise acerca da contribuição do Exercício para a construção de capacidades para a defesa nacional brasileira.

Sendo assim, o presente trabalho está dividido em: introdução, seguida de uma seção teórico-metodológica, a seguir, o trabalho apresentará de que maneira está organizada a defesa cibernética no Brasil e por fim, a última seção será a análise do EGC em questão, e por fim serão realizadas as considerações finais acerca do que foi apresentado. Dessa forma, o trabalho permitirá o entendimento acerca da aplicação do exercício "Guardião Cibernético" como uma maneira de fortalecimento da Defesa Nacional e como contribuição para o desenvolvimento das capacidades estratégicas das Forças Armadas no que tange à defesa cibernética, na identificação de vulnerabilidades das IC, além do incentivo à cooperação inter-agências desenvolvendo uma ação mais coordenada entre as forças.

2. A TEMÁTICA DA DEFESA CIBERNÉTICA

O presente trabalho versa sobre o EGC, aqui com ênfase em seu papel dentro da realidade da Defesa brasileira. Nesse sentido, será realizada uma revisão da literatura buscando compreender quais são os autores que discutem sobre os seguintes objetos relacionados à Defesa Cibernética: ciberespaço; Contexto Internacional da Defesa Cibernética e a Doutrina Cibernética. No escopo desse trabalho, abordamos os conceitos da literatura que estão relacionados ao tema e suas respectivas definições. Assim, a revisão de literatura possibilitará a análise descritiva, apoiada por conceitos do campo, que apoiarão a descrição a atuação do EGC. Como produto, esperamos que essas informações possam contribuir na discussão acerca do fortalecimento da Defesa Cibernética do Brasil, a variável dependente, por meio da identificação das variáveis independentes, como o número de participantes e os setores envolvidos no EGC.

Após as definições tratadas acima, se desenvolverá o capítulo metodológico, no qual, o desenho de pesquisa em questão versará sobre um estudo de caso, tendo como objeto de análise o EGC. O objetivo central será examinar e identificar os mecanismos e práticas cibernéticas que contribuem para a defesa nacional. Desse modo, possibilitará uma investigação da maneira em que o exercício auxilia na capacitação dos profissionais da área, no aperfeiçoamento dos sistemas das IC e na criação de protocolos de resposta a incidentes cibernéticos. Também será possível avaliar como ele contribui para a preparação do Brasil no âmbito da Defesa Cibernética ao longo dos anos e seu impacto na formulação de políticas voltadas à cibersegurança.

2.1 O Ciberespaço

Ao passo que o desenvolvimento tecnológico cresce exponencialmente, o meio cibernético se torna cada vez mais intangível, carregando consigo uma série de incertezas sobre o futuro do sistema internacional. Na atualidade, todos os países devem estar atentos às possíveis ameaças provenientes de um novo ambiente – além da terra, do mar e do ar e do espaço exterior – o ciberespaço, que também consiste em um novo domínio de guerra. O ciberespaço é considerado um “espaço virtual, composto por dispositivos computacionais conectados em redes, ou não, onde as informações digitais transitam, são processadas e/ou armazenadas” (Brasil, 2023, p.17). Não obstante, entende-se que a afirmação da existência de uma guerra cibernética pode ser dúbia, pois há um debate sobre ser possível, ou não, denotá-la

de “guerra”, no entanto, é importante salientar que, de acordo com Clarke & Knake (2010), a guerra cibernética já é uma realidade, e tudo que foi visto até hoje são apenas situações sugestivas de tudo aquilo que pode ser feito a partir dela.

Não obstante, o ciberespaço é caracterizado por sua complexidade e pela dificuldade de estabelecer fronteiras físicas ou jurídicas claras (Lessig, 1999). Esse ambiente é composto por uma vasta infraestrutura de redes interconectadas, dentre elas, dispositivos digitais, sistemas de comunicação e informações armazenadas que podem ser transmitidas dentro dos meios eletrônicos. A natureza descentralizada desse ambiente e o anonimato das ações permitem que qualquer ator realize operações cibernéticas de maneira dissimulada. Dessa maneira, ataques cibernéticos podem ser lançados a partir de qualquer ponto do mundo, muitas vezes dificultando a atribuição de responsabilidade[3], desafiando cada vez mais os tomadores de decisão (Nye, 2017).

Além das ameaças diretas, como ataques visando a sobrecarga dos sistemas, o ciberespaço também possibilita operações que envolvem campanhas de desinformação, espionagem e manipulação de dados com o objetivo de comprometer a estabilidade política e econômica de uma nação (Rid, 2020). Ademais, a interdependência das IC faz com que um ataque cibernético bem-sucedido possa ter efeitos devastadores. Portanto, a defesa cibernética se expande para além das proteções de sistemas militares, como também para toda a esfera governamental e privada, o que exige a cooperação interagências[4], em que diversos setores participem na formulação e implementação de políticas robustas capazes de reforçar a defesa cibernética de um país.

Diante da nova realidade que se molda a partir do meio cibernético, possibilitando ataques na velocidade da luz com rápida escalada ao nível global, é necessária a construção de uma capacidade de defesa cibernética apta a responder a qualquer ameaça. No geral, a defesa cibernética, na área dos estudos estratégicos, está relacionada à preparação e a capacidade de resposta contra terceiros que possam comprometer a segurança do país. Assim, é indispensável a compreensão, em termos de medida, da defesa cibernética como critério fundamental para garantir o bloqueio e/ou mitigação de toda e qualquer ameaça à nação (Clarke; Knake, 2010).

No que concerne ao contexto geral da Defesa Cibernética no sistema internacional, entende-se, portanto, que as atividades hostis realizadas no ambiente cibernético podem ser

---

[3]Os atacantes podem usar servidores remotos, além de implantar falsas provas em servidores de qualquer país para se despistar (Nye, 2017).

[4] “Espaço para desenvolver de modo mais completo, aprimorar e aplicar políticas públicas com maior eficácia e eficiência” (Pagliari; Oliveira, 2014, p. 15)

configuradas como operações de rede de computadores, distintas em três variações: de ataque, de exploração e de defesa (Williams; McDonald, 2018), entretanto, como apresentado pela autora Elinor Sloan (2016), em seu livro: "Modern Military Strategy", uma guerra ofensiva, que envolve o espectro de ataque dentro do meio cibernético, era considerado tabu por muitos durante a década dos anos 1990. No contexto dos Estados Unidos da América (EUA), abordado pela obra, o debate da época girava em torno do real papel que o Departamento de Defesa possuía. Assim, depois de uma série de discussões, a defesa passa a ser entendida como uma força-tarefa conjunta cujo objetivo era proteger as redes de computadores militares, e mais tarde, responsável por realizar missões também ofensivas (Sloan, 2016).

No entanto, em razão dos ataques contra a Estônia e a Geórgia em 2007 e 2008, respectivamente, o foco em manter uma abordagem estritamente defensiva foi deixado de lado em função do risco que os países corriam com o avanço das tecnologias e das dependências a elas. Torna-se, então, necessário, não apenas, a construção de capacidades defensivas, mas também associá-las à criação de armas cibernéticas com objetivos ofensivos (Sloan, 2016). Dessa maneira, entende-se que há uma mudança de perspectiva de estratégia, partindo de defesas ativas[5] para ofensivas ativas.

Em contrapartida, a doutrina da Organização do Tratado do Atlântico Norte (OTAN) foca, principalmente, nas questões que se referem à defesa da rede de computadores. Assim, a OTAN busca maneiras de desenvolver suas capacidades para "detectar, avaliar, prevenir e recuperar em casos de um ciberataque" (Sloan, 2016, p. 89, tradução própria). Ou seja, para essa instituição, é dada uma maior ênfase para meios mais preventivos de defesa, embora parte de sua equipe de pesquisadores passaram a se atentar às questões ofensivas também.

Além disso, a OTAN reconhece a importância da resiliência cibernética, promovendo a colaboração entre os países-membros para garantir a proteção de IC e sistemas estratégicos contra ameaças digitais. Para isso, a organização investe constantemente em pesquisas, treinamentos e simulações de ataques cibernéticos, buscando aprimorar sua capacidade de resposta. Um exemplo disso é o *Locked Shields*, um dos maiores exercícios de ciberdefesa do mundo, realizado anualmente pelo *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) da OTAN.

A defesa cibernética pode ser pensada como instrumento indispensável para garantir a segurança de informações confidenciais de um Estado e de seus cidadãos. Dessa forma, as ações militares, uma vez que necessárias para exercer poder, também são fundamentais para preservar capacidades e liberdade de ação no ambiente cibernético, mantendo-se em prontidão

[5]Se refere à capacidade de um país estar pronto par responder a um ataque, e não o iniciar (Sloan, 2016).

para se defender de ataques iminentes (Libicki, 2009). É importante perceber que Libicki, em sua obra "*Cyberdeterrence and Cyberwar*", busca, não apenas, explicar como se deve ocasionar a ciberdefesa, mas também o porquê de sua importância.

De uma maneira geral, um sistema de redes forte em defesa necessita de robustez, pois é "a capacidade de extrair tanto poder militar de sistemas sob tensão como de sistemas livres de tensão" (Libicki, 2009, p. 162, tradução própria). Sendo assim, entende-se que a capacidade de um Estado de adaptação diante das circunstâncias é essencial para garantir a demonstração de sua capacidade de defesa. Ou seja, dentro dos sistemas de rede de um país, as ações militares devem operar independente da situação, da mesma maneira, buscando a neutralização de suas ameaças enquanto sistemas comprometidos estão em recuperação, minimizando todos os danos possíveis.

Entende-se, portanto, que um Estado, apesar de focar em questões ofensivas voltadas ao ciberespaço, deve destinar majoritariamente parte de seus recursos ao desenvolvimento de estratégias de defesa. Assim, é possível determinar que a defesa cibernética está relacionada a tudo aquilo necessário para evitar que os atacantes tenham sucesso em suas operações e, caso tenham êxito, mitigar a possibilidade de se beneficiarem das informações extraídas dos sistemas alvos (Libicki, 2009).

2.2 Doutrina Cibernética dos Países Não-Agressivos

No cenário global atual, marcado pela crescente complexidade das ameaças no ciberespaço, as nações precisam adotar posturas estratégicas para garantir sua segurança e soberania digital. No entanto, a maneira como cada país aborda a defesa cibernética varia em diversas formas, em especial, no que se refere às nações consideradas não agressivas (Malagutti, 2021). Esses países, ao invés de adotarem uma postura predominantemente ofensiva no domínio cibernético, optam por estratégias mais diplomáticas e cooperativas, buscando mitigar riscos sem recorrer ao confronto direto.

É importante reiterar que diferente desses países com postura essencialmente defensiva, os EUA adquirem uma abordagem mais proativa, principalmente pela sua Estratégia de Cibersegurança em conjunto com as ações de órgãos como o Comando Cibernético do país (USCYBERCOM). Países com esse perfil não buscam apenas investir na proteção de suas IC, mas também o desenvolvimento de capacidades para dissuasão e ataques cibernéticos preventivos contra possíveis adversários. Do mesmo modo, a OTAN, que

historicamente focou na defesa de redes, amplia sua atuação no que tange às ações ofensivas para responder estrategicamente ameaças emergentes (Arts, 2018).

