MARCOS PAULO CARDOSO NONATO

HARLEY DE PINHO

A INTEGRAÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA (SMDC) COM A PROTEÇÃO CIBERNÉTICA DAS INFRAESTRUTURAS CRÍTICAS DE INTERESSE PARA DEFESA NACIONAL.

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

Orientador: Maj QCO R1 Carlos Maurício de Borges Mello

Brasília

2021

Marcos Paulo Cardoso Nonato
Idt 011103234-8 /MD-EB

Harley de Pinho
Idt 118141253-5 /MD-EB

MARCOS PAULO CARDOSO NONATO
HARLEY DE PINHO

A INTEGRAÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA (SMDC) COM A PROTEÇÃO CIBERNÉTICA DAS INFRAESTRUTURAS CRÍTICAS DE INTERESSE PARA DEFESA NACIONAL

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, 18 de OUTUBRO de 2021

CARLOS MAURÍCIO DE BORGES MELLO - Maj R1 EB (ESD)
Orientador

CLÁUDIO ALFREDO CUNHA DORNELLES - Cel R1 EB (ESD)
Membro 1

ALCIMAR SANCHES RANGEL – Prof. MSc. (ITI)
Membro 2

A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das Infraestruturas Críticas de interesse para Defesa Nacional.

Marcos Paulo Cardoso Nonato[1a]
Harley de Pinho[2a]

RESUMO

Este trabalho tem por finalidade chamar a atenção da importância da integração do SMDC com a proteção cibernética das infraestruturas de interesse da Defesa Cibernética. O aumento de ataques cibernéticos em estruturas estratégicas pelo mundo e a crescente necessidade de ações coordenadas com a finalidade de mitigar os seus efeitos, associado à deficiência de recursos humanos especializados no setor cibernético, serviram de motivação para o referido artigo. O estudo de estruturas nacionais de Segurança Cibernética pelo mundo como as existentes no Reino Unido e nos Estados Unidos lançou luz sobre a necessidade de propor ações que possam, em nível nacional, apresentar soluções de integração entre os entes responsáveis pela Defesa e Segurança Cibernética no Brasil. Este artigo está dividido em seis partes, incluindo uma conclusão e trazendo as considerações iniciais sobre a temática na introdução. Inicialmente, discorre-se sobre a interação do espaço cibernético e o SMDC. A terceira seção apresenta a segurança das infraestruturas baseada nas legislações vigentes. A quarta apresenta as iniciativas internas e experiências externas de integração do setor cibernético. A quinta propõe possíveis soluções para a integração e coordenação dentro do ecossistema cibernético brasileiro. E a conclusão, mostrando a importância da implementação de uma estrutura nacional para a Segurança Cibernética e as ações de proteção das infraestruturas de interesse da Defesa.
Palavras-chave: Segurança Cibernética. Defesa Cibernética. Infraestruturas Críticas.

The integration of the Military Cyber Defense System (MCDS) with the cyber protection of Critical Infrastructures of interest to National Defense.

ABSTRACT

The purpose of this paper is to draw attention to the importance of integrating the MCDS with cyber protection of infrastructure of interest to Cyber Defense. The increase of cyber attacks on strategic structures around the world and the growing need for coordinated actions in order to mitigate their effects, associated with the deficiency of specialized human resources in the cyber sector, served as motivation for this article. The study of national Cyber Security structures around the world, such as those in the United Kingdom and the United States, has shed light on the need to propose actions that can, at the national level, provide solutions for integration between the entities responsible for Defense and Cyber Security in Brazil. This article is divided into six parts, including a conclusion and bringing the initial considerations about the theme in the introduction. Initially, the interaction of cyberspace and the MCDS is discussed. The third section presents the security of the infrastructures based on the current legislations. The fourth presents internal initiatives and external experiences of cyber sector integration. The fifth proposes possible solutions for integration and coordination within the Brazilian cyber ecosystem. And the conclusion, showing the importance of implementing of a national structure for Cybersecurity and the actions of protecting the infrastructures of Defens´s interest.
Keywords: Cyber Security. Cyber Defense. Critical Infrastructures.

