HENRIQUE PRIMO VIEIRA

A DEFESA DAS INFRAESTRUTURAS CRÍTICAS BRASILEIRAS À LUZ DOS NORMATIVOS E DOS OBJETIVOS DO EXERCÍCIO GUARDIÃO CIBERNÉTICO: UMA ANÁLISE CONSTRUTIVA

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção de título de Especialista em Altos Estudos de Defesa.

Orientador: Prof. Dr. Ivan Carlos Soares de Oliveira – Cel (EB) R1

Brasília
2023

Brasília, DF, 27 de novembro de 2023

Henrique Primo Vieira

HENRIQUE PRIMO VIEIRA
PESQUISADOR

HENRIQUE PRIMO VIEIRA

A DEFESA DAS INFRAESTRUTURAS CRÍTICAS BRASILEIRAS À LUZ DOS NORMATIVOS E DOS OBJETIVOS DO EXERCÍCIO GUARDIÃO CIBERNÉTICO: UMA ANÁLISE CONSTRUTIVA

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 16 de novembro de 2023

IVAN CARLOS SOARES DE OLIVEIRA – Cel Eng R1 EB (ESD)
Orientador

MARCO AURÉLIO CARVALHO LEANDRO – CF RM1 (ESD)
Membro 1

JOÃO FRANSWILLIAM BARBOSA – CMG (ESD)
Membro 2

A defesa das infraestruturas críticas brasileiras à luz dos normativos e dos objetivos do Exercício Guardião Cibernético: uma análise construtiva

Henrique Primo Vieira[1]

RESUMO

No contexto contemporâneo, a segurança cibernética emerge como uma preocupação vital, especialmente quando considerada sob a lente da proteção das infraestruturas críticas. Este estudo destaca a relevância do Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro, na coordenação das ações de defesa cibernética no Brasil. Entre essas ações tem-se o Exercício Guardião Cibernético (EGC), um exercício de simulação do tipo "*tabletop*", implementada pelo ComDCiber desde 2018, que busca avaliar a prontidão e capacidade de resposta dos órgãos públicos e empresas privadas brasileiras a incidentes cibernéticos que possam afetar infraestruturas críticas. Assim, o objetivo desta pesquisa é analisar os resultados obtidos através do EGC nos anos recentes, à luz de seus objetivos e de acordo com os normativos vigentes, buscando identificar eficácias e áreas de melhoria. Além disso, foram elucidados conceitos-chave na área de cibersegurança, como Espaço Cibernético e Segurança Cibernética, baseados na documentação oficial. A metodologia foi desenvolvida em três fases: inicialmente, uma revisão bibliográfica delineou o arcabouço normativo pertinente à defesa cibernética e à natureza das infraestruturas críticas. Em seguida, avaliações documentais e levantamentos junto ao ComDCiber aprofundaram os resultados do EGC, identificando pontos fortes e áreas de melhoria, com técnicas como análise descritiva e de conteúdo. Particular atenção foi dada ao setor de Telecomunicações, devido à sua transversalidade e potencial vetor de ameaças cibernéticas. Por fim, foi realizada uma discussão sobre os resultados, apontando oportunidades para otimizar a efetividade do EGC na promoção da resiliência cibernética das infraestruturas críticas brasileiras.

Palavras-chave: exercício guardião cibernético; infraestruturas críticas; defesa cibernética.

The defense of Brazilian critical infrastructures considering the regulations and objectives of the Cyber Guardian Exercise: a constructive analysis.

ABSTRACT

In the contemporary context, cybersecurity emerges as a vital concern, especially when considered through the lens of protecting critical infrastructures. This study highlights the relevance of the Brazilian Army's Cyber Defense Command (ComDCiber) in coordinating cyber defense actions in Brazil. Among these actions is the Cyber Guardian Exercise (EGC), a tabletop simulation exercise, implemented by ComDCiber since 2018, which seeks to assess the readiness and response capacity of Brazilian public bodies and private companies to cyber incidents that may affect critical infrastructure. Therefore, the objective of this research is to analyze the results obtained through EGC in recent years, in light of its objectives and in accordance with current regulations, seeking to identify efficiencies and areas for improvement. Furthermore, key concepts in cybersecurity were elucidated, such as Cyber Space and Cyber Security, based on official documentation. The methodology was developed in three phases: initially, a bibliographic review outlined the regulatory framework relevant to cyber defense and the nature of critical infrastructures. Then, documentary evaluations and surveys with ComDCiber deepened the EGC results, identifying strengths and areas for improvement, with techniques such as descriptive and content analysis. Particular attention was given to the Telecommunications sector, due to its transversality and potential vector of cyber threats. Finally, a discussion was held on the results, pointing out opportunities to optimize the effectiveness of the EGC in promoting the cyber resilience of Brazilian critical infrastructures.

Keywords: *cyber guardian exercise; critical infrastructures; cyber defense*.

---

[1] Especialista em Gestão de Telecomunicações da TELEBRAS S.A.

1 INTRODUÇÃO

A segurança cibernética é um tema central para a proteção das infraestruturas críticas, como sistemas de energia, transporte, telecomunicações e serviços financeiros, cujo funcionamento é vital para a estabilidade e bem-estar da sociedade (BRASIL, 2016).

O Comando de Defesa Cibernética (ComDCiber) é o órgão do Exército Brasileiro (EB) responsável por planejar, orientar e coordenar as atividades de defesa cibernética no país, sendo, portanto, peça central do Sistema Militar de Defesa Cibernética (SMDC). O Exercício Guardião Cibernético (EGC) brasileiro é um exercício do tipo *tabletop*, ou exercício de mesa, realizado pelo ComDCiber desde 2018 com o objetivo de avaliar a capacidade de resposta dos órgãos públicos e empresas privadas brasileiras a incidentes cibernéticos contra as infraestruturas críticas do país.

Os exercícios *tabletop* são simulações construtivas de cenários de ataques cibernéticos, realizados em sala de treinamento, com situações próximas ao real previsto, envolvendo representantes de várias entidades, como governo, setor privado e outras partes relevantes interessadas. O objetivo desses exercícios é testar a efetividade e operacionalidade, e melhorar a preparação, coordenação e resposta a incidentes cibernéticos, bem como fortalecer a cooperação entre as partes envolvidas.

No contexto de infraestruturas críticas de um país, como energia, transporte, serviços financeiros e telecomunicações, a realização de exercícios simulados do tipo *tabletop* são particularmente importantes. Eles permitem a identificação de vulnerabilidades, avaliação da prontidão operacional, treinamento de equipes de resposta a incidentes, e desenvolvimento de planos de contingência para garantir a resiliência dessas infraestruturas diante de ameaças cibernéticas.

Nesse sentido, o EGC, evento anual organizado e conduzido pelo ComDCiber, tem como objetivo simular um ambiente de guerra cibernética que envolve setores estratégicos do Brasil, dentre os quais, água, energia, financeiro, nuclear, transporte e telecomunicações, para testar e avaliar a prontidão e a capacidade de resposta do país para enfrentar ameaças cibernéticas a essas infraestruturas. Além do exercício *tabletop*, de simulação construtiva, os diversos participantes também são divididos em uma equipe "azul" (*blue team*) e uma equipe "vermelha" (*red team*) para realizar simulações virtuais de ataques e defesas cibernéticas a essas estruturas, com o objetivo de treinar procedimentos técnicos para combater as vulnerabilidades de seus sistemas e suas redes de comunicação de dados. Desde sua criação em 2018, o EGC tem se

mostrado uma importante ferramenta para aprimorar a segurança cibernética no país (SILVA, 2020).

Portanto, o EGC se apresenta como uma importante iniciativa do ComDCiber para aprimorar a segurança cibernética brasileira, arregimentando os setores da sociedade envolvidos com a defesa cibernética relacionados a infraestruturas críticas.

Neste contexto, é importante pesquisar os resultados obtidos nos exercícios para entender o que tem funcionado bem e onde há espaço para melhorias para aprimorar as resiliências das infraestruturas críticas, como resultado desses exercícios. Assim, a proposta desse trabalho de analisar os resultados alcançados com o EGC brasileiro, nos últimos anos, e a governança normativa voltada para infraestruturas críticas, está diretamente relacionada ao campo de estudo cibersegurança, uma das áreas prioritárias da Estratégia Nacional de Defesa (END) e da Política Nacional de Defesa (PND) (BRASIL, 2016, 2020c), voltada para a proteção das infraestruturas estratégicas do país. Além disso, a segurança cibernética é um fator chave para a competitividade de um país no cenário internacional, pois a vulnerabilidade da infraestrutura crítica pode colocar em risco a segurança nacional, a economia e a sociedade como um todo. A análise dos resultados alcançados pelos exercícios Guardião Cibernético, à luz de seus objetivos e de acordo com as diretrizes do END e PND, pode fornecer *insights* valiosos para fortalecer a segurança digital e resiliência das infraestruturas críticas do Brasil.

Considerando esse contexto, o presente estudo pretende investigar se os resultados do Exercício Guardião Cibernético brasileiro e as promulgações normativas no período indicam se os seus objetivos foram alcançados, e impactaram no aprimoramento da segurança cibernética das infraestruturas críticas do Brasil. Assim, a questão que se pretende responder é: como os resultados alcançados com o Exercício Guardião Cibernético brasileiro, conduzido pelo ComDCiber, entre os anos de 2018 e 2022, impactaram a segurança cibernética das áreas de infraestruturas críticas no Brasil, e quais são as lições aprendidas e propostas de melhoria resultantes (para) desses exercícios, à luz dos normativos vigentes?

A análise dos resultados obtidos visa, também, buscar informações para identificar pontos fortes e fracos desses exercícios, que podem contribuir com a segurança cibernética das infraestruturas críticas do Brasil e orientar futuras ações para evoluir o ambiente realístico das simulações de defesa cibernética das infraestruturas críticas no Brasil, criando um ambiente cada vez mais capacitado para resistir a ameaças cibernéticas e manter operações essenciais mesmo em face de ataques.

Dessa forma, o presente trabalho tem por objetivo geral verificar a evolução normativa e analisar o atingimento dos objetivos do EGC para o incremento da defesa das infraestruturas

críticas, a partir do levantamento dos normativos produzidos e dos resultados dos exercícios no período de 2018 a 2022. Para atingir esse objetivo, três objetivos específicos foram buscados como passos para analisar o problema. Assim, o primeiro objetivo específico é estudar o arcabouço normativo que disciplina a segurança cibernética, sua relação com as infraestruturas críticas e a concepção do Exercício Guardião Cibernético. O segundo é identificar os resultados dos exercícios para avaliar a evolução quantitativa e qualitativa ao longo dos cinco anos de análise. O terceiro objetivo é analisar os resultados obtidos, identificando os pontos fortes e fracos dos exercícios, e se há lacuna para melhoria dos exercícios para buscar melhor atingir seus objetivos.