Em contrapartida, Marcelo Malagutti, em "*Software Power as a Cyber-Dissuasion Tool for Non-Agressive Nations*", busca explicar o conceito de "*Software Power*" como a capacidade de um Estado em se inserir na disputa de poder do ambiente cibernético (Malagutti, 2021). Dessa forma, entende-se que esse grupo de países, apesar de refletirem suas diretrizes políticas e culturais de não-agressivos, podem e devem buscar sua imposição dentro do cenário cibernético global como maneira de garantir sua presença nos debates que giram em torno do assunto do ciberespaço.

Ao focar a análise do ambiente cibernético dos países não agressivos, entende-se que há uma forte tendência[6] a um modelo de resolução de conflitos mais passivo, de maneira que o diálogo seja a primeira opção (Malagutti, 2021). Assim, o Brasil, inserido nesse grupo de países não-agressivos, busca um posicionamento de menor confronto ao se relacionar com os demais. Essa característica brasileira está repetidamente explícita em diversos documentos oficiais, principalmente nos que se refere às tomadas de decisão da defesa brasileira, incluindo a defesa cibernética.

Logo, a ciberdefesa deve ser entendida como uma prioridade estratégica para todas as nações, independente de um perfil mais agressivo ou não no cenário internacional. No contexto atual, em que a dependência de sistemas digitais e a vulnerabilidade a ataques cibernéticos tendem a crescer cada vez mais, é indispensável que os países desenvolvam capacidades defensivas e ofensivas. No entanto, é fundamental que, no caso do Brasil, a defesa cibernética esteja alinhada aos princípios do próprio país e a busca por meios de reforçar o desenvolvimento das suas próprias capacidades, de modo a estar sempre preparado para o enfrentamento de possíveis ameaças no contexto cibernético. Dessa forma, a defesa brasileira será capaz de garantir, não apenas a segurança dos sistemas vitais do Estado, mas também, garantir a segurança de seus cidadãos.

2.3 Do estudo de caso do EGC

O presente trabalho se desenvolverá sob o enfoque de uma pesquisa qualitativa, em que o objetivo é investigar um fenômeno específico, configurando um estudo de caso (n=1). Segundo o autor Van Evera (1997), os estudos de caso exploram profundamente um

[6]Outros fatores somados também importam na caracterização do posicionamento das nações, como a cultura (Malagutti, 2021).

fenômeno em um contexto particular, ou seja, por meio deste, será possível explorar o fenômeno do fortalecimento da defesa nacional brasileira por meio do EGC e entender como o respectivo exercício contribui para o fortalecimento da defesa cibernética do país.

Além disso, é importante reafirmar que o estudo de caso é especialmente útil para compreender situações específicas a fim de explorar eventos contemporâneos, ele consiste no estudo aprofundado de um ou poucos objetos, a fim de garantir o conhecimento detalhado acerca do que será analisado (Gil, 2002). Por muito tempo acreditava-se que o estudo de caso não servia para investigações rigorosas, situação que muda na contemporaneidade, em que acredita-se na melhor adequação desse tipo de abordagem para investigar um fenômeno específico dentro de seu próprio contexto (Evera, 1997). Nesse sentido, a utilização do Estudo de Caso para essa análise permitirá:

> a) explorar situações da vida real cujos limites não estão claramente definidos; b) preservar o caráter unitário do objeto estudado; c) descrever a situação do contexto em que está sendo feita determinada investigação; d) formular hipóteses ou desenvolver teorias; e e) explicar as variáveis causais de determinado fenômeno em situações muito complexas que não possibilitam a utilização de levantamentos e experimentos (Gil, 2002, p. 54).

Assim, entende-se que o EGC seria um caso representativo do fenômeno da preparação da defesa brasileira, uma vez que se consolidou como um dos principais exercícios voltados ao aprimoramento das capacidades nacionais no domínio cibernético, é considerado o maior exercício simulado no hemisfério sul (Defesanet, 2021). O treinamento não apenas fortalece a cooperação entre instituições civis e militares, mas também proporciona um ambiente controlado para o desenvolvimento de estratégias e respostas eficazes diante de ameaças cibernéticas cada vez mais sofisticadas.

Para tanto, por meio da revisão de literatura, da contextualização descritiva acerca do surgimento do exercício e das análises posteriormente apresentadas, será possível compreender a contribuição deste objeto para a construção das capacidades brasileiras de defesa. Além disso, a sistematização das edições do EGC ao longo dos anos permite uma avaliação crítica sobre os avanços obtidos e os desafios enfrentados. Essa abordagem possibilita não apenas uma visão aprofundada do exercício, mas também uma reflexão da sua contínua execução e inovação das estratégias de defesa do Brasil.

Para a coleta de dados, o trabalho utilizou-se de fontes secundárias e primárias. As fontes secundárias estão relacionadas à revisão de literatura, em que será feita a busca por artigos que tratam sobre a Defesa Cibernética. Por outro lado, as fontes primárias consistem principalmente em documentos oficiais lançados pelo governo brasileiro acerca da realização

de edições do EGC. Esses dados são indispensáveis para compreender como o exercício é estruturado, os desafios a serem enfrentados e quais os resultados obtidos a partir de sua realização em termos de defesa nacional. A escolha dessas fontes se justifica pela necessidade de garantir maior confiabilidade e profundidade na análise.

Logo, a análise de dados será conduzida utilizando uma abordagem qualitativa, de maneira interpretativa, com o intuito de identificar padrões, e as relações que demonstrem o papel do EGC na defesa brasileira. Ademais, a análise seguirá utilizando os conceitos e argumentos identificados na revisão de literatura para reforçar o entendimento do objeto. Nesse sentido, a seguinte abordagem permitirá compreender como o EGC reflete as teorias apresentadas pelos autores selecionados, além de identificar as variáveis independentes do fenômeno. A variável dependente será o fortalecimento da defesa nacional, centrada aqui na defesa cibernética, enquanto as variáveis independentes incluíram os conceitos de operações no ciberespaço e as iniciativas de preparação cibernética.

Por fim, entende-se que a análise será realizada em etapas, começando pela organização dos dados e categorização das informações em tópicos relevantes, como objetivos do exercício e as atividades desenvolvidas. Em seguida, será feita a descrição da relação entre as práticas realizadas no exercício e os avanços na defesa cibernética nacional. Dessa forma, haverá a análise dos resultados, discutindo o que foi obtido em relação à literatura existente, às políticas de defesa cibernética do Brasil e relevantes índices internacionais com relação ao nível de desenvolvimento das capacidades de defesa cibernética, explorando como o EGC se insere e contribui para o contexto geral de defesa nacional.

3. A DEFESA CIBERNÉTICA NO BRASIL

A crescente digitalização das IC e o aumento das ameaças cibernéticas exigiram que o Brasil adotasse medidas estratégias para fortalecer sua segurança no ciberespaço. Nesse sentido, identifica-se a criação do ComDCiber como um marco fundamental na estruturação da defesa cibernética do país, visando a proteção de redes e sistemas essenciais para a soberania nacional. É importante destacar, portanto, os planos, diretrizes e estratégias que consolidam a relevante papel que o Comando tem no fortalecimento das capacidades de defesa brasileira.

3.1 A Política Nacional de Defesa e a Estratégia Nacional de Defesa

Inicialmente, é válido salientar que, ao nível político, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é responsável pela Segurança Cibernética do país diante do aumento das ameaças digitais. Nesse contexto, entende-se que o GSI desempenha papel fundamental na formulação e implementação de políticas voltadas à proteção dos sistemas governamentais no âmbito da segurança, um exemplo prático de suas ações voltadas para a segurança nacional foi a criação do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, o qual monitora e responde a incidentes cibernéticos que podem afetar, não apenas a Administração Pública Federal (APF), mas também a sociedade civil (Brasil, 2025).

Entretanto, no que concerne ao âmbito da Defesa Cibernética e considerando o Brasil um país pacífico no cenário internacional – virtude a qual o Estado brasileiro busca reafirmar com o passar dos anos –, é importante salientar que, mesmo mantendo essa postura, o país busca a implementação de políticas que garantam ao Estado brasileiro o cumprimento de seus objetivos, a fim de se defender de qualquer possível ameaça, de modo a assegurar o patrimônio nacional e a integridade territorial (Brasil, 2020). Por consequência, a ascensão de novas ameaças frente às instabilidades no sistema internacional instigou o país a buscar por uma defesa mais robusta por meio do planejamento estratégico de Estado, o que resultou na consolidação da Política Nacional de Defesa (PND) em 2005[7] e da Estratégia Nacional de Defesa (END) em 2008.

Esses dois documentos permitiram à Defesa Nacional do Brasil, uma orientação mais clara no que se refere à defesa do país, em que a PND busca estabilizar diretrizes gerais para a proteção da soberania e dos interesses nacionais, enquanto a END detalha estratégias

[7]Atualização da antiga Política de Defesa Nacional (PDN) criada em 1996 (Brasil, 2020).

necessárias para fortalecer a capacidade de defesa do Brasil. De maneira pioneira, esses documentos inauguram os debates acerca do desenvolvimento de estruturas de defesas cibernéticas a partir do estabelecimento, em 2008, de três novos setores estratégicos: nuclear, espacial e cibernético (Brasil, 2020). Diante da crescente importância do ciberespaço como um novo domínio de conflitos, ambos os documentos passaram a incorporar a necessidade de proteger IC e garantir a preparação contra possíveis ameaças cibernéticas.

Ainda no contexto da END, destaca-se a importância de reforçar a "Capacidade de Proteção", na qual a Estratégia volta a reafirmar a importância do desenvolvimento da defesa no campo cibernético:

> Reforçar a Capacidade de Proteção requer a adequação e estruturação dos sistemas de vigilância nas áreas de interesse e de controle sobre o território nacional, as Águas Jurisdicionais Brasileiras, o espaço aéreo sobrejacente e espaço exterior, o espaço cibernético e outras áreas de interesse. (Brasil, 2020, p.37).

Nesse sentido, a END atribui a cada uma das forças (Marinha, Exército e Força Aérea) um setor sob a sua responsabilidade, sendo o Exército responsável especificamente pelo Setor Cibernético. Assim, entende-se que o setor em questão tem uso dual, em que suas capacidades são destinadas, prioritariamente, para as tecnologias de comunicação das Forças Armadas, garantindo interoperabilidade, e também na atuação integrada, garantindo segurança entre elas (Brasil, 2020). A defesa brasileira busca, a partir dessa estratégia, a melhoria no setor de segurança da informação, garantindo a segurança das IC brasileiras, fazendo necessária a consolidação do setor cibernético, reforçado pela aprovação da Doutrina Militar de Defesa Cibernética Brasileira.

3.2 A Doutrina Militar de Defesa Cibernética Brasileira

A Doutrina Militar de Defesa Cibernética Brasileira, a qual tem por finalidade estabelecer diretrizes e procedimentos centrados no assunto da Defesa Cibernética, em especial a estabilização do Sistema Militar de Defesa Cibernética (SMDC), em tempo de sua primeira edição (2014), marcou a criação do ComDCiber[8]. Nesse mesmo ano, no que tange ao cenário externo, houve o reconhecimento do espaço cibernético como domínio operacional pela OTAN, o que possibilitou que os debates acerca da Defesa Cibernética evoluíssem cada vez mais (Brasil, 2023). Nesse sentido, a aprovação da Doutrina veio em hora para buscar um entendimento comum acerca do pensamento sobre o meio cibernético dentro do Ministério da

[8]Apenas ativado no ano de 2016 (Brasil, 2023).