---

[1] Coronel da Arma de Comunicações do Exército Brasileiro. Mestre em Operações Militares.
[2] Coronel da Arma de Comunicações do Exército Brasileiro. Mestre em Operações Militares.
[a] Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Defesa (ESD), 2021.

1 INTRODUÇÃO

Em um mundo digital amplamente conectado, as ameaças cibernéticas se tornaram cada vez mais reais. Os ataques cibernéticos não respeitam fronteiras e, na maioria das vezes, não revelam seus autores. Dessa maneira, o estudo aprofundado de assuntos afetos às ações no espaço cibernético se torna de relevância reconhecida para a Defesa Nacional.

A Política Nacional de Defesa (PND) estabelece os objetivos para o preparo e o emprego de todas as expressões do Poder Nacional em prol da Defesa Nacional. A complexidade do tema demanda que se articulem ações do Ministério da Defesa com as de outros órgãos do Estado e da sociedade brasileira. Neste marco normativo foram analisados os ambientes nacional e internacional, orientando para a atenção que deve ser dada à segurança e à defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional. Ressalta, ainda, que a exploração e o ataque a esses sistemas poderão comprometer diversas atividades vitais para o funcionamento das instituições do País, como as desempenhadas pelas infraestruturas críticas (BRASIL, 2016a).

A Estratégia Nacional de Defesa (END), por sua vez, orienta os segmentos do Estado por meio de estratégias e ações estratégicas de defesa, com o intuito de atingir os objetivos nacionais de defesa, especificados na PND. Neste documento também são elencadas as capacidades nacionais de defesa, implementadas por intermédio da participação coordenada e sinérgica de órgãos governamentais e, se for o caso, de entes privados. Destacam-se, dentre essas capacidades, as de Proteção, Pronta-resposta, Dissuasão, Coordenação e Controle e Gestão da Informação, nas quais se enfatiza a necessidade de se desenvolver atributos de proteção e resiliência no ambiente cibernético (BRASIL, 2016b).

Nesse contexto, é fundamental elencar possíveis alvos compensadores para ataques cibernéticos. Vários exemplos de ações cibernéticas bem-sucedidas ao longo da história recente têm como alvo um mesmo setor dos países que foram vítimas: as infraestruturas críticas.

A Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) define como infraestruturas críticas as instalações, os serviços, os bens e os sistemas, cuja interrupção ou destruição, total ou parcial, provoque impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade. Dessa forma, é necessário um conjunto de medidas, de caráter preventivo e reativo, para preservar ou restabelecer a prestação dos serviços essenciais prestados por essas infraestruturas (BRASIL, 2018a).

As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas estruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.

A proteção cibernética a ser provida a essas estruturas possui características semelhantes às aplicadas aos demais setores, sendo uma atividade de caráter permanente e que tem por objetivo neutralizar ataques e exploração cibernética aos dispositivos computacionais nos níveis de decisão político, estratégico e tático. A cada um desses níveis será atribuído determinado tipo de ação a saber: segurança, defesa e guerra cibernética, respectivamente (BRASIL, 2014).

Nesse diapasão, foi conferido ao Ministério da Defesa a responsabilidade por esta proteção nos níveis estratégico e tático, ou seja, Defesa Cibernética e Guerra Cibernética. Para garantir o cumprimento dessa missão foi criado o Sistema Militar de Defesa Cibernética (SMDC), instituído em construções adequadas, disposto de tecnologias avançadas, de recursos humanos qualificados, de doutrinas e procedimentos bem definidos.

A Segurança Cibernética, ou seja, sob a égide do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Porém, a Política Nacional de Segurança da Informação (PNSI) estabelece que compete ao Ministério da Defesa apoiar este Gabinete nas atividades relacionadas à Segurança Cibernética, e elaborar as diretrizes, os dispositivos e os procedimentos de defesa que atuem nos sistemas relacionados à Defesa Nacional contra-ataques cibernéticos (BRASIL, 2018b).

Assim, este tema, que trata sobre a integração do SMDC com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional, encontrou lastro, tanto nas necessidades impostas por diversos documentos normativos, como nos recentes acontecimentos veiculados em livros, revistas especializadas e na mídia em geral, tendo como objetivo a análise desta integração, tão importante para proteção dos ativos cibernéticos.