Para alcançar os objetivos propostos, este trabalho foi realizado em três etapas. Na primeira etapa, a metodologia adotada foi a revisão bibliográfica para levantar informações sobre o arcabouço normativo envolvendo segurança e defesa cibernética, infraestruturas críticas, sobre o EGC e os exercícios cibernéticos realizados até o momento. Na segunda etapa, foi realizada levantamento dos resultados dos exercícios, baseado em avaliação documental e entrevista com o ComDCiber, organizador do EGC, com o objetivo de identificar os pontos fortes e fracos das respostas dadas pelos participantes, na coleta e análise de dados sobre os exercícios realizados; e nos resultados das Análises Pós-Ação (APA). Nessa etapa, foram utilizadas técnicas de análise de dados, como a análise descritiva e a análise de conteúdo. Na terceira etapa, fez-se a discussão dos resultados levantados e avaliado oportunidades de melhorias para a evolução do EGC e para a segurança cibernética para as infraestruturas críticas.

O artigo está estruturado da seguinte forma: na próxima seção, será apresentado o referencial teórico sobre os normativos e principais conceitos sobre segurança cibernética, infraestruturas críticas e exercícios cibernéticos; na seção seguinte, será descrito o Exercício Guardião Cibernético concebido pelo ComDCiber; nas duas próximas seções, serão apresentados e discutidos os resultados obtidos sobre os EGC de 2018 a 2022; e na última seção, serão feitas as considerações finais e as recomendações para trabalhos futuros.

2 SEGURANÇA E DEFESA CIBERNÉTICA PARA INFRAESTRUTURAS CRÍTICAS NO BRASIL

Para analisar e entender o cenário brasileiro de segurança e defesa cibernética, para que se possa buscar atingir os objetivos desse artigo, faz-se necessário descrever o arcabouço

normativo no setor cibernético e de infraestruturas críticas, as previsões legais e os principais termos relacionados a esse tema.

2.1 POLÍTICA E ESTRATÉGIA NACIONAL DE DEFESA

Como ponto de partida, deve-se avaliar a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) sob o prisma aqui a ser investigado, qual seja, a defesa e segurança cibernética.

A Política Nacional de Defesa (BRASIL, 2016), documento de mais alto nível do País em questões estratégicas de Defesa, positiva que o Estado, como provedor da segurança da população brasileira, é o responsável por coordenar as ações relacionadas à Defesa Nacional, na qual estabelece os Objetivos Nacionais de Defesa – OND, que devem ser permanentemente perseguidos pela Nação.

Nesse viés, a PND vigente, assevera, em sua análise do ambiente nacional, que o amplo espectro de possibilidades no ambiente cibernético requer especial atenção à segurança e à defesa desse espaço virtual, cujas informações contidas são essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações, e dos quais depende parcela significativa das atividades humanas (BRASIL, 2016).

Na mesma direção, a Estratégia Nacional de Defesa (BRASIL, 2016) trata da reorganização e reorientação das Forças Armadas, da organização da Base Industrial de Defesa e da política de composição dos efetivos da Marinha, do Exército e da Aeronáutica. A END define, ainda, os três setores tecnológicos essenciais, e, portanto, estratégicos, que devem ser fortalecidos para a Defesa Nacional a saber: o nuclear, o cibernético e o espacial. O documento delegou à Marinha do Brasil a gerência do programa nuclear; ao Exército Brasileiro, a liderança da defesa cibernética em território nacional; e à Força Aérea, o setor espacial. No Setor Cibernético, as capacitações deverão buscar ao mais amplo espectro de emprego civil e militar. As ações de Defesa devem buscar aprimorar a Segurança da Informação e das Comunicações e a Segurança Cibernética, em todas as instâncias do Estado, com ênfase na proteção das Estruturas Estratégicas relacionadas à Tecnologia da Informação. Ainda, deverá ser fortalecida a atuação colaborativa entre o Setor de Defesa e a comunidade acadêmica nacional, os setores público e privado e a Base Industrial de Defesa.

Em seu texto, a END também apresenta as Ações Estratégicas de Defesa – AED que visam orientar as medidas que deverão ser implementadas no sentido da consecução dos

Objetivos Nacionais de Defesa. Dentre as mais de oitenta AED, pode-se destacar ao menos cinco relacionadas ao setor cibernético (grifo nosso):

AED-1 - Desenvolver os setores estratégicos de defesa (nuclear, **cibernético** e espacial);

AED-2 - Contribuir para o incremento do nível de segurança das **Estruturas Estratégicas**;

AED-9 - Desenvolver as capacidades de monitorar e controlar o espaço aéreo, o **espaço cibernético**, o território, as águas jurisdicionais brasileiras e outras áreas de interesse;

AED-10 - Incrementar as capacidades de defender e de explorar o **espaço cibernético**;

AED-69 - Promover o desenvolvimento da **tecnologia cibernética**.

Portanto, observa-se que a PND e a END apontam que o Estado deve atuar em todas as frentes para garantir a segurança e defesa nacional e colocam o setor cibernético como uma frente estratégica, observando a proteção das Estruturas Estratégicas.

Além da PND e END, há outros documentos que trazem normatização para o setor cibernético, notadamente relacionados às infraestruturas críticas nacionais, tanto no âmbito da Defesa quanto do âmbito de políticas públicas (por exemplo, PNSI, E-Ciber), que serão analisadas a seguir.

2.2 CONCEITOS E MARCOS NORMATIVOS

A PND, a END, a Política Nacional de Segurança da Informação (PNSI), a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), a Estratégia Nacional de Segurança Cibernética (E-Ciber), o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic) e o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (elaborado pela ANATEL) são importantes instrumentos para a proteção e defesa do Brasil no ciberespaço.

Antes, porém, de se avaliar as contribuições desses normativos para o setor cibernético, notadamente relacionados à segurança das infraestruturas críticas nacionais, tanto no âmbito da Defesa quanto do âmbito de políticas públicas, faz-se necessário caracterizar alguns conceitos, baseados no Glossário das Forças Armadas - MD35-G-01, atualizado até 2020 (BRASIL, 2015) e na Doutrina Militar de Defesa Cibernética - MD31-M-07 (BRASIL, 2014), que trarão maior entendimento e suportarão uma análise crítica do tema:

a. Espaço cibernético;
b. Segurança Cibernética;
c. Sistema Militar de Defesa Cibernética;

d. Defesa e Proteção Cibernética;
e. Guerra Cibernética;
f. Prontidão Cibernética;
g. Resiliência Cibernética;
h. Segurança das Infraestruturas Críticas.

a) O Espaço Cibernético pode ser caracterizado como um espaço virtual, composto por dispositivos computacionais conectados em rede ou não, onde as informações digitais transitam, são processadas e armazenadas (BRASIL, 2011). Por ser virtual, não possui fronteiras tangíveis, sendo, portanto, mais vulnerável a ataques . Conforme Segundo (2019), este espaço é essencial para garantir o funcionamento dos sistemas de informações, gerenciamento e comunicações, dos quais depende uma parcela significativa das atividades humanas.

b) A Segurança Cibernética é um conceito de segurança fundamental que abrange a proteção de sistemas, redes e informações contra ameaças e ataques cibernéticos (MARINHO, 2022). De acordo com o Glossário das Forças Armadas - MD35-G-01 (BRASIL, 2015), a segurança cibernética visa “assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas”. De outro modo, envolve medidas para garantir a integridade, confidencialidade e disponibilidade dos sistemas de informação.

c) O Sistema Militar de Defesa Cibernética (SMDC) é um componente vital no contexto da segurança cibernética. Segundo o mesmo glossário (BRASIL, 2015), ele se refere ao conjunto de recursos, de pessoal e de capacidades técnicas aptos a serem empregados de forma coordenada, no espaço cibernético, para defender os interesses nacionais. O Comando de Defesa Cibernética é o órgão central do SMDC, um comando operacional conjunto, permanentemente ativado e com capacidade interagências. A capacidade interagências é caracterizada pela atuação colaborativa com representantes de órgãos da administração pública federal, de infraestruturas críticas e de outros órgãos, instituições e empresas, públicos ou privados, de interesse da Defesa (BRASIL, 2020d). Ainda, o SMDC atua em conjunto com outras políticas e estratégias nacionais para garantir a segurança cibernética do país, protegendo as infraestruturas críticas e minimizando os impactos de eventuais incidentes cibernéticos.

d) A Defesa e a Proteção Cibernética são fundamentais para garantir a proteção de informações sensíveis e a continuidade das operações em infraestruturas críticas de interesse da Defesa Nacional. De acordo com o glossário (BRASIL, 2015), no âmbito militar, a defesa cibernética compõe-se de um conjunto de ações estratégicas para proteger os sistemas de

informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. A defesa cibernética envolve a implementação de políticas, procedimentos e tecnologias para garantir a segurança dos sistemas e dados A proteção cibernética é a ação em si, de caráter permanente, que visa neutralizar ataques e exploração de vulnerabilidades contra os dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética (BRASIL, 2014).

e) A Guerra Cibernética é um termo que descreve ações cibernéticas conduzidas em um contexto militar ou de conflito. O glossário (BRASIL, 2015) define como ações ofensivas e defensivas no espaço cibernético, que visam enfraquecer as capacidades do inimigo ou proteger os próprios recursos cibernéticos. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC), cuja utilização será proporcional à dependência do oponente em relação à TIC. A guerra cibernética pode ter impactos significativos na segurança nacional e na economia do país.

f) A Prontidão Cibernética refere-se à capacidade de responder efetivamente às ameaças cibernéticas. Como definido no glossário (BRASIL, 2015), isso implica estar preparado para identificar, avaliar e mitigar ameaças cibernéticas de forma rápida e eficaz, sendo fundamental para garantir a continuidade das operações em infraestruturas críticas e a proteção de informações sensíveis.

g) A resiliência cibernética é a capacidade de resistir a ataques cibernéticos, recuperar-se e continuar a operar de maneira eficaz. De acordo com o glossário (BRASIL, 2015), a resiliência cibernética é essencial para garantir a continuidade das operações em infraestruturas críticas em face de ameaças cibernéticas, e se for o caso restabelecê-las prontamente após uma ação adversa.

h) A Segurança das Infraestruturas Críticas é uma preocupação perene, não apenas para as Forças Armadas, mas também para a sociedade em geral. De forma sintética, pode ser entendida como um arcabouço de medidas, preventivas e reativas contra ameaças cibernéticas, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas (BRASIL, 2018a). Importante observar que a segurança das infraestruturas críticas se faz relevante, tanto para garantir a continuidade das operações em setores essenciais para o país, quanto pela sua transversalidade setorial, dado que um evento adverso que impacte negativamente um setor específico pode induzir danos colaterais a outros setores interdependentes. Ilustrativamente, um ataque perpetrado contra uma instalação de geração de energia hidrelétrica pode acarretar consequências de alto impacto, por exemplo, para uma

estação de tratamento de água ou para uma infraestrutura de telecomunicações que dependem da energia dessa usina (NONATO; PINHO, 2021) que por sua vez, podem afetar as instalações bancárias, atingindo o sistema financeiro, e em forma de cascata, no limite, trazer caos a um país.