Defesa, buscando a atuação conjunta das três Forças Armadas a fim de defender o Brasil no espaço cibernético.

Essa doutrina está fundamentada na necessidade de garantir a segurança de, não apenas das IC que se fazem necessárias ao país, mas também a proteção de dados sensíveis e a capacidade de resposta a ataques cibernéticos. O modelo adotado pela doutrina em questão segue uma abordagem predominantemente defensiva, reafirmando os princípios de uma nação não agressiva (Malagutti, 2021), alinhando-se à política do país, prezando por soluções diplomáticas e cooperação internacional. Por outro lado, o mesmo documento reconhece a importância de medidas proativas, reafirmando a necessidade do país em se manter em prontidão para qualquer cenário que possa ocorrer.

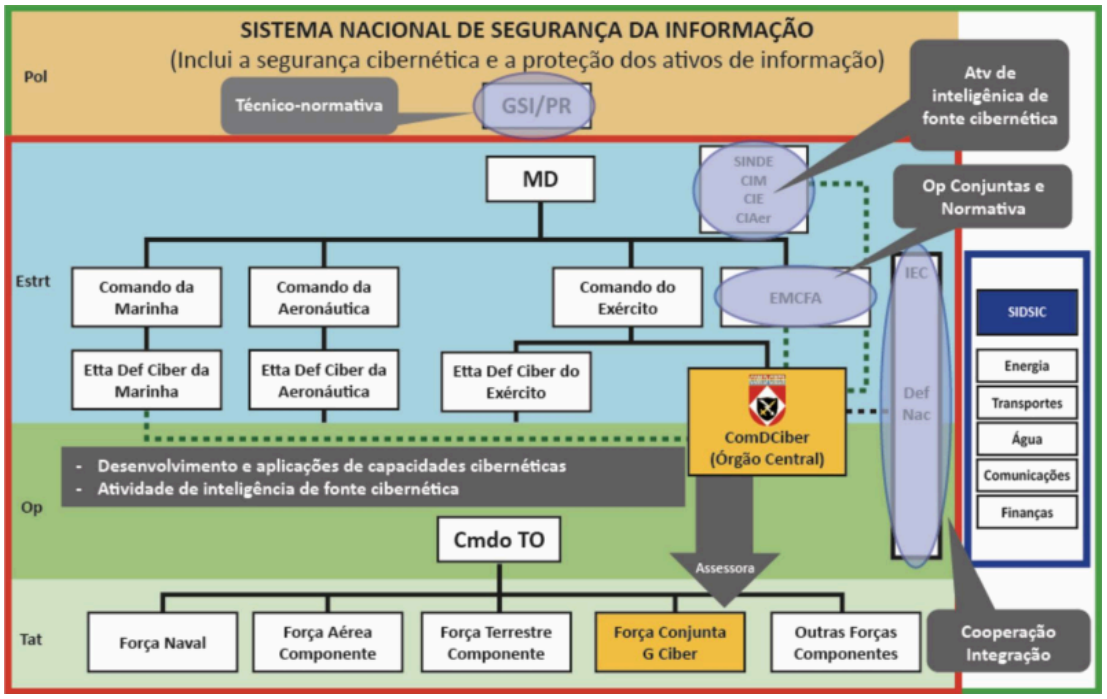
Nesse sentido, como uma das consequências da aprovação da Doutrina, houve a criação do ComDCiber, ativado em 2016, que impulsionou o Brasil buscar pela estruturação de sua atuação no campo cibernético, de modo a adotar medidas que envolvem a capacitação dos recursos humanos e desenvolvimento de tecnologias aptas à cibersegurança e a implementação de protocolos para a proteção de IC. A criação desse comando representou um avanço significativo na consolidação da defesa nacional, pois permitiu uma atuação coordenada e estratégica diante das crescentes ameaças no mundo digital. Assim, vem como um importante fator no desenvolvimento de capacidades de defesa cibernética brasileira, promovendo o intercâmbio de conhecimentos e a formulação de diretrizes mais eficazes para a segurança do espaço cibernético brasileiro, ao passo que busca atingir objetivos alinhados à própria doutrina.

Além da ativação do ComDCiber, é válido salientar a publicação de um novo decreto em 2018, (Decreto nº 9.637/2018) instituindo a Política Nacional de Segurança da Informação (PNSI), a qual abrange questões relacionadas principalmente à defesa cibernética (Brasil, 2018). Não obstante, em 2020, institui-se a Estratégia Nacional de Segurança Cibernética (E-Ciber), buscando prosperar, em termos nacionais, o Brasil no quesito digital, reforçando a defesa brasileira a possíveis ameaças cibernéticas, fortalecendo sua defesa dentro do cenário internacional, mesmo que ambos os documentos não se apliquem no quesito de operações militares.

Para além das características anteriormente citadas da doutrina, outro ponto fundamental, presente em seu terceiro capítulo, é referente ao SMDC, em que é considerado “um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais” (Brasil, 2023, p.27) responsáveis em garantir a segurança e a utilização correta do espaço cibernético. Sendo assim, para melhor entendimento acerca da presença dos

diversos setores da sociedade brasileira é importante a visualização de sua estruturação conforme imagem abaixo (Figura 1):

Figura 1 - Sistema Militar de Defesa Cibernética



Fonte: Doutrina Militar de Defesa Cibernética Brasileira, 2023.

Nesse sentido, entende-se que a defesa cibernética é um objeto complexo de ser lidado, e em razão do caráter dinâmico e evolutivo das ameaças digitais, reconhece a necessidade de uma participação ativa da sociedade de uma maneira geral, ou seja, não apenas do Estado, mas também do setor privado, a academia e a sociedade civil. Essa necessidade é abordada na própria doutrina, como se constata na citação abaixo:

> A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o MD e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a END (Brasil, 2023, p. 27).

Assim, entende-se que o órgão central para o funcionamento do SMDC é o ComDCiber, uma vez que é responsável por assessorar o Ministro de Estado da Defesa na implantação do próprio sistema, garantindo a defesa necessária para a proteção do ambiente cibernético (Brasil, 2023). No entanto, se faz relevante a opinião de outros setores da sociedade, incluindo o setor acadêmico, responsável por realizar pesquisas do meio a fim de preencher lacunas dos assuntos relacionados. Dessa forma, a colaboração entre governo,

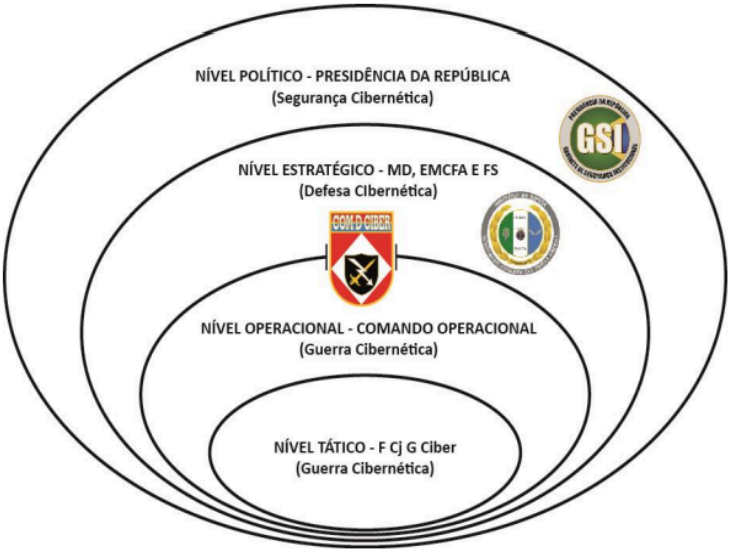
academia e setor privado – tríplice hélice – se torna essencial para fortalecer as capacidades cibernéticas do país, promovendo uma abordagem mais integrada e eficiente no enfrentamento das ameaças digitais.

3.3 O Comando de Defesa Cibernética

O desenvolvimento do setor de defesa cibernética no Brasil teve impacto significativo nos diferentes níveis de atuação, sejam eles (1) políticos tratando-se da coordenação e das normas da segurança cibernética, (2) estratégicos no que se refere à definição das políticas e diretrizes, (3) operacional sobre a implementação das anteriores, e (4) tático para a execução das ações específicas. Nesse sentido, o setor consolida sua atuação de maneira mais efetiva, organizando-se em busca de garantir um arcabouço normativo e institucional mais eficiente e capaz de responder às ameaças cada vez mais complexas. Assim, criaram-se específicas de governança, determinando as responsabilidades de cada um dos níveis de atuação (Brasil, 2023). Essa estrutura organizacional reflete a necessidade de alinhamento entre a formulação de políticas, a execução das estratégias de defesa e a aplicação de medidas operacionais, o que aumenta a proteção do país no âmbito da defesa cibernética.

Para melhor compreender a atuação do ComDCiber, é importante entender de que maneira ficaram dispostos os níveis de decisão do Setor Cibernético, a partir da sua consolidação, ainda em 2008, proveniente da END. Tem-se: 1. ao nível político a Segurança Cibernética, coordenada pelo Gabinete de Segurança Institucional da Presidência da República, a qual abrange a Administração Pública Federal e as IC; 2. ao nível estratégico a Defesa Cibernética a cargo do Ministério de Defesa (MD), do Estado-Maior Conjunto das Forças Armadas (EMCFA) e dos Comandos das Forças Armadas (FA), e a presença do ComDCiber, que também se estende a nível operacional; 3. a nível operacional e tático entende-se a presença da Guerra Cibernética, a cargo dos Comandos Operacionais ativados e das Forças Componentes. Veja esquema abaixo (Figura 2):

Figura 2 - Níveis do Setor Cibernético Brasileiro



Fonte: Doutrina Militar de Defesa Cibernética Brasileira, 2023.

A priori, no que se refere ao nível político, e à Segurança Cibernética, tem-se o GSI como principal ator que domina as atividades de proteção cibernética e se relaciona com o SMDC, externamente, de maneira colaborativa e integrativa para garantir a proteção das IC que são de interesse da Defesa Nacional (Brasil, 2023). Para mais, adentrando na Defesa Cibernética, tem-se ao nível estratégico, a cargo do MD, do EMCFA e das FA, interação com o GSI nos assuntos referentes à Defesa Nacional, esses atores passam a incluir a atuação do ComDCiber como órgão central do SMDC, e a principal diferença para o nível anterior é a exclusividade nos assuntos de defesa e não mais de segurança (Brasil, 2023).

O ComDCiber, órgão que opera tanto a nível operacional, no âmbito da guerra cibernética, como também ao nível estratégico, na defesa cibernética, é o garantidor da implantação do importante SMDC (Brasil, 2023), de maneira que permita à Defesa Nacional, uma maior capacidade de atuação no que concerne à defesa cibernética. Dessa forma, o ComDCiber é reconhecido como órgão central do SMDC, e considerado um Comando Operacional Conjunto, integrante do Exército Brasileiro e subordinado ao seu Departamento de Ciência e Tecnologia (DCT) que passa, a partir de 2016, a integrar as atividades da defesa cibernética dentro do MD ao nível estratégico (Epex, 2023).