Este trabalho busca revelar as iniciativas de integração já existentes, apresentando os aspectos positivos e suas oportunidades de melhoria. Ao mesmo tempo, busca apresentar as lacunas que ainda existem entre os atores nos níveis decisórios do País e os responsáveis pela proteção das infraestruturas, chegando, por fim, a uma proposta de estrutura nacional que possa preencher os hiatos do problema levantado, se existirem.

O trabalho foi realizado por meio de abordagem qualitativa, com foco no aprofundamento e compreensão dos atos normativos que balizam a Segurança Cibernética e a Defesa Cibernética, bem como da segurança das infraestruturas críticas. Esse estudo se alongará até o cabedal doutrinário e bibliográfico nessas áreas.

No que tange às técnicas e instrumentos, o trabalho em questão foi alicerçado em pesquisa bibliográfica e análise documental, possibilitando a realização do diagnóstico e análise da capacidade de atuação do SMDC e dos sistemas que realizam a proteção das infraestruturas críticas.

A pesquisa bibliográfica permitiu compreender os conceitos que abrangem o estudo, bem como o aprofundamento de ideias consideradas como referências sobre a temática de proteção cibernética.

2 **A INTERAÇÃO DO ESPAÇO CIBERNÉTICO E O SISTEMA MILITAR DE DEFESA CIBERNÉTICA**

Para estudar a interação entre o espaço cibernético e o SMDC é necessário, inicialmente, explorar os conceitos e as características desses dois ambientes. Dessa forma, a apresentação desses entes facilitará a compreensão de como eles interagem e como o SMDC tem se inserido na exploração do espaço cibernético.

2.1 O ESPAÇO CIBERNÉTICO

O espaço cibernético é, por natureza, desprovido de fronteiras tangíveis, sendo que nele tanto o setor público como o privado, civis e militares, atores nacionais e internacionais, interagem de forma simultânea, interdependente e interligada. Por essas razões, não é um ambiente seguro e protegido, sendo vulnerável a ataques que podem ter como consequências perdas relevantes de ordem econômica e social ou ameaças à Defesa Nacional, quer no plano da degradação ou destruição de estruturas estratégicas, quer no plano da negação do acesso a recursos informacionais (BRASIL, 2014).

2.2 O SISTEMA MILITAR DE DEFESA CIBERNÉTICA

Diante deste novo domínio, o SMDC foi criado em cumprimento à Política Cibernética de Defesa, aprovada pela Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012, com a

finalidade de assegurar, de forma conjunta, o uso efetivo do espaço cibernético pelas Forças Armadas.

O SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal, essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses (BRASIL, 2020a).

O órgão central do SMDC é o Comando de Defesa Cibernética (ComDCiber), Comando Operacional Conjunto, permanentemente ativado e com capacidade interagências, pertencente à estrutura regimental do Exército Brasileiro. Tem como missão, respeitadas as competências das Forças Singulares e dos Comandos Operacionais ativados: planejar; orientar; coordenar; integrar; e executar atividades relacionadas ao desenvolvimento e à aplicação das capacidades cibernéticas (BRASIL, 2020a).

A Figura 1 apresenta a estrutura conjunta do ComDCiber e a qual Força está atribuído o comando ou a chefia.

Figura 1 - Estrutura do ComDCiber

Fonte: Adaptado de ComDCiber (2021)

Para cumprir sua missão, o ComDCiber é assim constituído:

a) Centro de Ações Cibernéticas (CAC) que tem como missão executar as atividades de Defesa e Guerra Cibernética, observando as técnicas, táticas e procedimentos específicos da atividade;

b) Centro de Gestão Estratégica (CGE) que tem como missão coordenar os processos afetos ao planejamento, gestão estratégica, relações institucionais, gestão do conhecimento e de talentos no âmbito do ComDCiber;