Esses conceitos são essenciais para a compreensão das estratégias de segurança cibernética, tanto no âmbito da Defesa quanto das políticas públicas, e são a base para uma análise dessas estratégias e seus impactos no cenário cibernético brasileiro.

2.2.1 Política Nacional de Segurança da Informação

A PNSI foi instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional. Nessa política, a segurança da informação abrange em seu arcabouço a segurança cibernética, a defesa cibernética, bem como a segurança física e a proteção de dados organizacionais (BRASIL, 2018b). Tendo em vista essa abrangência, a PNSI definiu como instrumentos a Estratégia Nacional de Segurança da Informação (ENSI) e os planos nacionais. A ENSI deverá conter as ações estratégicas e os objetivos relacionados à segurança da informação, e construída em módulos contemplando a Segurança Cibernética, a Defesa Cibernética, a Segurança das Infraestruturas Críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados (BRASIL, 2018b).

2.2.2 Política Nacional de Segurança de Infraestruturas Críticas

O Decreto nº 9.573, de 22 de novembro de 2018, aprovou a PNSIC, a qual define infraestruturas críticas como instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2018b). Ainda, a PNSIC caracteriza a segurança das infraestruturas críticas como um conjunto de diretrizes e medidas externas para a proteção de ativos e sistemas de importância estratégica no Brasil. Apresenta, também, as orientações indispensáveis ao esforço conjunto a ser desenvolvido pelos órgãos e entidades dos setores público e privado no que diz respeito à atividade de segurança de infraestruturas críticas. A PNSIC é, portanto, essencial para garantir a resiliência das infraestruturas críticas, como energia, transporte, comunicações e finanças, contra ameaças e ataques cibernéticos.

A PNSIC também define, como instrumentos para sua a implementação, a Estratégia Nacional de Segurança de Infraestruturas Críticas, o Plano Nacional de Segurança de Infraestruturas Críticas, e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (SIDSIC) (BRASIL, 2018b).

A ENSIC, aprovada pelo Decreto n° 10.569, de 9 de dezembro de 2020, é um documento que consolida conceitos e identifica os principais desafios para a atividade de segurança de infraestruturas críticas. Ela define eixos estruturantes e objetivos estratégicos para criar as melhores condições para que o país possa se antecipar às ameaças e aproveitar as oportunidades de aprimoramento da segurança de infraestruturas críticas. A Estratégia Nacional de Segurança de Infraestruturas Críticas serve como orientação estratégica e de referência para as ações estratégicas elaboradas para o Plansic.

2.2.3 Estratégia Nacional de Segurança Cibernética

Considerando a Segurança Cibernética como a área mais crítica a ser abordada, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) elencou a E-Ciber como o primeiro módulo da ENSI a ser elaborado (SEGUNDO, 2019).

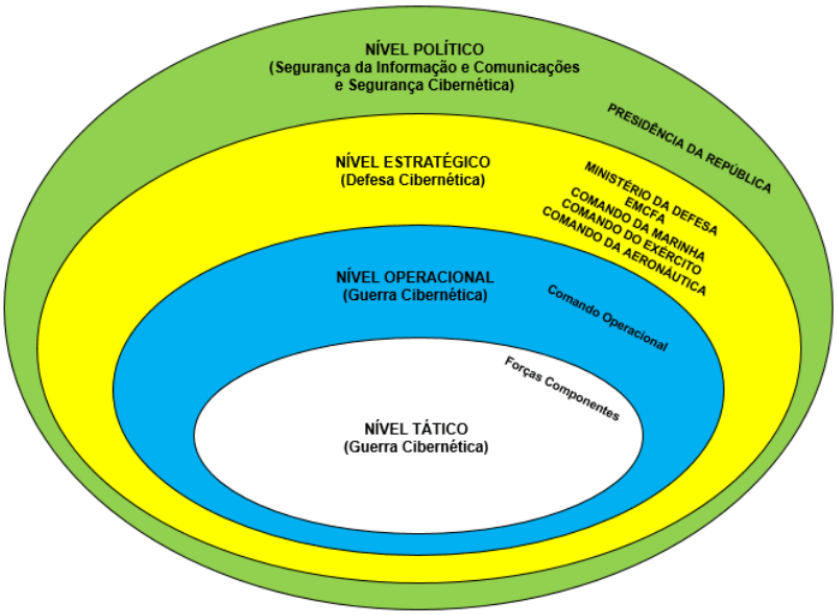
A E-Ciber foi aprovada pelo Decreto nº 10.222, de 05 de fevereiro de 2020 (na forma de seu anexo), conforme disposto no inciso I do art. 6º do decreto que instituiu a PNSI, e assevera que:

> No atual cenário de ameaças cibernéticas, é provável que as organizações experimentem o **mesmo tipo de ataque**, o que ressalta a importância das **informações sobre fato, sobre o tratamento realizado e sobre as lições aprendidas**. Nesse contexto, visa-se à **atuação conjunta** em prol da **segurança cibernética**, e considera-se de suma importância a criação de um **ambiente colaborativo**, do qual participem a **administração pública, o setor privado, a academia e a sociedade em geral**.
> Um exemplo de **ação colaborativa** é o **exercício Guardião Cibernético**, organizado anualmente pelo **Comando de Defesa Cibernética, em parceria com o Gabinete de Segurança Institucional da Presidência da República**. A atividade consiste em treinamento de ações de proteção cibernética, por meio da **cooperação** entre **Forças Armadas, órgãos parceiros e representantes das infraestruturas críticas**, ao adotar técnicas virtuais de simulação e práticas de gestão de incidentes. O exercício emprega gabinetes de crise das áreas de tecnologia da informação e comunicação, de comunicação social, jurídica e da alta administração dos participantes, que são levados a apresentar soluções para os eventos cibernéticos com impacto nas organizações, incluindo o nível **decisório-gerencial** (gestão de crise) e o **nível técnico** (resposta a incidentes) das empresas e de órgãos de governo. (BRASIL, 2020a, grifo do autor).

A E-Ciber, além de preencher uma importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com o objetivo de modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e indivíduos sobre o assunto (BRASIL, 2020a). Dentre suas ações estratégicas, busca elevar o nível de proteção das infraestruturas críticas, de modo a aumentar sua resiliência, através da promoção de interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética, bem como incentivar a participação dessas infraestruturas críticas em exercícios cibernéticos.

Alinhado à E-Ciber, tem-se, portanto, no nível político e estratégico, figura 1, todo um normativo para as infraestruturas críticas, que começa com a PNSIC, de 2018, seguida da ENSIC, de 2020, e finalmente pelo Plansic, de 2022.

Figura 1 - Níveis de atuação do Setor Cibernético



Fonte: MD31-M-07 (BRASIL, 2014).

2.2.4 Plano Nacional de Segurança de Infraestruturas Críticas

O Plansic foi aprovado pelo Decreto nº 11.200, de 15 de setembro de 2022, e tem como objetivo implantar um sistema com metodologias para identificar as infraestruturas críticas e definir as responsabilidades dos órgãos envolvidos na segurança dessas infraestruturas. Ele define as áreas prioritárias de aplicação, prevê o envolvimento dos entes federados e da sociedade, destaca a gestão de riscos e o estudo de interdependência e reúne um conjunto de

ações estratégicas, com respectivas metas e prazos, elaboradas com o objetivo de estabelecer e organizar responsabilidades na implementação da PNSIC (BRASIL, 2022b).

Um de eixos estruturantes do Plansic é o de "envolver, nos exercícios Guardião Cibernético, setores abordados em Segurança de Infraestruturas Críticas, com meta de envolver dois ou mais setores de infraestruturas críticas na realização dos EGC a cada ano (BRASIL, 2022b)". Atualmente, em 2023, das áreas prioritárias elencadas na Plansic, quadro 1, apenas as áreas prioritárias de Águas e de Comunicações não estão completas, por ainda não terem sido incluídos os setores dessas áreas, de Barragens e Radiodifusão, respectivamente.

Quadro 1 - Setores de Segurança de Infraestruturas Críticas

ÁREA PRIORITÁRIA	SETOR
Águas	**Barragens**
	Abastecimento Urbano de Águas
Energia	Energia Elétrica
	Petróleo, Gás Natural e Biocombustíveis
Transporte	Terrestre
	Aéreo
	Aquaviário
Comunicações	Telecomunicações
	Radiodifusão
	Serviços Postais
Finanças	Finanças
Biossegurança e Bioproteção	Biossegurança e Bioproteção
Defesa	Defesa

Fonte: Adaptado de (BRASIL, 2022b), grifo do autor.

Por último, o Plansic integra-se a uma série de outras iniciativas de segurança como a Política Nacional de Inteligência (PNI)[2] e a Estratégia Nacional de Inteligência (ENINT)[3]. Essas iniciativas, quando analisam o ambiente estratégico para a atividade de inteligência, apontam ameaças e desafios às infraestruturas críticas nacionais, trazendo à luz os riscos de

[2] Decreto nº 8.793/2016 de 29.06.2016.
[3] Decreto Presidencial 14.503 de 15.12.2017.

sabotagem pela via cibernética. Nessa esteira, a ENINT assevera, dentre seus orientadores, a necessidade de intercâmbio de conhecimentos no campo cibernético entre os setores público, privado e academia, bem como o fortalecimento dos sistemas de segurança da informação nas estruturas críticas do País (BRASIL, 2017).

2.3 INFRAESTRUTURAS CRÍTICAS

A END definiu na AED-2 as Estruturas Estratégicas como sendo as infraestruturas relacionadas com sistema de captação, tratamento e distribuição de água, geração e distribuição de energia elétrica, sistemas de transporte, produção e distribuição de combustíveis, fianças, comunicações e cibernética.