Sob esse mesmo aspecto, é importante definir que o ComDCiber é responsável por buscar, organizar e executar atividades que estejam relacionadas ao desenvolvimento e à aplicação das capacidades cibernéticas brasileiras (Brasil, 2023). Não obstante, o Comando deve coordenar operações cibernéticas a fim de aumentar cada vez mais a proteção de

informações, não apenas do Governo (MD e FA), mas também garantindo a segurança das informações da sociedade civil como um todo. Dessa maneira, o Comando também se faz presente na elaboração dos Planos Estratégicos que busquem o fortalecimento da Defesa Brasileira no ambiente cibernético, frente às novas ameaças que surgem no cenário internacional.

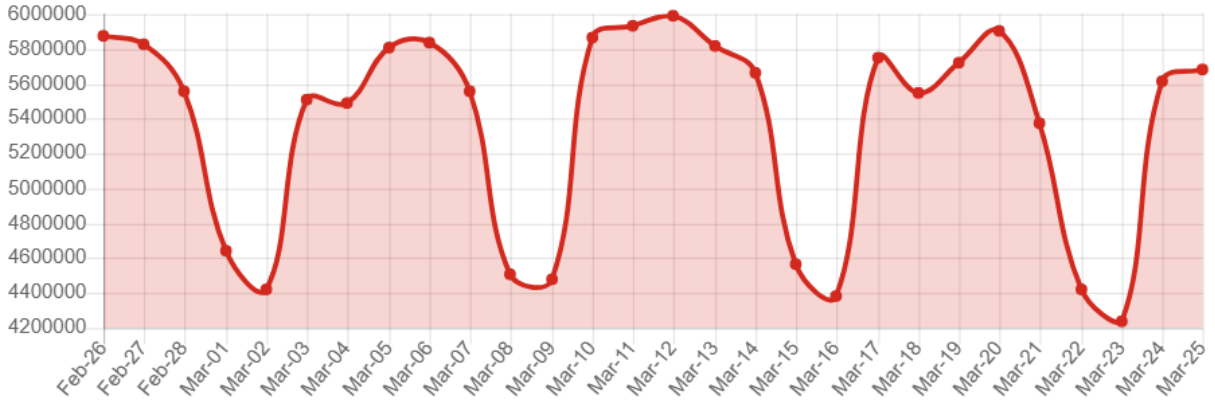
Dentro do ComDCiber há outras estruturas que convergem de maneira a garantir o melhor funcionamento do Comando. Dentre elas o Centro de Gestão Estratégica (CGE), coordenando os processos internos; o Centro de Coordenação de Operações Cibernética (CCOC) que busca aplicar as capacidades cibernéticas; o Centro de Ações Cibernética (CAC), o qual executa as operações de Defesa, voltadas para o sentido tático; e o Centro de Defesa Cibernética (CDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber). Dessa forma, o ComDCiber se torna apto para o cumprimento de suas atividades, seja a nível operacional, ou de gestão estratégica (Brasil, 2023).

Nos últimos tempos, diversas nações, incluindo o Brasil, enfrentam um aumento significativo nas ameaças cibernéticas que colocam em risco as infraestruturas críticas do país. Esses ataques têm se tornado cada vez mais sofisticados, exigindo uma resposta eficaz e bem estruturada para proteger os interesses nacionais e garantir a segurança dos cidadãos. Diante desse cenário, é necessário entender que o Brasil está incorporando cada vez mais a dimensão cibernética em suas estratégias de defesa, visando fortalecer a atuação defensiva no ciberespaço. A proteção do ciberespaço passa então a ser percebida como uma prioridade, uma vez que essas infraestruturas dependem de uma defesa robusta contra possíveis invasores cibernéticos.

Uma clara visualização acerca do impacto sofrido pelo Brasil dos ataques cibernéticos pode ser identificada no gráfico abaixo (Gráfico 1), em que mede o "fluxo de detecção de *malwares*[9] quando os objetos são acessados ao abrir, copiar, executar ou salvar operações" (Kapersky, 2025) no país:

[9]Termo utilizado para definir qualquer *software* malicioso, com a finalidade de prejudicar os dispositivos em que são ativados.

Gráfico 1 - Identificação de *malwares* no período de um mês no Brasil



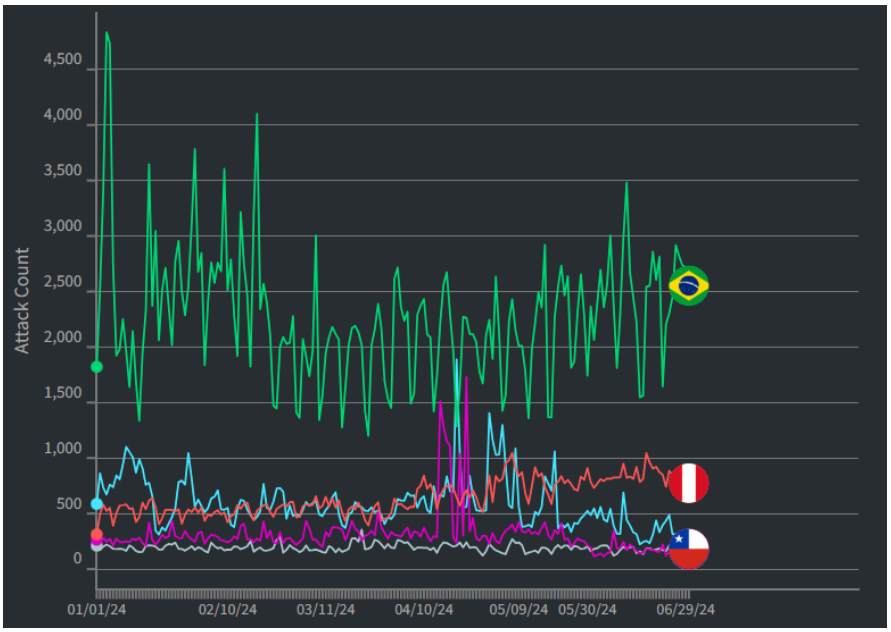
Fonte: Kaspersky, 2025.

Para além dos projetos já previstos nas estratégias de Defesa, o Brasil, um país de dimensão continental com importante relevância no contexto internacional, motivado pelo aumento das ameaças cibernéticas globais (Aurélio *et al.*, 2017) e a necessidade de fortalecer os setores estratégicos de defesa, buscou desenvolver o exercício do EGC. A realização de grandes eventos internacionais, como a Copa do Mundo em 2014 e as Olimpíadas em 2016, evidenciou as vulnerabilidades do país a possíveis ataques digitais. Diante desse cenário, o Brasil investiu no fortalecimento de suas capacidades de defesa cibernética, de maneira a consolidar o ComDCiber como um órgão central na proteção do ciberespaço nacional e promovendo exercícios, tal como o Guardião, para aprimorar a cooperação entre as Forças Armadas, órgãos governamentais, setor privado e a academia no enfrentamento a ameaças digitais (Brasil, 2024).

4. O GUARDIÃO CIBERNÉTICO: UMA ANÁLISE

O aumento das ameaças cibernéticas globais e a crescente dependência de IC conectadas à internet levaram o Brasil a reforçar suas capacidades de defesa digital. Nos últimos anos, ataques cibernéticos sofisticados contra setores estratégicos em diversos países evidenciaram a vulnerabilidade de sistemas essenciais, como energia, telecomunicações, transporte e financeiro. Em 2024, a NETSCOUT, uma empresa norte-americana responsável por ferramentas de monitoramento a ameaças cibernéticas, disponibilizou seu relatório com relação a ataques de tipo *Distributed Denial of Service*[10] (DDoS), o qual determinou que o Brasil tem uma frequência de 372.835 ataques DDoS por hora, tornando-o o maior alvo na América Latina (Netscout, 2024). Diante desse cenário, o Brasil reconheceu a necessidade de aprimorar a resiliência cibernética nacional, especialmente para proteger redes e sistemas críticos de possíveis ataques que poderiam comprometer a segurança e a estabilidade do país (TI Inside, 2024).

Figura 3 - Os 3 países latino-americanos mais atacados por DDoS por hora



Fonte: NETSCOUT; Atlas, 2024.

Para além desses dados, e como já citado anteriormente neste trabalho, o Brasil é um país que sedia regularmente eventos internacionais que atrai pessoas do mundo inteiro, em

[10]Ataques de Negação de Serviço: esse tipo de ataque se refere aos dispositivos comprometidos que são responsáveis por sobrecarregar os recursos do sistema-alvo, de maneira a inutilizá-lo para os usuários legítimos, causando interrupções em serviços críticos (Mello; Junior; Rocha, 2010).

destaque para a Copa do Mundo em 2014 e as Olimpíadas de 2016, que demandaram certo esforço com relação às estratégias de defesa cibernética por conta da magnitude desses eventos, e a necessidade de garantir que não houvesse ataques que impedissem a continuidade dos eventos (NEC, 2016). Além disso, no Brasil, o setor bancário tem importância significativa em razão do seu tamanho, de modo que se torna um alvo muito atrativo para o ataque de hackers, que cresceu 70% em um ano (Monitor Mercantil, 2024), entretanto, é um setor relativamente preparado, tendo em vista ser considerado o que mais investe em segurança cibernética, cerca de 10% do seu orçamento de tecnologia (Febraban, 2024). Nesse contexto, entende-se a necessidade de iniciativas que visem reforçar a defesa cibernética brasileira, assim, justificando a criação do EGC, por exemplo.

A partir da criação do EGC, em 2018 pelo ComDCiber, objetivando a promoção de simulações realistas de ataques cibernéticos e a avaliação das capacidades de resposta das organizações participantes, o exercício reúne representantes das Forças Armadas, órgãos governamentais, empresas privadas e instituições acadêmicas (Brasil, 2024). De uma maneira geral, seus objetivos partem do princípio da elaboração de estratégias que possam contribuir para a resiliência cibernética do país (ComDCiber, 2021), tendo por finalidade a identificação e a difusão das práticas mais bem sucedidas para o impedimento de ataques cibernéticos e a mitigação desses caso ocorram, reiterando o argumento proposto pelos autores Clarke e Knake em "*The Next Threat to National Security and What To Do About It*", e por Libicki em "*Cyberdeterrence and cyberwar*", nas quais, ambas as obras identificam as ações de defesa, independente de quais sejam, como responsáveis de desenvolver as capacidades de defesa, garantindo ao país segurança contra ataques iminentes, os bloqueando ou minimizando os impactos causados por estes.

4.1 Exercícios de Simulação

A realização de exercícios voltados ao desenvolvimento de meios de defesa cibernética são iniciativas extremamente importantes. É idealizado, no caso do EGC no Brasil, pelo governo nacional para avaliar a postura da defesa com relação às ameaças cibernéticas (FGV; EB, 2024). Exercícios de simulação podem ser realizados em âmbito nacional, setorial ou dentro de organizações, visando o aprimoramento e a capacidade de prontidão desses serviços. Para o Brasil, o EGC atua na simulação de ataques cibernéticos, possíveis incidentes dentro do ciberespaço sob diversos cenários como maneira de identificar

os problemas e na promoção de dinâmicas com os especialistas de cada área em questão (Brasil, 2024).