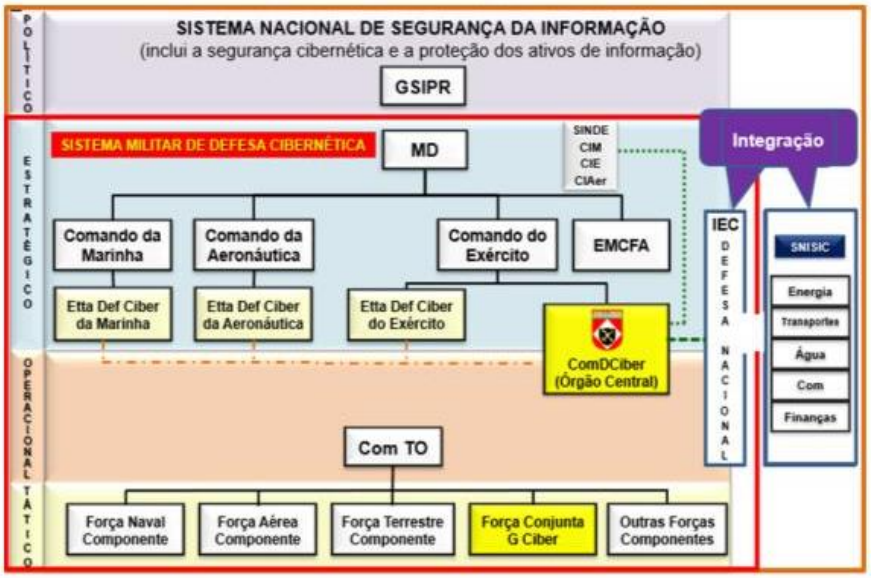
c) Centro de Coordenação de Operações Cibernéticas (CCOC) que tem como missão aplicar as capacidades cibernéticas, no âmbito do SMDC, realizando o planejamento das operações conjuntas, combinadas e interagências, a fim de contribuir para o uso efetivo do espaço cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional; e

d) Escola Nacional de Defesa Cibernética (ENaDCiber) que tem como missão capacitar recursos humanos para trabalhar no setor cibernético da Defesa Nacional (BRASIL, 2020b). As atribuições desta escola serão descritas na Seção 4.

A capacidade interagências do órgão central do SMDC caracteriza-se 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, 2020b).

A Figura 2 destaca a constituição do SMDC, bem como apresenta a necessidade de integração com o Sistema Nacional de Segurança de Infraestruturas Críticas (SNSIC). A proteção cibernética das Infraestruturas Críticas, de interesse da Defesa Nacional, é uma ação que interessa ao Estado Brasileiro e por isso precisa ser planejada e coordenada pelo Sistema Nacional de Segurança da Informação (SNSI), por meio de uma estrutura no nível político.

Figura 2 – Integração do Sistema Militar de Defesa Cibernética (SMDC) e o Sistema Nacional de Segurança de Infraestruturas Críticas (SNSIC)



Fonte: Adaptado de ComDCiber (2021)

Para que o SMDC seja capaz de cumprir sua finalidade, os órgãos que o compõem devem dispor de capacidades de Defesa Cibernética, ou seja, devem ser capazes de realizar, com efetividade, dentro dos limites de suas competências, todo o espectro de atividades cibernéticas.

A Figura 3 mostra os níveis de decisão e atores no Espaço Cibernético. O SMDC permeia de forma sinérgica os níveis Estratégico, Operacional e Tático.

Figura 3 - Níveis de decisão e atores no Espaço Cibernético

Fonte: BRASIL (2020b)

A efetividade operacional conjunta para combater no domínio cibernético será alcançada se forem identificadas claramente as capacidades a serem desenvolvidas, de modo a permitir a correta orientação, supervisão e condução do Sistema por parte do órgão central.

Para desenvolver, integrar e preparar, de modo contínuo e permanente, as capacidades cibernéticas das Forças Singulares e do Ministério da Defesa, o órgão central do SMDC se vale do Programa da Defesa Cibernética na Defesa Nacional (PDCDN). possibilitando o emprego operacional conjunto com efetividade.

O SMDC insere-se em um ambiente que contém outros sistemas e órgãos no contexto da Defesa Nacional. Portanto, faz-se necessário estabelecer seu relacionamento com os principais sistemas e órgãos com os quais interage ou poderá vir a interagir, sendo necessário identificar os principais óbices, desafios, riscos e impactos relacionados à sua operação. No trabalho em questão buscar-se-á propor uma solução para a integração do SMDC e as Infraestruturas Críticas de interesse da Defesa Nacional.