A PNSIC definiu e normatizou o conceito de infraestruturas críticas, com abrangência para toda a administração pública, com sendo "as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade" (BRASIL, 2018b). Embora a PNSIC não tenha definido em seu bojo as áreas prioritárias para a proteção cibernética, delegou essa definição para a ENSIC. Essa Estratégia Nacional de Infraestruturas Críticas, em seu anexo, estabeleceu que "as infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial para a segurança e soberania nacionais (BRASIL, 2020a)". Apesar de estabelecer essas áreas como rol prioritário, a ENSIC permite o estabelecimento de outros setores julgados de interesse para a Defesa Nacional (BRASIL, 2020a).

Portanto, depreende-se, aqui, que as Estruturas Estratégicas (EE) previstas na END são as Infraestruturas Críticas (IC) disciplinadas e priorizadas pela PNSIC e pela ENSIC.

2.4 O SETOR CIBERNÉTICO E O EXERCÍCIO GUARDIÃO CIBERNÉTICO

No nível estratégico tem-se, conforme já apresentado, a END, com primeira edição em 2008, onde foram definidos os três setores estratégicos para a segurança nacional: setor nuclear, setor cibernético e setor espacial. Em 2009, através da Diretriz Ministerial 014/MD/2009, houve a definição pelo Ministério da Defesa que a Marinha ficasse a cargo do setor nuclear, o Exército responsável pelo setor cibernético e a Aeronáutica encarregada do setor espacial. Na atualização da END 2020, que ainda está em apreciação pelo Congresso Nacional, os setores estratégicos, foram igualmente mantidos, e para o setor cibernético, em específico, a END consigna que as capacitações serão destinadas ao emprego dual em seu mais amplo espectro, e incluirão, como

parte prioritária, as tecnologias de comunicações visando aprimorar a Segurança da Informação e das Comunicações e Cibernética com ênfase na proteção das Estruturas Críticas (BRASIL, 2020c).

Para atender a delegação do setor cibernético ao Exército, definido pela END (BRASIL, 2012), foi ativado em 15 de abril de 2016 o Comando de Defesa Cibernética – ComDCiber, organização militar conjunta, na estrutura organizacional do Comando do Exército. Sua missão é planejar, orientar, coordenar, integrar e executar atividades relacionadas ao desenvolvimento e aplicação das capacidades cibernéticas, a fim de contribuir para o uso efetivo do espaço cibernético, bem como de capacitação no setor cibernético de defesa.

Em 2020 foi assinada a portaria do Ministério da Defesa criando o Sistema Militar de Defesa Cibernética, que estava previsto na Política Cibernética de Defesa[4], de 2012. Conforme já descrito, o SMDC tem o objetivo de assegurar o uso efetivo do espaço cibernético e protegê-lo contra ações hostis contra os interesses da Defesa Nacional. Para organizá-lo, a portaria define que o ComDCiber, comando operacional conjunto, permanentemente ativado e com capacidade interagências, é o seu órgão central (BRASIL, 2020d).

A capacidade interagências, desatacada pela portaria como predicado do ComDCiber, caracteriza-se pela atuação colaborativa com representantes dos órgãos da Administração Pública Federal, das Infraestruturas Críticas e de outros órgãos, instituições e empresas (públicas ou privadas) de interesse para a Defesa Nacional.

O ComDCiber, então, lida com as Infraestruturas Críticas segundo orientação, no nível político, pelo Gabinete de Segurança Institucional da Presidência da República. Havendo risco ou interesse para a Defesa Nacional, e sendo acionado pelo GSI/PR, o ComDCiber atua de modo a trazer a referida infraestrutura crítica para dentro do SMDC, e a partir desse ponto há atuação colaborativa e integrada do ComDCiber com essa infraestrutura.

O ComDCiber, no objetivo de cumprir sua missão, desenvolveu um exercício de integração para aproximar os setores responsáveis pelas Infraestruturas Críticas e de interesse da Defesa, e para contribuir para o incremento do nível de proteção do espaço cibernético nas infraestruturas críticas. O modelo do exercício adotado foi baseado no *Locked Shields*, exercício anual organizado pela CCDCOE (*Cooperative Cyber Defence Centre of Excellence*) da OTAN desde 2010, cujo foco está montado em cenários realistas, tecnologias de ponta e simulando toda a complexidade de um incidente cibernético, incluindo tomadas de decisão estratégicas e

[4] A Política Cibernética de Defesa foi aprovada pela Portaria Normativa nº 3.389/MD de 21 de dezembro de 2012.

gerenciais, aspectos jurídicos e de comunicação (NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE apud COSTA; FERREIRA; CABRAL, 2022).

No caso brasileiro, o exercício adota técnicas de simulação virtual (*blue team/red team*) e construtiva (*tabletop*). A simulação virtual busca identificar e difundir as melhores práticas das equipes de especialistas em tratamento de incidentes. A simulação construtiva permite exercitar o nível estratégico/gerencial dos entes participantes na solução de problemas cibernéticos simulados (PCS) por meio de ações envolvendo as áreas de segurança da informação, jurídica e de comunicação social das organizações (SILVA, 2020).

2.4.1 O Exercício Guardião Cibernético

Na revisão da literatura sobre treinamento em segurança cibernética para proteção de infraestrutura crítica, Chowdhury e Gkioulos (2021) apontam que a simulação de exercícios cibernéticos é uma ferramenta importante para avaliar a resiliência de uma organização contra ameaças cibernéticas. Esse estudo apresenta uma revisão dos tipos de simulação existentes, incluindo simulações baseadas em papel, simulações de rede e simulações de mesa (*tabletop*) e de ambiente virtual. O estudo conclui que a simulação de ambiente virtual é a mais eficaz para exercícios cibernéticos, pois permite a criação de cenários realistas e a avaliação de habilidades técnicas e comportamentais dos participantes. Além disso, a simulação de ambiente virtual pode ser usada para treinar equipes de resposta a incidentes e melhorar a colaboração entre as equipes de segurança.

Segundo Maglaras (2022), em seu trabalho sobre os desafios e soluções para a segurança cibernética de infraestruturas críticas, fazem parte das soluções para lidar com ataques contra infraestruturas críticas treinamentos de conscientização de segurança da informação para usuários e simulações de exercícios cibernéticos para os entes que atuam nas equipes de segurança. Nesse sentido, as simulações de exercícios cibernéticos se apresentam como uma solução para fortalecer a segurança das infraestruturas críticas, sendo uma forma eficaz de avaliar a resiliência de uma organização contra ameaças cibernéticas dado que as simulações de exercícios cibernéticos permitem criar cenários realistas e avaliar as habilidades técnicas e comportamentais dos participantes, além de treinar equipes de resposta a incidentes e melhorar a colaboração entre as equipes de segurança (MAGLARAS; JANICKE; FERRAG, 2022).

No Brasil, o ComDCiber realiza, desde 2018, o Exercício Guardião Cibernético, que é uma simulação de ataques cibernéticos em larga escala para avaliar a capacidade de resposta do país a ameaças cibernéticas às suas infraestruturas críticas e de defesa. Esse exercício tem

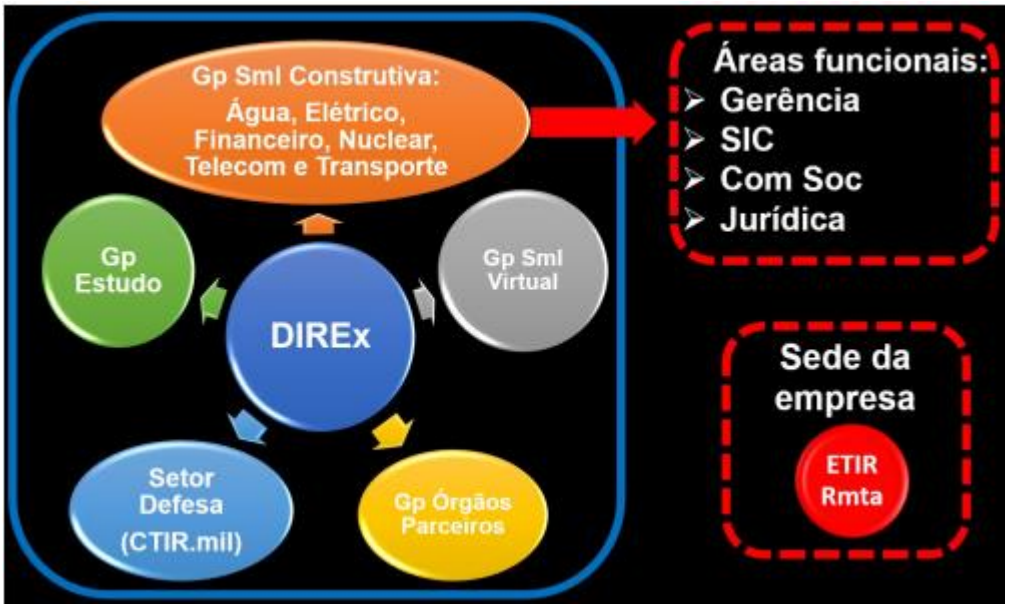
como principais objetivos: coordenar e integrar, em ambiente interagências, a segurança e defesa cibernéticas para a proteção de IC; exercitar o processo decisório em diferentes níveis de responsabilidade e competência, ressaltando a necessidade de atuação colaborativa na prevenção, solução e mitigação de danos causados por ameaças existentes no espaço cibernético; verificar a efetividade de procedimentos para a solução de incidentes em infraestruturas críticas da informação; contribuir para a atuação colaborativa e para o network entre Governo, Defesa, Setor Privado e Academia, por meio de simulações virtual e construtiva (*Tabletop Exercise* e SIMOC), bem como propondo contribuição doutrinária (Grupo de Estudo); e proporcionar ambiente favorável para que as empresas e organizações simulem incidentes que permitam colher ensinamentos para o aprimoramento de processos e protocolos internos (BRASIL, 2022a).