Além disso, outro aspecto a se destacar com relação aos exercícios de simulação é o fato de auxiliarem no desenvolvimento de certas habilidades ao longo de sua execução, que garantem o melhor preparamento dos governos com relação à defesa de IC: “prevenção; detecção/reação; análise forense; e ataque” (Chodhury; Gkioulos, 2021). Nesse sentido, a utilização de exercícios de uma maneira geral pode ser vista como uma maneira de auxiliar tanto os tomadores de decisão, na esfera política, como também o grupo responsável pelo ambiente operacional, pois aprimora as capacidades desses em se defenderem de um específico ataque cibernético que pode ter sido simulado previamente nesses eventos (Chodhury; Gkioulos, 2021).

Exercícios desse gênero devem acontecer para investigar o quão preparados os atores envolvidos estão em suas capacidades de resposta (FGV; EB, 2024), e podem funcionar de duas formas diferentes, definindo o tipo de abordagem que será utilizada e a finalidade deles, são elas: simulação virtual e simulação construtiva. A Fundação Getúlio Vargas, com apoio do Exército Brasileiro, desenvolveu um manual de orientação de exercícios que explicam ambos os tipos: a primeira consta com participantes majoritariamente da área da Tecnologia da Informação (TI), com o objetivo de garantir uma experiência empírica, com teste de habilidades e ferramentas técnicas para responder a ameaças cibernéticas, é desenvolvido em um ambiente virtual de treinamento, e busca garantir um aprendizado coletivo por meio de exercícios em equipe.

Por outro lado, a segunda atividade, de simulação construtiva, é realizada por meio de exercícios de discussão, com a presença de mediadores em um ambiente de incidentes cibernéticos hipotéticos. Esse tipo de exercício envolve diversas áreas do conhecimento, e é importante para o aprimoramento da comunicação entre diversos setores, buscando a cooperação entre eles a fim de bloquear e/ou mitigar qualquer ameaça cibernética. Ademais, tem por objetivo avaliar o estado de prontidão e a capacidade de resposta, identificando possíveis vulnerabilidades e onde pode haver aprimoramentos (FGV; EB, 2024).

4.2 Estruturação do Exercício Guardião Cibernético

É importante ressaltar que a aplicação do EGC está diretamente alinhada com os objetivos das políticas e diretrizes voltadas para a defesa cibernética, anteriormente apresentadas no presente trabalho. Além disso, especialmente ao que se refere no Plano

Nacional de Segurança de IC, indica-se, a partir de um de seus objetivos estratégicos, a designação das seguintes ações estratégicas: “2.2.4. Realizar exercício ou simulação conjunta de incidentes que envolva diferentes setores de Infraestruturas Críticas” e “2.2.5. Envolver, nos exercícios de Guardião Cibernético, setores abordados em Segurança de Infraestruturas Crítica” (Brasil, 2022), e estão, respectivamente, designadas ao GSI/PR e ao MD. Assim, reconhecendo a importância da realização de exercícios simulados, como o EGC, e a necessidade de incluir importantes setores de IC nas edições.

O EGC é considerado o maior exercício simulado de defesa cibernética do hemisfério sul (Brasil, 2024) e é realizado com frequência anual desde 2018, ano de sua primeira edição, sob o comando do ComDCiber. O evento reúne diversas organizações, estatais e privadas, participação de aliados internacionais e acadêmicos de diversas áreas, objetivando a cooperação interagência e internacional, fortalecendo cada vez mais a capacidade operacional das Forças Armadas. Posto isto, é identificável a característica de presença multissetorial no exercício, o que o caracteriza como uma simulação construtiva.

O EGC busca então organizar um ambiente simulado, dentro de uma plataforma virtual, que projeta, da maneira mais fiel possível, os elementos realistas do Estado Brasileiro (Brasil, 2022). Assim, os participantes irão simular como reagiriam aos incidentes hipotéticos propostos no exercício, praticando os processos previstos para interromper o ataque, buscando identificar, classificar e conter os danos (FGV; EB, 2024). Não obstante, são simuladas também situações de desastres completos, considerados níveis graves, em que devem trabalhar no quesito de recuperação, sendo avaliado então o tempo necessário para recuperar-se do ataque. Outros fatores que o EGC pode explorar estão voltados para avaliações de políticas já existentes no país, e também a atuação de seus atores em casos de vazamento de informações, por exemplo.

Entende-se, portanto, que as edições do EGC, de uma maneira geral, são organizadas em quatro diferentes linhas, envolvendo tanto simulações virtuais e construtivas, como previamente explicadas, mas também palestras de conscientização e grupos de estudos (Brasil, 2022). Dentro do EGC, os grupos de estudos acontecem para que ocorram discussões a fim de desenvolver estratégias que garantam a resistência a ataques cibernéticos por parte do país, enquanto as palestras estão mais voltadas para que civis e militares estejam mais conscientes quanto ao uso com maiores precauções do ambiente digital (higiene cibernética[11]). Já a simulação virtual e construtiva, respectivamente, utilizam de um Simulador de Operações

[11]“Conjunto de práticas essenciais que garantem a segurança e a proteção da rede e dos dados de uma organização”, maneiras de evitar e mitigar os riscos no ambiente cibernético (Brasil, 2023).

Cibernéticas (SIMOC) e operam sob diferentes áreas do conhecimento, soluções para os problemas hipotéticos criados.

4.3 Análise das edições do EGC (2018-2024)

A seguir, foi realizada uma análise anual de cada uma das edições do EGC já encerradas, abrangendo o período de 2018 a 2024, assim, identificando as informações-chave de cada uma de suas edições, destacando seus principais avanços, desafios enfrentados e inovações implementadas ao longo dos anos. Dessa forma, será possível uma melhor visualização da evolução do exercício em termos de estrutura, participantes e cenários simulados, refletindo o amadurecimento das estratégias de defesa cibernética no Brasil.

Além disso, essa análise permitirá observar as mudanças adotadas em resposta às novas ameaças emergentes no cenário digital, bem como os marcos alcançados ao longo das edições. Ao comparar os exercícios realizados anualmente, é possível identificar as tendências que se mantêm ao longo dos anos, os aperfeiçoamentos metodológicos e lições aprendidas, evidenciando o importante papel que o EGC tem no desenvolvimento e fortalecimento dos setores cibernéticos brasileiros (Brasil, 2018). Assim, a contínua aplicação dessas simulações reforça a importância do aprimoramento das capacidades de resposta a incidentes e da cooperação entre diferentes setores, consolidando o Brasil como um país que está em prontidão contra qualquer desafio que possa surgir.

O ano de 2018 marca o início das edições do EGC, ocorrido no mês de julho durante três dias em Brasília. O treinamento contou com a participação de mais de 150 representantes dentre 23 organizações. Além do setor de defesa do Brasil, dois outros setores importantes detentores de IC se fizeram presentes: Nuclear e Financeiro. De uma maneira geral, as organizações participantes se concentraram em: Ministérios da Defesa, Justiça e das Relações Exteriores; Gabinete de Segurança Institucional da Presidência da República; Forças Armadas; bancos públicos e privados; Banco Central; empresas dentro do setor nuclear; a academia e outros atores envolvidos no setor cibernético.

O cenário elaborado para servir de contextualização para o 1º EGC objetivava a integração do setor de defesa com outras instâncias do governo federal, entidades do setor privado e a academia na tentativa de desenvolver novas estratégias para a defesa nacional contra ameaças do meio cibernético. Além disso, foi possível identificar, por cada um dos setores, individualmente, os pontos a serem melhorados para suas próprias estruturas responsáveis pela defesa cibernética. Em paralelo às simulações, o Grupo de Estudos estava

responsável por se reunirem e debaterem aspectos diversos, principalmente na área de pesquisa, o que resultou no levantamento de questões relacionadas à criação de um Plano Nacional de Tratamento e Resposta a Eventos de Segurança Cibernética, o que mais tarde serviu de base para a aprovação da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), ainda em 2018, que previa, dentre muitas outras instâncias: "II - a integração entre as diferentes esferas do Poder Público, o setor empresarial e os demais segmentos da sociedade;" (Brasil, 2018, art. 2º), além de outras diretrizes voltadas para a segurança das IC do país.

No ano seguinte, em 2019, em razão do sucesso obtido com a realização da primeira edição, o treinamento voltou a acontecer, com o incremento de novos setores, sendo eles o Elétrico e de Telecomunicações (Defesanet, 2019), sem a exclusão dos setores que participaram no anterior[12]. Nesta edição, o gabinete de crise foi alinhado às áreas de tecnologia da informação, comunicação social, jurídica e administração. Contou com a participação dos mesmos setores do ano anterior e algumas adições, resultando em aproximadamente 200 integrantes de 40 diferentes organizações (Brasil, 2019).

De um modo geral, a edição 2.0 seguiu o mesmo esquema da primeira, três grupos distintos (gabinete de crise; grupo de estudos; equipe de simulação), em que simultaneamente buscavam atingir seus objetivos para desenvolver melhores capacidades de defesa cibernética. No entanto, diferente da 1.0 em que atingia uma abordagem mais voltada para a criação e o fortalecimento de uma rede de conexões entre os participantes, o II teve uma estrutura de Fórum, e contou com a participação de delegações estrangeiras. Ademais, dentro do SIMOC, as simulações de ataque se concentraram no meio elétrico, de telecomunicações, financeiro e nuclear[13], acontecendo de maneira intra e intersetorial.

Em consonância à sua antecessora, o EGC 2.0 também contribuiu para "a validação do Plano Nacional de Tratamento de Incidentes de Redes" (Brasil, 2019), consolidando diretrizes e aprimorados os meios para garantir maior êxito na gestão de incidentes cibernético em âmbito nacional. Além disso, os debates realizados durante o exercício seguem fornecendo subsídios estratégicos para o fortalecimento do SMDC, impulsionando o desenvolvimento de novas abordagens tecnológicas e a implementação de inovações que ampliam a resiliência das IC do país.

---

[12]A ideia inicial era de que a cada nova edição, os setores participantes deveriam ser substituídos e não acumulados, mas o sucesso fez com que os veteranos desejassem a sua inclusão novamente no evento.

[13]A adição do setor nuclear no Exercício do Guardião cibernético permitiu o debate por parte do Grupo de Estudos na pesquisa pela implantação do marco regulatório dentro desse setor, no que tange à defesa cibernética (Ministério da Defesa, 2019).

O EGC 3.0 foi discutido e idealizado para ocorrer no ano seguinte ao 2.0, mas, em razão da pandemia da COVID-19, sua realização foi apenas possível em 2021. Nesta edição, o exercício ocorreu em duas sedes diferentes, Brasília e São Paulo, e contou com a participação dos setores estratégicos de Água, Energia, Financeiro, Nuclear, Transporte e Telecomunicações (GSI, 2019), o que reuniu cerca de 350 participantes. Os envolvidos foram separados em duas equipes para simulações de ataques e defesas às IC, e tinha por objetivo gerar um Protocolo de Segurança Cibernética para o País.

O cenário hipotético do evento consistia em um grupo hacker simulando diversos ataques contra as IC, o grupo responsável pela defesa deveria tomar decisões em tempo real, divididos em seus comitês de crise de cada setor, a fim de estabelecer e defender os sistemas atacados. Ademais, passaram a ser discutidas questões relacionados aos desafios da próxima década, que envolvem desde inteligência artificial, rede móvel 5G até a computação quântica (Defesanet, 2021). Nesse mesmo ano incorporou-se a ideia de participação integrada e cooperativa, o que corresponde à participação dos seguintes times: o *blue team*, que se tornaram os responsáveis pela defesa computacional dentro do simulador, enquanto o *red team* era responsável pelo ataque, o *white team* pela arbitragem e o *green team* pelo suporte.