Nesse sentido, o EGC pretende ser um treinamento simulado que envolve a proteção cibernética, por intermédio da atuação colaborativa das Forças Armadas, dos Órgãos Parceiros e dos principais setores de Infraestruturas Críticas do Brasil, adotando técnicas de simulações construtiva e virtual de forma integrada. No EGC, tanto a simulação construtiva como a de ambiente virtual usam ferramentas para exercícios cibernéticos, permitindo a criação de cenários realistas e a avaliação de habilidades técnicas e comportamentais dos participantes. Em sua concepção, o exercício é composto por 3 grandes áreas:

1. Grupo de Estudo: tem como missão elaborar estratégias que contribuam para a resiliência cibernética do país. Nesse grupo, os temas são indicados pelos Setores e não pela Defesa (BRASIL, 2022a). No caso do setor de Comunicações, a Agência ANATEL em conjunto com as empresas reguladas utiliza o momento do grupo de estudos do EGC para realizar entregas que proporcionem o aumento da resiliência cibernética, como estudos sobre criptografia, proposição de novas portarias e normas de segurança etc.
2. Simulação virtual: a simulação virtual utiliza um Simulador de Operações Cibernéticas (SIMOC), no qual são reproduzidos sistemas de rede e computacionais utilizados pelos especialistas dos órgãos e empresas participantes. A simulação virtual tem o objetivo de identificar e difundir as melhores práticas de cada equipe de tratamento de incidentes de rede (ETIR) (SILVA, 2020).
3. Simulação construtiva (*tabletop exercise*): a simulação construtiva emprega gabinetes de crise das áreas de tecnologia da informação, comunicação social, jurídica e alta administração, que apresentam soluções para os Problemas Cibernéticos Simulados (PCS) com impacto nas organizações, encaminhados pela

Direção do Exercício (DIREx) ao grupo de simulação construtiva, conforme figura 2. A DIREx é formada por um representante do nível estratégico de cada órgão ou empresa participante. As discussões nos gabinetes de crise demandam ações nos níveis decisório/gerencial (gestão de crise) e técnico (resposta ao incidente) (NONATO; PINHO, 2021). A simulação construtiva permite, portanto, exercitar o nível gerencial das organizações participantes na solução de problemas cibernéticos simulados, por meio de ações envolvendo as áreas de segurança da informação, jurídica e de comunicação social de cada órgão ou empresa participante (BRASIL, 2022a).

Figura 2 - Concepção do EGC



Fonte: COMDCIBER (BRASIL, 2022a).

A elaboração dos PCS é coordenada pelo Estado-Maior Conjunto (EM Cj) do ComDCiber e envolve a ação integrada junto às entidades focais de cada área prioritária participante: Águas, Energia, Transporte, Comunicações, Finanças, Biossegurança e Bioproteção e Defesa (BRASIL, 2022a). Na maioria dos casos, a entidade focal é a agência reguladora do setor.

Como pano de fundo para a execução do exercício, é empregado cenário fictício de não-guerra, utilizado na Operação MERIDIANO do Ministério da Defesa, envolvendo as Forças Armadas e as áreas estratégicas de interesse para a Defesa Nacional (SILVA, 2020), partindo de uma situação de normalidade para um estado de grave crise no espaço cibernético.

Os participantes atuam de forma colaborativa e integrada nos esforços voltados para prevenir e solucionar incidentes definidos nos PCS envolvendo ativos de comunicação e informação relevantes para as infraestruturas críticas e demais setores estratégicos. Com o exercício, o Exército Brasileiro, por intermédio do ComDCiber, busca contribuir para a integração entre governo, setor privado e meio acadêmico, atuando de forma colaborativa conforme definido na E-Ciber, e para o incremento da proteção do espaço cibernético nacional, conforme definido na END, tendo ainda como objetivos verificar a eficácia dos procedimentos, aplicar boas práticas cibernéticas, empregar ferramentas de compartilhamento de informações e propiciar um ambiente para as empresas e organizações para simular práticas de proteção de incidentes.

Importante destacar, também, que através do EGC é possível reunir a tríplice hélice, onde se congregam a Indústria (setor privado), o Governo (Segurança – GSI/PR e Defesa – Forças Armadas e ComDCiber) e Academia discutindo Segurança Cibernética para o incremento da resiliência cibernética do país.

3 RESULTADOS RELACIONADOS COM OS OBJETIVOS DOS EGC

Baseado em levantamento documental junto ao ComDCiber, publicações em sítios da Internet, vídeos oficiais do Exército Brasileiro de apresentação da execução e resultados dos EGC, foram obtidas informações relevantes para a compreensão dos resultados dos exercícios para a defesa e proteção cibernética em ambientes de infraestrutura crítica. Além dos levantamentos quantitativos e qualitativos gerais dos EGC, buscou-se, também, conforme apresentado na sessão 2, levantar o arcabouço legal e normativo produzido e vigente no Brasil relacionado a segurança cibernética relacionada com infraestruturas críticas, foco do EGC, bem como uma ênfase no setor de Telecomunicações, por ser transversal a todos os setores e por ser um vetor necessário para os criminosos alcançarem o espaço cibernético privativo das organizações.

3.1 A EVOLUÇÃO DO GUARDIÃO CIBERNÉTICO

O EGC 1.0 ocorreu em 2018, no período de 3 a 6 de julho, com a participação 106 integrantes dos setores Nuclear, Financeiro, Defesa e órgãos parceiros, em um total de 23 organizações. Houve, portanto, dois setores de infraestrutura crítica (Nuclear e Financeiro) envolvidos, além da Defesa, em quatro dias de exercício. Foram apresentados 59 desafios para os operadores cibernéticos. Esses desafios simulados ocorreram exclusivamente intrassetor.

Teve como principal objetivo engajar os participantes para atuar de forma colaborativa na proteção de ataques no espaço cibernético e realizar o exercício do processo decisório em diferentes níveis; e como resultado destacado, entre os participantes, a integração entre os times das instituições, GSI/PR e ComDCiber, para troca de informação para que haja reação efetiva em casos de ataques cibernéticos para os setores envolvidos (BANDEIRA, 2018).

O grupo de estudos elencou as premissas básicas para a elaboração de um Plano Nacional de Tratamento e Resposta a Eventos de Segurança Cibernética. O material produzido foi utilizado como referência na elaboração de um Plano Nacional, que foi submetido ao GSI/PR, com previsão de aprovação para fevereiro/2019 (CAMPOS, 2020). Em 22/11/2018 foi aprovada a PNSIC estabelecendo, entre outras coisas, o Plansic, com os subsídios desse grupo de estudo.

A simulação virtual teve dois papéis: funcionar como apoio local da equipe de simulação construtiva na solução dos eventos e por identificar e tratar eventos em um ambiente de rede simulado, utilizando o programa Simulador de Operações Cibernéticas (SIMOC), disparados pela DIREx de cada empresa participante.

O EGC 2.0 ocorreu em 2019, no período de 2 a 4 de julho, com a participação 215 integrantes. Além dos setores Nuclear, Financeiro, Defesa e órgãos parceiros, do EGC 1.0, houve a inclusão de mais dois setores de infraestruturas críticas, Telecomunicações e Elétrico, congregando um total de 41 organizações. Houve, portanto, quatro setores de infraestrutura crítica envolvidos, em três dias de exercício. Note-se, aqui, que a concepção inicial do exercício era a de substituição e alternância de setores das infraestruturas críticas, sendo chamados dois setores a cada ano. Da avaliação do potencial de evolução do exercício e importância de unir mais setores para a execução de uma simulação intersetorial, cujos problemas simulados, com suas consequências, poderiam ser aplicados para tonar o exercício mais real, os setores Financeiro e Nuclear solicitaram sua participação no EGC 2.0. Essa foi uma lição aprendida e sugestão de evolução do EGC 1.0, que foi expandida para os demais exercícios (CAMPOS, 2020). O setor de Telecomunicações foi coordenado pela ANATEL e contou com a participação de 5 (cinco) empresas do setor.

Foram apresentados 57 Problemas Cibernéticos Simulados (PCS) para os operadores cibernéticos da simulação construtiva, considerando todos os setores. Como lição aprendida do EGC 1.0, este exercício aplicou problemas simulados com afetação intrassetor e intersetor, com o objetivo de provocar uma maior interação em as organizações, tendo em vista que no espaço cibernético alguns setores são transversais, como o Elétrico e o de Telecomunicações. O gabinete de crise de cada empresa/entidade foi composto de 4 representantes: um representante

da alta administração, um da gerência de TIC, um de comunicação social, e um do departamento jurídico. Os problemas simulados encaminhados pelo DIREx para o gabinete de crise deveriam ser resolvidos de forma hipotética, com registro da possível análise do evento, propostas de medidas preventivas e reativas e levantamento de possíveis impactos que poderiam ser causados pelo evento. Os representantes de alto nível, na DIREx de cada empresa/entidade, foram reunidos em um ambiente único, com objetivo que houvesse troca de informações intrassetor e intersetor. Os gabinetes de crise de cada setor foram separados por salas, havendo interrelação de gabinetes de crise apenas intrassetor. Dentro dessas propostas de tratamento dos PCS, cada empesa/entidade deveria exercitar seus processos e protocolos internos de comunicação, avaliação de impactos jurídicos e de imagem (SILVA, 2020). As respostas foram avaliadas pelo DIREx de cada empresa/entidade, mas sem um gabarito para validação das respostas dadas pelo gabinete de crise. Como tanto a DIREx quanto o gabinete crise são formados por participantes de nível gerencial das áreas estratégicas de cada entidade as respostas dadas foram de alto nível, focados em treinar processos de comunicação e tratamento do evento, e não quanto às técnicas de mitigação e resolução técnica dos ataques propriamente dito.

A simulação virtual, como no EGC 1.0, utilizou o programa Simulador de Operações Cibernéticas (SIMOC), para simular uma rede computacional que seria sujeita a ataques cibernéticos. Cada empresa/entidade participante enviou um especialista técnico para atuarem de forma conjunta, formando um único *blue team*, que é o time de defesa para tratamento de incidentes de redes, responsável por buscar e identificar as vulnerabilidades na rede simulada. Diferente do EGC 1.0, a simulação virtual de 2019 não teve seus cenários disparados e coordenados pela DIREx de cada empresa participante, ocorrendo de forma isolada. Dessa forma, não houve correlação entre os problemas cibernéticos tratados pela simulação construtiva com as vulnerabilidades de rede tratada pelos especialistas na simulação virtual.

No grupo de estudos, as atividades foram separadas em salas temáticas para cada setor. No setor de Telecomunicações, coordenado pela ANATEL, foram abordados os temas relacionados com desvio de tráfego na Internet (*BGP hijacking*), criação de uma criptografia nacional e guerra cibernética no contexto das corporações.

O EGC 3.0 estava previsto para ser executado em 2020. O planejamento inicial foi preparado, todavia, devido a pandemia de COVID-19, foi cancelado. O EGC 3.0 foi replanejado para o 2021, e ocorreu no período de 5 a 7 de outubro, com a participação 350 integrantes. Além dos setores do EGC 2.0, houve a inclusão de mais dois setores de infraestruturas críticas: Água e Transportes (aviação civil e aquaviários), congregando um total de 75 organizações. Houve, portanto, seis setores de infraestrutura crítica, além da Defesa, envolvidos, em três dias de

exercício. O setor de Telecomunicações foi coordenado pela ANATEL e contou com a participação de 8 (oito) empresas do setor.