Em 2022 ocorreu a 4ª edição do EGC, também sediado em dois lugares simultâneos, similar ao seu antecessor, 3.0, contou com a participação dos setores de energia, financeiro, nuclear, transporte, água e comunicações, além da colaboração das Forças Armadas, do Governo e Órgãos Parceiros (Brasil, 2022). Ao todo, cerca de 450 participantes se reuniram em agosto do mesmo ano para a realização do evento, este que contou com a incorporação dos Correios no que tange ao setor de comunicações. Os problemas hipotéticos foram expandidos para além dos setores das IC, envolvendo também Governo e órgãos parceiros.

Seguindo a mesma lógica das edições anteriores, buscou cumprir o seu objetivo de aprimoramento das capacidades de resposta nacional contra incidentes cibernéticos, simulando ataques complexos contra as IC do país, inspirados nos ciberataques recentes que ocorreram ao redor do mundo, tais como o de tipo *ransomware*[14] (ComDCiber, 2022). O EGC 4.0 pode reforçar a cooperação internacional, de modo a conectar os grupos observadores externos com representantes de organizações internacionais de nações parceiras, possibilitando a troca de experiência e práticas em segurança cibernética.

A 5ª edição do EGC ocorreu em 2023, sediada pela Escola Superior de Defesa (ESD) em Brasília, contando com a participação de mais de 500 integrantes e 111 organizações.

[14]Ataques que criptografam arquivos do disco rígido para que o sistema de arquivos se torne ilegível e o Sistema Operacional não consiga iniciar (ComDCiber, 2022).

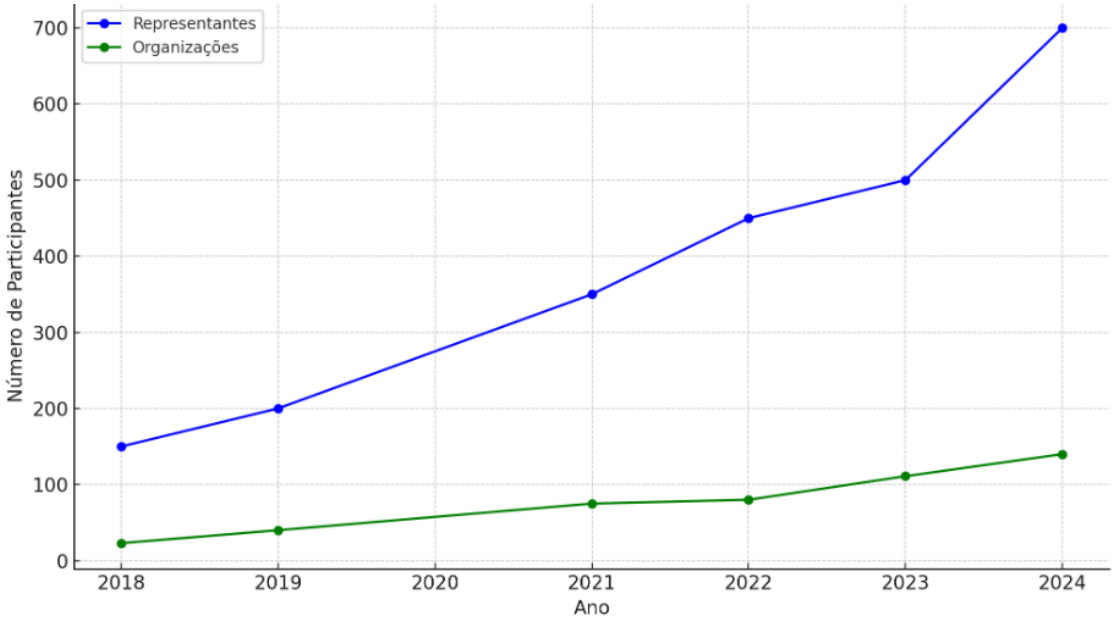
Ocorreu também, similar as duas edições anteriores, simultaneamente em Brasília e em São Paulo, buscando aprimorar as ações preventivas e protetivas contra ataques cibernéticos (ESD, 2023). Seguiu-se os padrões de suas antecessoras, com atividades voltadas para a simulação construtiva, virtual e os grupos de estudos. Somando-se à participação dos setores já conhecidos, como de água, energia, transporte, comunicações, finanças, nuclear e de defesa, foram incorporados os setores de Biossegurança e Bioproteção e Governo Digital.

A edição também foi contemplada com a presença de integrantes do Fórum Ibero-Americano de Defesa Cibernética, este que reúne 13 países, o que permitiu aos países participantes conhecer de perto o funcionamento do exercício e sua importância para o território brasileiro. É importante perceber, portanto, que a construção das capacidades de defesa cibernética do país depende da participação multissetorial, além do compartilhamento de informações dentro da cooperação interagência, o EGC 5.0, como os anteriores, buscou atingir os objetivos de prevenção e solução de incidentes que envolvem questões como segurança da informação, e ataques cibernéticos contra IC brasileiras (Defesa Aérea & Naval, 2023).

A 6ª edição do EGC e última, até o momento, ocorreu em 2024 simultaneamente em São Paulo e em Brasília, reunindo mais de 700 participantes e cerca de 140 organizações e representantes de mais de 30 países (Brasil, 2024). Contou com a presença dos mesmos setores presentes nas edições anteriores: Defesa, Águas, Energia, Transporte, Comunicações, Finanças, Biossegurança/Bioproteção e Nuclear. Foi também o segundo ano em que o GSI/PR participou do exercício como coordenador de uma das simulações de Gabinete de Crises, buscando subsidiar as tomadas de decisão no que tange às preocupações dentro do ambiente cibernético.

No mais, as características da simulação se mantiveram bem similares às anteriores, mas sempre reiterando de maneira mais afirmativa o objetivo do exercício em promover a resiliência cibernética do país dentro dos setores estratégicos responsáveis pela IC do país, reforçando as diretrizes previstas pelo PNSIC, de modo a ampliar as capacidades operacionais dos órgãos responsáveis pela defesa brasileira. A evolução do número de participantes demonstra a confiança adquirida, com o passar dos anos, pelos setores e organizações mais variados do país, como representado pelas linhas crescentes no gráfico abaixo (Gráfico 1):

Gráfico 2 - Número de Participantes nas edições do EGC



Fonte: elaboração própria, 2025.

Além disso, outro ponto a se destacar é a incrementação de novos setores ao longo das edições, característica que era prevista, inicialmente, como um fator de substituição e não adição (Campos, 2020), o que resultou na cooperação interagências, aumentando a troca de informações, garantindo um melhor fortalecimento das capacidades de defesa cibernética brasileira, resultado esse que pode ser apoiado no argumento dado pela Elinor Sloan (2016), a qual definia a defesa como uma "força-tarefa conjunta" em prol dos objetivos da nação. Soma-se também as diferentes resoluções e diretrizes que foram aprovadas ao longo dos anos de aplicação das simulações, que em partes foram subsidiadas por discussões realizadas dentro do EGC, principalmente pelos Grupos de Estudos, como o próprio PNSIC, o Plano Nacional de Tratamento de Incidentes de Redes, o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (Brasil, 2020) e o Plano de Gestão de Incidentes Cibernéticos (Brasil, 2022), por exemplo.

Não obstante, é possível identificar que, para além das regulamentações anteriormente citadas, houve marcos no desenvolvimento do SMDC, propriamente dito, com a consolidação do E-Ciber no ano de 2020, o qual "é a orientação manifesta do Governo Federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área de segurança cibernética" (Brasil, 2020, p.3). Outrossim, o Decreto nº 11.856, de 26 de Dezembro de 2023 que instituiu a Política Nacional de Cibersegurança e o Comitê

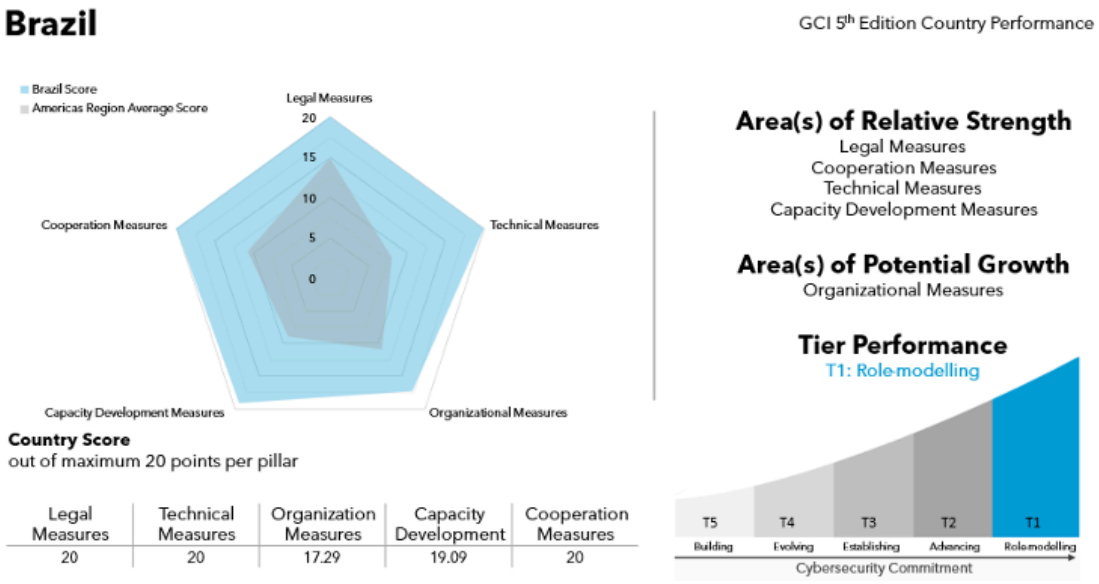
Nacional de Cibersegurança, o qual também tem por finalidade orientar a atividade de segurança cibernética do país (Brasil, 2023).

Outra questão importante, trata-se da *International Telecommunication Union* (ITU) – União Internacional de Telecomunicação – que é uma agência especializada no âmbito tecnológico para a Organização das Nações Unidas (ONU), inserida nesta agência, encontra-se o *Global Cybersecurity Index* (GCI) – Índice Global de Segurança Cibernética – , o qual mede o comprometimento dos países no que tange a segurança cibernética em âmbito global. Por meio deste, é possível realizar uma comparação entre os relatórios publicados nos anos de 2018 e 2024, identificando as diferenças entre o período que marcou o início das simulações do EGC até o momento mais recente, demonstrando a correlação entre eles.

Ambos os relatórios dividem por regiões do mundo para melhor identificar e analisar as questões relacionadas aos esforços dedicados à segurança cibernética de cada país. Ao analisar a seção das Américas no relatório de 2018, é possível perceber que o Brasil é colocado como um país com nível de comprometimento mediano em uma escala de três níveis (GCI, 2018). Além disso, ocupa a 70ª posição global e a 6ª posição regional, com seu índice de 0.577, atrás de países como Paraguai, México, Uruguai, Canadá e os Estados Unidos. No mais, o relatório não busca se aprofundar muito nas questões brasileiras, uma vez que não tem tamanha relevância em comparação aos demais países explorados.

No entanto, quando analisado o último relatório publicado em 2024, o cenário se torna muito diferente. No que concerne à atuação global, o Brasil é colocado no nível 1 dos países com papéis principais no tema, estes que possuem pontuação entre 95-100, e compartilha o nível com nações como Austrália, Dinamarca, Egito, Estados Unidos, Reino Unido e Japão, por exemplo. Ademais, no quesito regional é o único país, além dos EUA, a estar nesse primeiro nível, tornando-se o 2º das Américas.

Figura 4 - Análise do Brasil pelo GCI

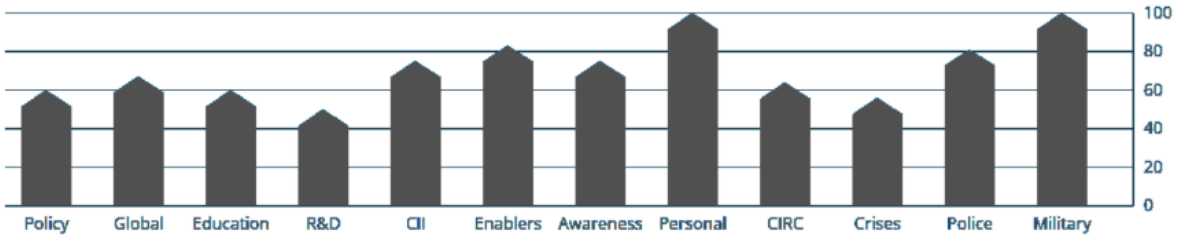


Fonte: GCI, 2024.

Conforme apresentado pela figura acima (Figura 4), o relatório de 2024 identifica que o Brasil, dentro de uma escala 0-20, possui em cada uma das 5 categorias pontuações muito altas, para melhor descrição, a pontuação máxima foi estabelecida em: 1. Medidas Legais; 2. Medidas Técnicas; e 3. Medidas de Cooperação. Para as outras duas categorias de Medidas de Organização e Capacidade de Desenvolvimento, apesar de não serem maximizadas, ficaram bem próximas, com 17,29 e 19,09 respectivamente, de modo que o GCI identifica como área de potencial crescimento a primeira. Assim, todo esse conjunto de características com essas pontuações coloca o Brasil na posição T1, a mais alta do índice.

Outro índice relevante a ser percebido é o *National Cyber Security Index* (NCSI) – Índice de Segurança Cibernética Nacional – , em que mede também a preparação dos países em prevenir as ameaças cibernéticas e lidar com os incidentes que ocorreram. Muito similar ao GCI, o NSCI identifica e mensura as capacidades de cada nação em lidar com a insegurança do meio cibernético. É possível identificar que, em seu dado mais antigo de 2019, o Brasil ocupava a 82ª colocação do ranking de segurança, mas que com o passar dos anos, e com a continuação da aplicação do EGC, chegou a atingir a 24ª colocação, em dados de 2025. No mais, o índice também divide em 12 categorias de segurança cibernética e aponta a porcentagem atingida por cada um dos países, conforme gráfico abaixo (Gráfico 3):

Gráfico 3 - Porcentagem do nível de cumprimento das categorias do NCSI



Fonte: NCSI, 2025.

Os principais pontos a serem identificados no gráfico acima é que o Brasil cumpre 100% no quesito da defesa militar e na proteção pessoal de dados cibernéticos, no entanto, tem apenas 50% no que concerne à pesquisa e desenvolvimento (R&D) na área de segurança cibernética. Portanto, conforme apresentado por Libicki (2009) em "*Cyberdeterrence and cyberwar*", ações partindo da estratégia da defesa cibernética de um país devem estar correlacionada a quaisquer capacidades de defesa que aumentem as chances de falhas dos atacantes e a mitigação dos danos caso ocorram, sendo importante, não apenas a defesa militar, mas também capacidades que partem de outras fontes, como a academia, ponto que o Brasil pode aprimorar, conforme apresentado no gráfico acima.

De um modo geral, o índice também caracteriza que o Brasil tem um nível muito alto de liderança em segurança cibernética, além de alto nível de desenvolvimento de políticas na área, que pode ser percebido de maneira prática pela consolidação das regulamentações anteriormente citadas nesse trabalho. Ademais, no que tange aos indicadores de prevenção e de resposta, o país atinge altas pontuações, demonstrando que as capacidades de defesa cibernética estão cada vez mais aprimoradas, ações estas que são subsidiadas pela execução contínua e aprimoramento do EGC. Logo, conforme apresentado por Clarke & Knake (2010), ao passo que o Brasil desenvolve cada vez mais suas capacidades, identifica-se que a defesa cibernética é fundamental para garantir que haja um bloqueio contra qualquer ameaça, e a mitigação de seus danos.

Assim, entende-se que, apesar do Brasil estar, atualmente, em posições relevantes no que diz respeito às preparações da defesa cibernética contra possíveis ameaças, ainda existem aspectos a serem melhorados, melhorias estas que também fazem parte do objetivo do próprio EGC. Como indicado pelo NCSI, o país sofre com a baixa atenção dada para a academia, setor importante para a discussão e a pesquisa de políticas que visam a melhoria do setor de defesa. Outro ponto importante a ser destacado é que o EGC, por focar estritamente em questões relacionadas aos setores das IC, acaba deixando de lado outras áreas também

importantes para o funcionamento de um país, como questões relacionadas à saúde e educação.

Ao simular cenários de ataques cibernéticos em larga escala, o EGC proporciona uma plataforma prática para testar e aprimorar as estratégias e procedimentos estabelecidos pela doutrina cibernética. Ademais, o exercício envolve a coordenação entre diferentes órgãos do governo e da iniciativa privada, fortalecendo a capacidade de resposta a incidentes e a resiliência das IC do país. No mais, o EGC também contribui para o alinhamento contínuo das políticas de segurança cibernética com a realidade do ciberespaço, de modo a garantir a melhor aplicação das estratégias de defesa cibernética na mitigação de riscos e vulnerabilidades, conforme previsto pela Política Nacional de Cibersegurança (Brasil, 2023).

5. CONSIDERAÇÕES FINAIS

Nos últimos tempos, diversas nações, incluindo o Brasil, enfrentam um aumento significativo nas ameaças cibernéticas que colocam em risco as IC de diversos países. Esses ataques têm se tornado cada vez mais sofisticados, exigindo uma resposta eficaz e bem estruturada para proteger os interesses nacionais e garantir a segurança dos cidadãos. Diante desse cenário, é necessário entender como o Brasil está incorporando a dimensão cibernética em suas estratégias de defesa, visando fortalecer a atuação defensiva no ciberespaço. A proteção do ciberespaço se tornou uma prioridade em razão da defesa robusta que as IC necessitam contra possíveis invasores cibernéticos.

Entende-se, portanto, que o crescimento dos incidentes no ambiente cibernético, terreno este propenso a vulnerabilidades e ameaças constantes em razão da sua natureza dinâmica, interconectada e rodeada de anonimidade, fez com que os países buscassem aumentar suas capacidades de defesa cibernética. Além da velocidade com que as tecnologias se desenvolvem, a intensa digitalização dos serviços essenciais tornam as IC do país bastante vulneráveis a riscos de ataques cibernéticos, espionagem, desinformação e sabotagem. Não obstante, a dificuldade em identificar os atacantes torna o ciberespaço um campo de batalha desafiador.

Além disso, diferentemente dos conflitos tradicionais, travados em campos de batalhas físicos com uso de armas tradicionais, as ações no ambiente cibernético podem ser realizadas por qualquer pessoa, de qualquer lugar, e de inúmeras maneiras ao mesmo tempo, gerando uma sensação de insegurança para todos que utilizam dos meios digitais. Essa sensação exige uma adaptação constante das estratégias de defesa da nação, como o desenvolvimento de novas políticas, melhor utilização das tecnologias e treinamentos especializados para mitigar os riscos e lidar com os possíveis incidentes que ocorrerem.

Assim, é importante entender como os países, atualmente, estão lidando com essas problemáticas. No caso do presente trabalho, buscamos explorar como o Brasil, desde 2018, procura desenvolver suas capacidades de defesa, analisando especificamente a contribuição das aplicações das diferentes edições do EGC. O estudo sobre o exercício e sua contribuição para o fortalecimento da defesa brasileira revela a crescente importância de se investir em estratégias eficientes para proteger as ICs do país.

A pesquisa realizada demonstrou que o EGC, ao simular cenários de ameaças cibernéticas em contextos hipotéticos, mas fielmente dispostos à realidade, promoveu a cooperação entre diversos setores, incluindo órgãos públicos e privados, se mostrando

essencial para o aprimoramento das capacidades de resposta a ataques cibernéticos. Ademais, a constante evolução das ameaças no ciberespaço exige que o Brasil, assim como outros países, esteja cada vez mais preparado para lidar com os desafios impostos por essa nova forma de guerra, cujas consequências podem ser tão devastadoras quanto as de um conflito convencional.

Não obstante, a análise histórica, contextual e anual das edições do EGC, como objetivo definido no escopo do trabalho, evidenciou o compromisso do Brasil em fortalecer sua defesa cibernética, buscando melhorar a interoperabilidade entre as Forças Armadas e demais agências governamentais, além de incentivar que empresas do setor privado também busquem meios para fortalecer sua segurança cibernética. No entanto, mesmo que o exercício demonstre avanços significativos, perceptíveis pelo crescimento em número de participantes e organizações envolvidas, é necessário continuar investindo em inovações e meios de garantir maior segurança no meio cibernético, defesas capazes de lidar com as ameaças emergentes.

Por meio dos índices GCI e NCSI, é possível visualizar que a contínua execução do exercício, aliada às adaptações e evoluções deste, permite ao Brasil perceber uma melhoria significativa das suas posições em índices relevantes relacionados à defesa e a segurança cibernética brasileira. Os saltos em ranking que o Brasil faz com relação ao cumprimento de normas relacionadas à garantia de segurança, além do forte desempenho em quesitos de desenvolvimento de novas políticas como o PNSIC, o E-Ciber demonstra a vontade que o país tem de crescimento nesse âmbito. A defesa do ambiente cibernético não é apenas uma questão militar, principal setor responsável dentro do território brasileiro, mas é um desafio que envolve a sociedade como todo, por isso a importância da participação de diversos setores relacionados às principais IC do país, além da incisiva participação da academia dentro dos Grupos de Estudos organizados dentro do EGC.

Em suma, a realização do EGC, ao simular esses diferentes cenários por meio do SIMOC, é uma ferramenta vital para o Brasil aprimorar suas estratégias de defesa, testar sua resiliência e prontidão caso seja necessário. O objetivo do presente trabalho era responder a seguinte pergunta: qual o papel do exercício “Guardião Cibernético” no desenvolvimento de uma defesa cibernética do Brasil? A partir de tudo que foi analisado e explorado anteriormente, entende-se que o EGC tem papel fundamental e pioneiro no que tange às políticas voltadas para o fortalecimento das capacidades de defesa brasileira, uma vez que por meio deste foram possíveis aprovações de diversas regulamentações, além do crescimento obtido em pontuação referente aos índices utilizados, demonstrando que, apesar de necessitar de melhorias, o exercício vem como forte contribuinte para garantir que o Brasil esteja

melhorando cada vez mais sua frente contra às ameaças cibernéticas de um mundo cada vez mais digitalizado.