Importante destacar, na linha temporal, que em 17 de novembro de 2020 foi aprovada a Portaria nº 3.781/GM-MD que criou o SMDC, tendo como órgão central o ComDCiber, com capacidade interagências, caracterizado pela atuação colaborativa de órgãos e empresas da administração pública ou privada, de infraestruturas críticas, dessa forma alinhado, no nível estratégico, com os objetivos do Guardião Cibernético.

O exercício de 2021 seguiu a mesma mecânica do EGC 2.0, com 76 Problemas Cibernéticos Simulados (PCS) na simulação construtiva, considerando todos os setores. Porém, devido ao crescimento do tamanho do exercício e a quantidade de participantes, o EGC 3.0 foi planejado para ocorrer com dois locais, Brasília e São Paulo. Foi mantida a organização espacial com reunião dos membros da DIREx de todas as empresas/setores em mesmo ambiente, e os gabinetes de crise separados em ambiente por setor. Esse foi o primeiro exercício com acesso remoto de participantes, já com vistas a superar as limitações físicas de um único local para suportar a ampliação de participantes e organizações. Nesse sentido, o setor de Telecomunicações foi deslocado para o Comando da 2ª Divisão de Exército (2ª DE), em São Paulo. Com isso, a DIREx e o gabinete de crise da simulação construtiva do setor trabalharam de forma isolada, com trocas de experiências apenas intrassetor, penalizando um dos principais objetivos do exercício, que é a interação intersetores.

A simulação virtual, por outro lado, incrementou sua execução com adoção do modelo internacional de *Cyber Defense Network*, defendendo uma rede computacional por meio de simulador cibernético (BRASIL, 2021). Além do *blue team* e *red team*, foi acrescentado o *white team*, equipe responsável pela arbitragem do jogo, avaliando a atuação do *blue team* na defesa e análise das vulnerabilidades exploradas pelo *red team*.

No grupo de estudos, as atividades foram direcionadas para elaborar estratégias que contribuíssem para a resiliência cibernética do país a partir de cada setor estratégico. Também foi patrocinado como parte das atividades previas do exercício a realização de palestras de higiene cibernética divulgadas nas empresas/entidades participantes, com o apoio do CERT.br. No setor de Telecomunicações, coordenado pela ANATEL, foram discutidos definição de forma e de procedimentos para a realização de ciclos de avaliação de vulnerabilidades, previstos no Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740/2020.

O EGC 4.0 ocorreu 2022, no período de 16 a 19 de agosto, com a participação 450 integrantes. Foram mantidas as áreas do EGC 3.0, com complementação dos setores de Energia

e Transportes (terrestres) e a inclusão dos Correios no setor de Comunicações, congregando um total de 120 organizações. Houve, também, a expansão na duração do exercício para 4 dias. O setor de Telecomunicações foi coordenado pela ANATEL e contou com a participação de 12 (doze) empresas do setor, além dos Correios.

Esse exercício seguiu a mesma lógica dos exercícios anteriores, com 792 Problemas Cibernéticos Simulados (PCS) na simulação construtiva, considerando todos os setores. Com a expansão do tamanho do exercício, da quantidade de organizações e de participantes, e com a experiência do EGC 3.0, o EGC 4.0 ocorreu com dois locais, Brasília e São Paulo. Diferente do exercício anterior, neste EGC o *hub* remoto de São Paulo foi multisetorial. Assim, tanto em Brasília como em São Paulo, havia representantes da simulação construtiva (DIREx e gabinete de crise) de todos os setores das infraestruturas críticas, permitindo, assim, o compartilhamento de aprendizados e experiências. Foi mantida a mesma organização espacial da DIREx e dos gabinetes de crise. Nesse ano, houve expansão do alcance dos PCS, com integração para o Governo e os órgãos parceiros. Com o aumento da quantidade de setores e diversidade de participantes foi possível maior interação dos times das empresas do setor.

Na simulação virtual, não houve novas alterações no formato do exercício. Com um dia a mais de duração do exercício, foi possível incrementar o volume de atividades.

No grupo de estudos, as atividades foram direcionadas a realização de palestras de higiene cibernética dentro das empresas/entidades participantes, na fase preparatória do exercício, com o apoio de material do CERT.br. No setor de Telecomunicações, a ANATEL discutiu e apresentou a aprovação do Plano Setorial de Gestão de Incidentes Cibernéticos.

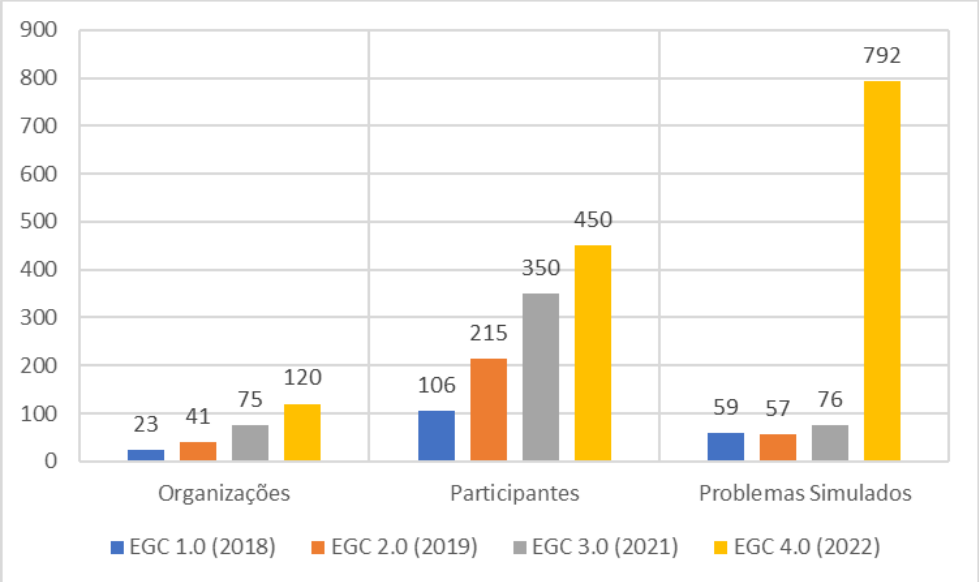
Em todos os EGC foi utilizado um portal de notícias para dar mais realidade do cenário de fundo da operação meridiano. Todavia, as notícias publicadas dos eventos ocorridos no cenário de fundo não guardaram correlação com os PCS executados nas fases de normalidade, agravamento da crise, pico da crise e retorno à normalidade. Isso ocorreu pois os PCS foram elaborados pelos participantes, coordenados pelos pontos focais (normalmente a agência reguladora do setor), mas sem a preocupação com a linha de tempo de execução do exercício (da normalidade ao pico da crise), e sem qualquer correlação com o cenário da operação meridiano ou com as notícias apresentadas, pois esses não eram conhecidos previamente, na fase de preparação do exercício, pelos participantes. A consequência disso é que, como tanto a DIREx como o gabinete de crise não possuem especialistas para tratar tecnicamente os eventos, mas membros do nível estratégico-decisório, há uma dificuldade de propor um tratamento para a causa raiz e avaliação do impacto/gravidade de cada PCS, cabendo ao gabinete de crise uma dose de criatividade para imaginar uma resposta para esses itens. A maior preocupação das

empresas/entidades na elaboração dos PCS, em atividade prévia à execução simulação construtiva, é trazer para o exercício os mais recentes e recorrentes tipos de ataques conhecidos, que afetam e são de interesse de determinado setor, e não, necessariamente, problemas contextualizados ao cenário fictício da operação.

Observe-se aqui, que embora o período de avaliação dos EGC tenha sido de 2018 a 2022 (5 anos), somente quatro exercícios foram realizados, tendo em vista que no ano de 2020 não foi possível realizar o EGC3.0, que foi adiado para o ano seguinte devido a pandemia de COVID-19.

O Gráfico 1 apresenta, portanto, a evolução quantitativa dos exercícios do Guardião Cibernético ao longo dos anos, destacando o aumento significativo no número de organizações (de 23 para 120), de participantes (de 106 para 450) e de problemas simulados (de 59 para 792), de 2018 a 2022.

Gráfico 1 - Evolução quantitativa do EGC



Fonte: Elaborado pelo autor (2023).

O quadro 2 apresenta, de forma sintética, a evolução quantitativa de setores das infraestruturas críticas previstas na Plansic, ano-a-ano, bem como as evoluções implementadas no EGC de um ano para o outro, para o incremento do volume de participantes, de cenários simulados, de adequação da infraestrutura e melhoria do próprio exercício.

Quadro 2 - Evolução da inclusão dos setores das IC a cada edição do EGC

	EGC 1.0 (2018)	EGC 2.0 (2019)	EGC 3.0 (2021) [5]	EGC 4.0 (2022)
Quantidade de Organizações - Setores envolvidos	3 - Nuclear 7 - Financeiro 4 - Defesa 8 - Órgãos Parceiros ComDCiber	7 - Nuclear, 10 - Financeiro, 6 - Telecomunicações 4 - Elétrico 4 - Defesa 8 - Órgãos Parceiros ComDCiber Grupo de Observadores	5 - Nuclear 8 - Financeiro 9 - Telecomunicações 8 - Elétrico 2 - Água 10 - Transporte (ANAC/ANTAQ) 4 - Defesa 11 - Órgãos Parceiros ComDCiber 3 - Academia 3 - Organizações Internacionais	7 - Nuclear 8 - Financeiro 14 - Comunicações 12 - Elétrico 5 - Água 21 - Transporte (ANAC/ANTAQ) 4 - Defesa 14 - Órgãos Parceiros ComDCiber 12 - Academia 3 - Org Internacionais 7 – HUB São Paulo
Ações Evolutivas Implementadas	- Plano de Ação para Estruturas Estratégicas do Setor Cibernético	- Inclusão dos Setores Telecom e Elétrico - Problemas Cibernéticos Simulados (PCS) integrados intersetores - 1º Workshop sobre Gestão de Risco Cibernético pelo NIST[6] - Apresentação da Plataforma MISP – *Malware Information Sharing Platform*.	- Inclusão dos Setores Água e Transporte (ANAC e ANTAQ) - Chamamento Público para apoio a estruturação do evento - HUB Remoto SP (Telecomunicações)	- Setor Energia completo (ANEEL/ONS e ANP) - Setor Transporte completo, incluído ANTT - Integração dos PCS com Governo e Órgãos parceiros - Setor Comunicações incluído os Correios - Setor Financeiro só planejamento - HUB SP (Simulação Construtiva)
Duração do exercício (sem APA)	2,5 dias	2 dias	2 dias	3 dias

Fonte: Elaborado pelo autor (2023). Adaptado de ComDCiber – apresentação da 2ª RPA para o EGC 5.0, em 25/07/2023.