REFERÊNCIAS

ANDRESS, J.; WINTERFELD, S. **Cyber warfare: techniques, tactics and tools for security practitioners**. Amsterdam; Boston: Elsevier, 2014.

ARTS, Sophie. Offense as the New Defense: New Life for NATO's Cyber Policy. **The German Marshall Fund of the United States, Policy Brief**, v. 39, p. 1-9, 2018.

AURÉLIO, Marcos, *et al*. **Guia de Defesa Cibernética na América Do Sul**. 2017.

BRASIL. Agência Nacional de Telecomunicações. **Resolução nº 740, de 21 de dezembro de 2020**. Diário Oficial da União: seção 1, Brasília, 22 dez. 2020. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740. Acesso em: 17 mar. 2025.

BRASIL. **Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.Gov)**. 2025. Disponível em: https://www.gov.br/ctir/pt-br. Acesso em: 27 mar. 2025.

BRASIL. **Comando Militar do Sudeste recebe mais uma vez o Exercício Guardião Cibernético**. 2022. Disponível em: https://cmse.eb.mil.br/index.php/ultimas-noticias-categoria/708-cmse-recebe-mais-uma-vez-o-exercicio-guardiao-cibernetico#:~:text=Conduzido%20pelo%20Comando%20de%20Defesa, nacional%20e%20das%20infraestruturas%20críticas. Acesso em: 10 mar. 2025.

BRASIL**. Decreto nº 9.573, de 22 de novembro de 2018**. Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União: seção 1, Brasilía, DF, 23 nov. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9573.htm. Acesso em: 11 mar. 2025.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética - E-Ciber. Diário Oficial da União: seção 1, Brasília, DF, 6 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 18 mar. 2025.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e dispõe sobre a governança de cibersegurança na administração pública federal. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11856.htm. Acesso em: 18 mar. 2023.

BRASIL. **Exercício Guardião Cibernético recebe diplomata e parlamentares na ESD**. 2024. Disponível em: https://www.gov.br/esd/pt-br/central-de-conteudo/noticias/exercicio-guardiao-cibernetico-recebe-diplomata-e-parlamentares-na-esd. Acesso em: 10 mar. 2025.

BRASIL. Exército Brasileiro. **Comandante do Exército acompanha o Exercício Guardião Cibernético 6.0**. 2024. Disponível em:

https://www.eb.mil.br/web/noticias/w/comandante-do-exercito-acompanha-o-exercicio-guardiao-cibernetico-6.0. Acesso em: 10 mar. 2025.

BRASIL. Exército Brasileiro. **Exército coordena maior exercício cibernético do hemisfério sul**. 2024. Disponível em: https://www.eb.mil.br/web/noticias/w/exercito-coordena-maior-exercicio-cibernetico-do-hemisferio-sul#:~:text=Histórico%20do%20Exercício%20Guardião%20Cibernético&text=A%20edição%20de%202023%2C%20por,aumentar%20a%20resiliência%20cibernética%20brasileira. Acesso em: 17 mar. 2025.

BRASIL. FAB. **Comandante de Operações Aeroespaciais visita Exercício Guardião Cibernético 6.0**. 2024. Disponível em: https://www.fab.mil.br/noticias/mostra/43283/DEFESA%20CIBERNÉTICA%20-%20Comandante%20de%20Operações%20Aeroespaciais%20visita%20Exercício%20Guardião%20Cibernético%206.0. Acesso em: 17 mar. 2025.

BRASIL. **Gabinete de Segurança Institucional da Presidência da República (GSI/PR)**. 2023. *Higiene Cibernética: boas práticas para a segurança no ciberespaço*. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/fasciculos/Fasciculo_higiene_cibernetica.pdf. Acesso em: 27 mar. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 120, de 21 de dezembro de 2022**. Diário Oficial da União: seção 1, Brasília, 22 dez. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918. Acesso em: 17 mar. 2025.

BRASIL. GSI. **Exercício Guardião Cibernético 3.0**. 2021. Disponível em: https://www.gov.br/gsi/pt-br/centrais-de-conteudo/noticias/2021/exercicio-guardiao-cibernetico-3.0. Acesso em: 15 mar. 2025.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. 2023.

BRASIL. Ministério da Defesa. **Em Brasília, exercício cibernético integra Forças Armadas com órgãos públicos e privados**. 2019. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/em-brasilia-exercicio-cibernetico-integra-forcas-armadas-com-orgao-publicos-e-privados. Acesso em: 14 mar. 2025.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Política Nacional de Defesa. Brasília, DF: MD, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 14 fev. 2025.

BRASIL. **Política Nacional de Segurança da Informação**. Decreto nº 9.637, de 26 de dezembro de 2018.

CAMPOS, Maxli Barroso. **[GTER 48 | GTS 34] Exercício Guardião Cibernético: Um estudo de caso de sucesso no Brasil**. YouTube. 15 de jan. 2020. Disponível em: https://www.youtube.com/watch?v=cWOwICGONPM. Acesso em: 17 mar 2025.

CHOWDHURY, N.; GKIOULOS, V. **Cyber Security Training for Critical Infrastructure protection: a Literature Review**. Computer Science Review, v. 40, n. 2, p. 100361, maio 2021.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War: The Next Threat to National Security and What To Do About It**. Nova York: Ecco, 2012.

CLAUSEWITZ, Carl Von. **Da guerra**. Tradução de Maria Teresa Ramos. São Paulo: Martins Fontes, 2003.

CMSE. **CMSE recebe mais uma vez o Exercício Guardião Cibernético. Comando Militar do Sudeste**. 2022. Disponível em: https://cmse.eb.mil.br/index.php/ultimas-noticias-categoria/708-cmse-recebe-mais-uma-vez-o-exercicio-guardiao-cibernetico. Acesso em: 17 mar. 2025.

COMDCIBER. **Curso Superior de Inteligência Estratégica, ESG**. 2021. Brasília.

COMDCIBER. **Exercício Guardião Cibernético 4.0 - Cenário Fictício do Exercício.** 2022. Brasília. Disponível em: https://cdn.brasildefato.com.br/documents/728256d0fb10a8531429bdd35c72daf8.pdf. Acesso em: 17 mar. 2025

DEFESA AÉREA & NAVAL. **Exercício Guardião Cibernético 5.0: Forças Armadas, órgãos públicos e empresas realizam grande treinamento.** 2023. Disponível em: https://www.defesaaereanaval.com.br/ciberseguranca/exercicio-guardiao-cibernetico-5-0-forcas-armadas-orgaos-publicos-e-empresas-realizam-grande-treinamento. Acesso em: 17 mar. 2025.

DEFESANET. **EGC 2.0 - Exercício Guardião Cibernético 2.0**. 2019. Disponível em: https://www.defesanet.com.br/defesa/egc-2-0-exercicio-guardiao-cibernetico-2-0/. Acesso em: 10 mar. 2025.

DEFESANET. **Guardião Cibernético 3.0 – Maior exercício de defesa do Hemisfério Sul**. 2021. Disponível em: https://www.defesanet.com.br/cyberwar/guardiao-cibernetico-3-0-maior-exercicio-de-defesa-do-hemisferio-sul/. Acesso em: 17 mar. 2025.

EPEX. **Defesa Cibernética**. 2023. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica>.

ESD**. Escola Superior de Defesa sedia a 5ª edição do Exercício Guardião Cibernético**. 2023. Disponível em: https://www.gov.br/esd/pt-br/central-de-conteudo/noticias/escola-superior-de-defesa-sedia-a-5a-edicao-do-exercicio-guardiao-cibernetico. Acesso em: 17 mar. 2025.

FEBRABAN. **FEBRABAN Tech 2024: Bancos à frente na segurança**. 2024. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/febraban-tech-2024-bancos-a-frente-na-seguranca/. Acesso em: 27 mar. 2025.

FGV; EB. **Manual de Orientação sobre Exercícios de Cibersegurança**. Rio de Janeiro: Fundação Getulio Vargas, 2024. Disponível em: https://www.fgv.br/fgvnoticias/fgv-e-exercito-brasileiro-lancam-manual-de-ciberseguranca-durante-egc-60. Acesso em: 10 mar. 2025.

GIL, A. C. **Como elaborar projetos de pesquisa**. [s.l.] São Paulo Atlas, 2002.

KASPERSKY. **Mapa de Ciberameaças da Kaspersky**. 2025 Disponível em: https://cybermap.kaspersky.com/pt/stats#country=215&type=OAS&period=m. Acesso em: 26 mar. 2025.

LESSIG, Lawrence. **Code and Other Laws of Cyberspace**. New York: Basic Books, 1999.

LIBICKI, M. C. **Cyberdeterrence and cyberwar**. Santa Monica, Ca: Rand, 2009.

MALAGUTTI, Marcelo Antonio Osller. **Software Power as a Cyber-Dissuasion Tool for Non-Aggressive Nations**. 2021. Tese (Doutorado em Ciências Militares). Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.

MELLO, Fábio P.; JUNIOR, Ricardo C. M.; ROCHA, Daniel, G. **Análise de Ataques DDoS**. 2010.

MONITOR MERCANTIL. **Setor bancário é o que mais investe em segurança cibernética**. 2024. Disponível em: https://monitormercantil.com.br/setor-bancario-e-o-que-mais-investe-em-seguranca-cibernetica/. Acesso em: 27 mar. 2025.

NCSI. **National Cyber Security Index – Brazil**. 2025. Disponível em: https://ncsi.ega.ee/country/br/?allData=1. Acesso em: 18 mar. 2025.

NEC. **Olimpíadas exigem cuidados com a segurança da informação**. 2016. Disponível em: https://blog.nec.com.br/olimpiadas-exigem-cuidados-com-si. Acesso em: 10 mar. 2025.

NETSCOUT. **DDoS Threat Intelligence Report**: LATAM and Brazil. 2024. Disponível em: https://www.netscout.com. Acesso em: 10 mar. 2025.

NYE, Joseph, S. **Deterrence and Dissuasion in Cyberspace.** International Security, v. 41, n.3, p. 44-71. 2017.

PAGLIARI, Graciela De Conti; OLIVEIRA, Marcos Aurélio Guedes de. 2014. **Defesa e Cooperação Interagências**. Recife: Editora UFPE. Coleção Defesa e Fronteiras Virtuais, v. 2.

RID, Thomas. **Active Measures: The Secret History of Disinformation and Political Warfare**. New York: Farrar, Straus and Giroux, 2020.

SLOAN, E. C. **Modern Military Strategy**. [s.l.] Routledge, 2016.

TI INSIDE. **Relatório alerta para vulnerabilidades que ameaçam infraestruturas globais**. Disponível em:

https://tiinside.com.br/04/11/2024/relatorio-alerta-para-vulnerabilidades-que-ameacam-infraestruturas-globais. Acesso em: 10 mar. 2025.

VIEIRA, H. P. **A defesa das infraestruturas críticas brasileiras à luz dos normativos e dos objetivos do Exercício Guardião Cibernético: uma análise construtiva**. Repositorio.esg.br, 2023.

WILLIAMS, P.; MCDONALD, M. **Security studies: An Introduction**. 3. ed. London ; New York: Routledge, Taylor & Francis Group, 2018.

EVERA, Stephen Van. **Guide to Methods for Students of Political Science**. Ithaca: Cornell University Press, 1997.