3.2 EVOLUÇÃO QUALITATIVA DO GUARDIÃO CIBERNÉTICO

Do levantamento dos registros das APA, de cada um dos anos do exercício, foi possível recuperar alguns resultados qualitativos dos resultados de cada EGC, conforme (quadro 3):

[5] Devido a pandemia de COVID-19 o EGC 3.0 em 2020, embora tenha sido planejado, foi cancelado.
[6] Apresentado o *Cybersecurity Framework* por especialistas norte-americanos do *National Institute of Standards and Tecnology* (NIST)(2018).

Quadro 3: Compilados das análise pós-ação

	Resultados Análise Pós-Ação - APA[7]
2018	• O Alcance do objetivo inicial, de integração da defesa, do governo, do setor privado e da comunidade acadêmica na busca de iniciar a construção de estratégias de defesa mais robustas; • Individualmente, os participantes identificaram oportunidades de melhoria em suas respectivas estruturas de proteção cibernética; • Não houve interação entre setores.
2019	• Aprendizado da necessidade de interação entre empresas e com órgãos parceiros, bem como a troca de informações sobre ataques e reação; • Atuação colaborativa e integrada de especialistas nas áreas de IT, Com Social, Jurídica e Alta Adm. das empresas/organizações – melhoria do processo intraempresa; • Validação do PNTIR.
2021	• Integração com órgãos parceiros ao EGC, porém com interação incipiente; • Palestras de higiene cibernética nas entidades/empresas; • Isolamento do Setor de Telecomunicações em São Paulo, sem outros setores, prejudicou o acompanhamento do exercício e a interação intersetor; • Palestras de higiene cibernética nas entidades/empresas, provocadas pelo EGC como atividade prévia.
2022	• Gabinete de Crise – momentos de interação entre todos os times das prestadoras do setor, Correios e Anatel, aumentando a interação intrassetores; • Compartilhamento de percepções durante o exercício, entre todos os setores, na DIREx, evidenciando a dificuldade de entendimento para acionamento de órgãos parceiros; • Proximidade física com outros setores na DIREx; • Oportunidade de melhoria para a comunicação intrasetorial e intersetorial; • Diversidade dos setores e quantidade de participantes; • Houve melhor interação com órgãos parceiros. • Palestras de higiene cibernética nas entidades/empresas, provocadas pelo EGC como atividade prévia.

Fonte: Elaborado pelo autor (2023).

3.3 RESULTADOS NO SETOR DE TELECOMUNICAÇÕES

O setor de telecomunicações tem aproveitado os EGC para produzir estudos e propostas de normatização para evolução da segurança e resiliência do setor. Várias ações têm sido capitaneadas pela ANATEL junto aos grupos de estudo do EGC, seja para discussões, consultas e até mesmo validações de documento e normativos, que tem redundado posteriormente em novos regulamentos normativos.

[7] Devido a pandemia de COVID-19 o EGC 3.0 previsto ocorrer em 2020, embora tenha sido planejado, foi cancelado. A sua execução se deu no ano de 2021.

Nessa seara temos a Resolução nº 740 , de 21 de dezembro de 2020, que aprovou (na forma de seu anexo) o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), cujo objetivo é estabelecer condutas e procedimentos para a promoção da segurança nas redes e serviços de telecomunicações, incluindo a Segurança Cibernética e a proteção das Infraestruturas Críticas de Telecomunicações (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2020); o Ato nº 77, de 05 de janeiro de 2021, que estabeleceu Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações, documento que traz recomendações aos fabricantes e fornecedores visando minimizar ou corrigir vulnerabilidades por meio de atualizações de *software/firmware* ou por meio de recomendações em configurações e também estabeleceu um Programa de Supervisão de Mercado; e mais recentemente, apresentado e assinado, durante a Análise Pós-Ação do EGC 4.0, em 19.08.2022, o Plano Setorial de Gestão de Incidentes Cibernéticos – Versão 1.0.

Um dos resultados consequência do amadurecimento do Brasil em segurança cibernética pode ser verificada na publicação do Indice Global de Segurança Cibernética (do original em inglês *Global Cybersecurity Index* – GCI) da União Internacional de Telecomunicações (UIT).

A UIT, uma agência da Organização das Nações Unidas (ONU), especializada em tecnologia da informação e comunicações, publica periodicamente o relatório do Indice Global de Cibersegurança que avalia o compromisso dos 193 Estados-Membros da UIT com relação à segurança cibernética. O índice mede o comprometimento dos países com a segurança cibernética em cinco pilares: medidas legais (legislação e regulamentação), medidas técnicas (equipes, mecanismos e recursos técnicos), medidas organizacionais (instituições, políticas e estratégia de segurança cibernética a nível nacional), medidas de capacitação (promoção de programas de educação, formação, desenvolvimento e certificação), e medidas de cooperação (parcerias e acordos internacionais, parcerias público-privada, intra-agências e interagências e redes de informação). Dessa forma, o objetivo do GCI seria o de ajudar e incentivar os países a identificar áreas de melhorias relacionadas à segurança cibernética, indicando aquelas medidas que teriam oportunidades de melhorias para ajudar a aumentar a resiliência cibernética.

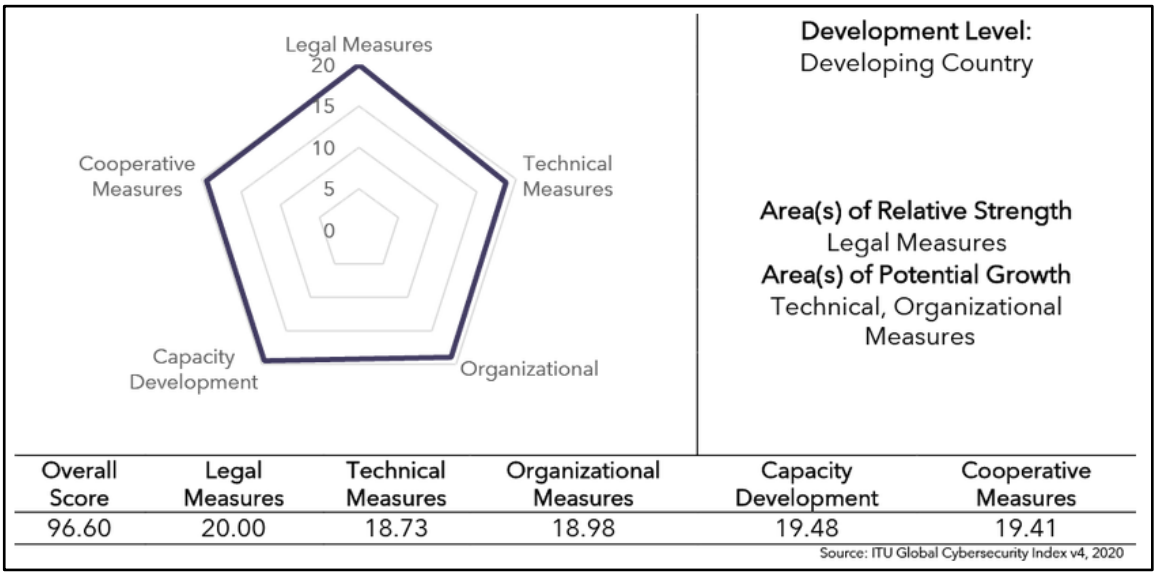
Na avaliação de 2018 do GCI[8], o Brasil figurava na 70ª posição no ranking mundial e em 6ª posição nas América. A avaliação seguinte do GCI[9], publicada em 2021, o Brasil saltou para a 18ª posição no ranking mundial e para 3º nas Américas. Esta evolução está fortemente

[8] *Global Cybersecurity Index* (GCI) 2018 – Relatório produzido pela União Internacional de Telecomunicações – UIT https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[9] *Global Cybersecurity Index* (GCI) 2020 – Relatório produzido pela União Internacional de Telecomunicações – UIT, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

relacionada com a melhoria do ambiente legal, regulatório e normativo, desenvolvimento de capacidades e medidas de cooperação.

Do resultado publicado em 2021, figura 3, segundo o CGI, as áreas com maior potencial de crescimento, com reflexo direto para a melhoria da segurança cibernética brasileira, estão relacionadas às medidas técnicas e organizacionais, importantes pontos de influência do EGC.

Figura 3 - Perfil do Brasil avaliado pelo Índice Global de Segurança Cibernética - UIT - 2020



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.60	20.00	18.73	18.98	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2020

Fonte: ITU Global Cybersecurity Index v4, 2020.

4 DISCUSSÃO DOS RESULTADOS

Conforme apresentado nesse estudo, o Brasil possui uma série de normativos específicos, que fornecem diretrizes detalhadas para a proteção das infraestruturas críticas no espaço cibernético. Esses instrumentos destacam a importância da colaboração entre o setor de defesa, a comunidade acadêmica, os setores público e privado, promovendo um ambiente de cooperação que é fundamental para enfrentar ameaças cibernéticas em constante evolução. A aprovação do Plano Nacional de Segurança de Infraestruturas Críticas (Plansic) em 2022 é um passo significativo, pois estabelece metodologias para identificar as infraestruturas críticas e define responsabilidades claras para a segurança dessas infraestruturas, fortalecendo ainda mais a base normativa para a segurança cibernética das infraestruturas críticas.

O exercício Guardião Cibernético teve quatro edições entre 2018 e 2022, com o objetivo de engajar os participantes para atuar de forma colaborativa, em ambiente interagências, na proteção de ataques no espaço cibernético, realizar o exercício do processo decisório em

diferentes níveis, verificar a efetividade de procedimentos para a solução de incidentes em infraestruturas críticas , bem como propor contribuição doutrinária.

Observa-se, dos dados levantados, que o EGC apresentou progresso quantitativo, porém, quanto ao objetivo de integração e interação intrassetorial e intersetorial, para reforço da resiliência cibernética das infraestruturas críticas, que ocorre de forma crescente durante cada EGC, o resultado ainda é superficial pós-exercício. Conforme apresentado por Nonato e Pinho (2021), em seu trabalho sobre a integração do SMDC com a proteção das infraestruturas críticas, apesar da integração entre setores existir durante o EGC, "a integração no nível de pronta-resposta a incidentes cibernéticos é ainda incipiente entre os próprios órgãos das infraestruturas críticas, dificultando a sinergia para uma proteção mais eficiente". **Uma melhoria para buscar superar essa lacuna seria a elaboração de PCS com impactos intersetoriais, com a mesma evolução da crise, o que provocaria, per se, a interação dos setores.**

De forma complementar, os gabinetes de crise também poderiam ser agrupados em mesmo ambiente, contanto com pelo menos um gabinete de setor no mesmo espaço, provocando uma relação interagências, capacidade característica da atuação colaborativa. Dessa maneira, uma rede de inter-relacionamento poderia ser melhor criada, para perdurar pós-ação.

Ainda sobre os PCS e o objetivo de verificar a eficácia dos procedimentos, não há, no modelo do EGC um juiz ou mediador que avalie as respostas dadas pelo gabinete de crise para verificar se são pertinentes e atendem à solução do problema simulado. Nesse sentido seria interessante que houvesse uma espécie de gabarito com itens mínimos que deveriam conter na resposta, que resolvem o problema, além daqueles que são procedimentos internos de cada entidade.

Quanto ao realismo do exercício, dada todas as ferramentas disponibilizadas pelo ComDCiber, verificou-se que **falta um sincronismo entre o cenário de fundo da operação, as notícias publicadas da simulação construtiva, bem como das situações simuladas no SIMOC com os PCS executados nas fases de normalidade, agravamento da crise , pico da crise e retorno à normalidade. Uma forma de superar esse ponto seria utilizar a fase preparatória, em reuniões entre os pontos focais de cada setor, sob orientação do ComDCiber, para montar, em conjunto, a linha de tempo de execução do exercício (da normalidade ao pico da crise), as notícias veiculadas e os PCS, de forma a haver uma maior correlação entre esses elementos.** Assim, a evolução da crise no cenário proposto traria maior realidade para a análise de cada PCS apresentados na linha do tempo, com avaliação dos

setores, por impacto e gravidade. Dessa forma, haveria maiores insumos para o gabinete de crise, ao receber um PCS para analisar, realizar as correlações de impactos e gravidade, com insumos das notícias veiculadas, exigindo menor dose de criatividade para responder o impacto e gravidade dos PCS nas entidades/empresas participantes; e, dessa forma, então, colher respostas mais enriquecidas para um dos objetivos do exercício, que é a de reação frente aos tipos de cenários apresentados.

Do levantamento realizado, pode-se afirmar que o EGC tem como forças a integração entre governo, setor privado e meio acadêmico, característica fundamental para lidar com ameaças cibernéticas complexas que afetam múltiplos setores. Outro impacto positivo é a expansão significativa de participantes envolvidos, que contribui para a representatividade do exercício e reflete a crescente conscientização sobre a importância da segurança. Importa destacar, também, que as lições aprendidas compiladas na Análise Pós-Ação (APA) permitem a identificação de lições podem ser aplicadas para fortalecer a postura cibernética das organizações envolvidas e do próprio exercício. Ainda, a aplicação de boas práticas cibernéticas, o emprego de ferramentas de compartilhamento de informações e a simulação de práticas de proteção de incidentes.

Algumas limitações podem ser levantadas como pontos de atenção. Como o EGC já é um exercício em grande escala, limitações de recursos (tempo, pessoal e infraestrutura) podem representar um desafio para a expansão contínua dos exercícios. Assim, o crescimento do EGC, com a inclusão de novos setores e organizações, deve ser gerenciado de forma sustentável, para que mantenha sua eficácia. Finalmente, identificar áreas de melhoria durante a Análise Pós-Ação (APA) é uma coisa, mas implementar efetivamente essas melhorias em organizações do setor público e privado é outra. A implementação eficaz das lições aprendidas pode ser uma fraqueza se não for adequadamente abordada.

5 CONSIDERAÇÕES FINAIS

A segurança cibernética é um tema cada vez mais relevante na atualidade, especialmente em relação à proteção de infraestruturas críticas e à defesa nacional. O Brasil tem adotado diversas políticas e estratégias para garantir a segurança cibernética do país, como a PND, a END, a PNSI, a PNSIC, a E-Ciber, o Plansic, bem como os exercícios de treinamento, com simulação construtiva e virtual.

A atuação conjunta dessas políticas e estratégias, através do Sistema Militar de Defesa Cibernética, é fundamental para garantir a segurança cibernética do país, protegendo as

infraestruturas críticas e minimizando os impactos de eventuais incidentes cibernéticos, patrocinando, assim, a evolução da resiliência cibernética brasileira.

Do Exercício Guardião Cibernético verifica-se que evoluiu ao longo das suas quatro edições, implementando aprendizados em um processo de melhoria contínua e expansão. Os dados levantados mostram que os resultados têm sido atingidos em diferentes graus de maturidade, mas mantendo a evolução constante como característica na busca do alcance pleno de seus objetivos, que irão produzir, como consequência, o aumento da resiliência cibernética.

Em resumo, a análise revela que o Brasil está adotando uma abordagem abrangente e estratégica para a segurança cibernética das infraestruturas críticas. Os normativos existentes e em desenvolvimento, juntamente com a ênfase na colaboração e no treinamento, refletem um compromisso em proteger o país contra ameaças cibernéticas e garantir a resiliência das infraestruturas críticas.

Por último, sugere-se como trabalho futuro, estudar *frameworks* de avaliação dos resultados de exercícios de simulação *tabletop*, ou investigar a implementação das lições aprendidas nas entidades participantes, por meio de estudo de caso.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). **Brasil é o terceiro país das américas em segurança cibernética**. Brasília, DF: ANATEL, 2021. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/brasil-e-o-terceiro-pais-das-americas-em-seguranca-cibernetica. Acesso em: 25 maio 2023.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). **Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações**. Brasília, DF: ANATEL, 2020. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/brasil-e-o-terceiro-pais-das-americas-em-seguranca-cibernetica. Acesso em: 25 maio 2023.

ARAUJO, José Euclides Oliveira de. **A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil**. Brasília, DF: Escola Superior de Guerra, 2020. Disponível em: https://repositorio.esg.br/handle/123456789/1258. Acesso em: 4 ago. 2023.

BANDEIRA, Frederico. **Guardião Cibernético I e II.** Fórum Infraestruturas do Mercado Financeiro, 2018. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/Documents/sistema_pagamentos_brasileiro/Forum_SPB/Exercicio_Guardiao_Cibernetico.pdf. Acesso em: 4 ago. 2023.

BRASIL. **Decreto n. 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética - E-Ciber e Anexo. Brasília, DF: Presidência da República, 2020a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 17 jun. 2023.

BRASIL. **Decreto n. 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas e Anexo. Brasília, DF: Presidência da República, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 7 jun. 2023.

BRASIL. **Decreto n. 11.200, de 15 de setembro de 2022**. Aprova a Plano Nacional de Segurança de Infraestruturas Críticas – Plansic e Anexo. Brasília, DF: Presidência da República, 2022b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm. Acesso em: 24 jun. 2023.

BRASIL. **Decreto n. 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança da Informação. Brasília, DF: Presidência da República, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm. Acesso em: 17 jun. 2023.

BRASIL. **Decreto n. 9.637, de 26 de dezembro de 2018**. Aprova a Política Nacional de Segurança das Infraestruturas Críticas. Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 17 jun. 2023.

BRASIL. **Decreto Presidencial 14.503 de 15 de dezembro de 2017**. Aprova a Estratégia Nacional de Inteligência. Brasília, DF: Presidência da República, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Dsn/Dsn14503.htm. Acesso em: 17 jun. 2023.

BRASIL. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. 1. ed. 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 5 jun. 2023.

BRASIL. Exército. Comando de Defesa Cibernética. **Planejamento do Exercício Guardião Cibernético 3.0**. Brasília: COMDCIBER, 2021. Documento interno.

BRASIL. Exército. Comando de Defesa Cibernética. **Concepção do Exercício Guardião Cibernético 4.0 -** Atualizado em 08 de abril de 2022. Brasília, DF: COMDCIBER, 2022a. Documento interno.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas. Ministério da Defesa. Estado-Maior Conjunto Das Forças Armadas (MD35-G-01)**. 5. ed. 2015. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf/view. Acesso em: 5 jun. 2023.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2012.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2016.

BRASIL. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa. 2020c.

BRASIL. **Portaria Normativa n. 3781, de 17 de novembro de 2020**. Cria o Sistema Militar de Defesa Cibernética e dá outras providencias. Brasília, DF: Ministério da Defesa, 2020d. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 5 jun. 2023.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. **Desafios estratégicos para segurança e Defesa Cibernética**. Brasília, DF: Secretaria de Assuntos Estratégicos, 2011. 220 p. Disponível em: http://livroaberto.ibict.br/handle/1/612. Acesso em: 5 jun. 2023.

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: 24 jul. 2023.

CHOWDHURY, Nabin; GKIOULOS, Vasileios. **Cyber security training for critical infrastructure protection: A literature review**. Computer Science Review, v. 40, p. 100361, 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S1574013721000010. Acesso em: 24 jul. 2023.

CISA, Cybersecurity and Infrastructure Security Agency, EUA. **Critical Infrastructure Sectors**. Disponível em: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. Acesso em: 25 maio 2023.

COSTA, Álvaro Lobo; FERREIRA, André Luiz Alves; CABRAL, Victor José Queiroz. **A criação de uma agência brasileira de segurança cibernética como estratégia de defesa nacional**. 2022. Disponível em: https://repositorio.esg.br/handle/123456789/1650. Acesso em: 25 maio 2023.

MAGLARAS, Leandros; JANICKE, Helge; FERRAG, Mohamed Amine. **Cybersecurity of Critical Infrastructures: Challenges and Solutions. Sensors**, v. 22, n. 14, p. 5105, 7 Jul 2022. Disponível em: https://www.mdpi.com/1424-8220/22/14/5105. Acesso em: 25 maio 2023.

MARINHO, Rafael Costa et al. **A defesa cibernética na proteção da propriedade intelectual dos produtos e sistemas de defesa do exército brasileiro**. 2022. Brazilian Journal of Development, v. 8, n. 1, p. 35-53, 2022. Disponível em: https://www.enabed2021.abedef.org/resources/anais/15/enabed2020/1626489457_ARQUIVO_3e9af3ea02082378f0af6138260ab3f4.pdf. Acesso em: 25 maio 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica**, versão 1.1, U.S. Chamber of Commerce – 2018.

NONATO, Marcos Paulo Cardoso; PINHO, Harley de. **A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional**. 2021. Disponível em: https://repositorio.esg.br/handle/123456789/1426. Acesso em: 25 maio 2023.

SEGUNDO, Célio Borges Taquary. **A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos**. Curso de Altos Estudos em Defesa (CAED).

2019. Disponível em: https://repositorio.esg.br/handle/123456789/1205. Acesso em: 25 maio 2023.

SILVA, Walbery Nogueira de Lima e. **Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional**. Data & Hertz, v. 1, n. 1 jan./dez, p. 52-59, 2020. Disponível em: http://www.ebrevistas.eb.mil.br/datahertz/article/view/6796. Acesso em: 25 maio 2023.