3 A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

A preocupação com a segurança dessas infraestruturas de interesse estratégico não é uma exclusividade brasileira, pelo contrário, ela surgiu em outros países, motivadas por acontecimentos que impactaram a história mundial. Nesse contexto, diversas nações, inclusive o Brasil, vem buscando se preparar, por meio de diretrizes e normas, com o intuito de evitar danos como os vistos no passado e que serão apresentadas nesta seção.

3.1 PRINCIPAIS CONCEITOS E MARCOS NORMATIVOS

Os ataques terroristas desencadeados em 11 de setembro de 2001 foram um divisor de águas na preocupação com segurança das infraestruturas críticas. A partir desses acontecimentos a atenção para o assunto se tornou mundial. Além do Estados Unidos da América (EUA), a União Europeia e o Conselho de Segurança da Organização das Nações Unidas, também buscaram melhorar suas condições de proteção, emitindo diretrizes e resoluções, com o intuito de reduzir falhas e ampliar os meios disponíveis para essas ações de segurança. Ressalta-se que esses organismos internacionais buscaram garantir que as iniciativas não se restringissem à segurança interna de cada país, mas também, que se criassem condições de um ambiente cooperativo entre os membros, com o intuito de se multiplicar os esforços (BRASIL, 2020c). Tal fator mostra que um dano em uma infraestrutura crítica de um

determinado país pode ser tão grave a ponto de se criar um efeito dominó que comprometeria outras estruturas e a vida, sem respeitar fronteiras estatais.

A Portaria Nº 02, do Gabinete de Segurança Institucional da Presidência da República, de 8 de fevereiro de 2008, elencou como infraestruturas críticas no Brasil, as que operam nos setores de comunicações, de energia, de transportes, de finanças e de águas, dentre outras. Como característica comum elas possuem um caráter estratégico para o País, sendo essenciais para a segurança, a soberania, a integração e o desenvolvimento econômico e social.

No que se refere ao conceito de segurança de infraestruturas críticas é possível resumi-lo como o conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas (BRASIL, 2018a). A peculiaridade dessa segurança está no fato da necessidade de integração, já que uma ação que prejudique um setor poderá acarretar dano aos demais. Por exemplo, um ataque a uma usina hidrelétrica poderá ser fatal a uma usina de tratamento de águas ou a uma central de telecomunicações, já que ambas necessitam da energia elétrica gerada pela primeira.

A segurança das infraestruturas críticas pode ser afetada de várias formas. Por ação da natureza como tempestades, inundações e terremotos ou por ação do ser humano como atentados terroristas, roubos, negações de serviço e ataques estatais (FERREIRA, 2020). O Brasil, apesar de ser um país de dimensões continentais, possui um baixo histórico de acidentes naturais. No que tange a ação humana, o risco não pode ser considerado baixo, tendo em vista que a motivação para ataques em ambiente cibernético se encontra em um espectro que vai desde a ideologia política até a busca da obtenção de lucros.

Nesse contexto, a primeira edição da END, relacionava a atividade de segurança de infraestruturas como estratégica, atribuindo ao GSI/PR a função de coordenar, avaliar, monitorar, reduzindo os riscos a estas estruturas (BRASIL, 2008). Somente 10 (dez) anos depois, o Governo brasileiro publicaria a PNSIC, caracterizando a segurança de infraestruturas críticas como uma atividade de Estado, sinalizando à sociedade brasileira, a prioridade atribuída ao tema no âmbito da segurança institucional. Essa política elenca nos artigos 2º e 3º, seus princípios e objetivos:

> Art. 2º São princípios da PNSIC:
> I - a prevenção e a precaução, com base em análise de riscos;
> II - a integração entre as diferentes esferas do Poder Público, o setor empresarial e os demais segmentos da sociedade;
> III - a redução de custos para a sociedade decorrente de investimentos em segurança; e
> IV - a salvaguarda do interesse da defesa e da segurança nacional.
> Art. 3º São objetivos da PNSIC:

> I - a prevenção de eventual interrupção, total ou parcial, das atividades relacionados às infraestruturas críticas ou, no caso de sua ocorrência, a redução dos impactos dela resultantes;
> II - o estabelecimento de diretrizes e instrumentos para salvaguardar as infraestruturas críticas consideradas indispensáveis à segurança nacional;
> III - a integração de dados sobre ameaças, tecnologias de segurança e gestão de riscos;
> IV - a identificação das relações de interdependência entre as infraestruturas críticas no País;
> V - o desenvolvimento, com enfoque na prevenção, de uma consciência acerca da segurança de infraestruturas críticas; e
> VI - o estabelecimento da prevalência do interesse da defesa e da segurança nacional na proteção, na conservação e na expansão das infraestruturas críticas. (BRASIL, 2018a, p.02)

Como consequência, em 2020, foi elaborado um documento orientando a busca para alcançar os objetivos supramencionados, a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC). A ENSIC elenca os eixos estruturantes (articulação institucional, conscientização e capacitação, fomento às ações e gestão de dados e informações), os objetivos e as iniciativas estratégicas para a elaboração de um Plano Nacional de Infraestruturas Críticas (BRASIL, 2020c).

3.2 O ENFOQUE DA SEGURANÇA CIBERNÉTICA PARA AS INFRAESTRUTURAS CRÍTICAS

Os eixos estruturantes, objetivos e inciativas estratégicas da ENSIC irão construir um ambiente propício ao desenvolvimento da Segurança Cibernética das infraestruturas críticas. Porém, é importante focar no eixo estruturante Gestão de Dados e Informações que possui os objetivos e iniciativas estratégicas listados no Quadro 1.

Quadro 1 - objetivos e iniciativas estratégicas do eixo estruturante gestão de dados e informações

OBJETIVOS ESTRATÉGICOS	INICIATIVAS ESTRATÉGICAS
1. Promover, no âmbito da administração pública e do setor privado, a geração, a disponibilização e a atualização periódica de dados íntegros, consistentes e padronizados sobre infraestruturas críticas e ameaças.	1.1 Orientar a organização, a tempestividade na atualização, na transmissão e no armazenamento dos dados sobre infraestruturas críticas e ameaças.
	1.2 Acompanhar a evolução da segurança das infraestruturas críticas, com base em métricas e periodicidade pré-definidas no Plano Nacional de Segurança de Infraestruturas Críticas e nos planos setoriais (relatórios, indicadores e ferramentas, entre outros).

2. Desenvolver um sistema dedicado à gestão de informações relacionadas à segurança de infraestruturas críticas.	2.1 Dispor de um sistema dedicado (central) para a captação, a integração, o armazenamento e o compartilhamento de informações relacionadas à segurança das infraestruturas críticas.
	2.2 Promover o compartilhamento de informações relevantes para a segurança de infraestruturas críticas, considerando regras de segurança da informação e a legislação específica.
3. Incentivar a adoção de recursos e de procedimentos voltados para a Segurança Cibernética nas infraestruturas críticas.	**3.1 Estimular os responsáveis pelas infraestruturas críticas a ampliarem seus investimentos em recursos cada vez mais avançados de Segurança Cibernética.**
	3.2 Orientar as infraestruturas críticas a observarem a Estratégia Nacional de Segurança Cibernética, principalmente o disposto no item 2.3.5 do Anexo ao Decreto nº 10.222, de 2020.

Fonte: Adaptado de ENSIC (2020c, p.09, grifo nosso)

O Item 3 do Quadro 1 aponta para a importância da Segurança Cibernética para as infraestruturas críticas, ratificando a necessidade de recursos e procedimentos. Cabe ressaltar que a segurança das infraestruturas críticas é de responsabilidade não só do setor privado, que obtém lucros financeiros pelos serviços que presta, mas também do poder público, que usufrui de tais serviços para a garantia do desenvolvimento do país, da soberania do estado e, até mesmo, da sobrevivência de sua população.

Nesse sentido, no que se refere às iniciativas estratégicas, pode-se observar o encontro e a interdependência estabelecida pelos marcos normativos que tratam sobre as infraestruturas críticas e Segurança Cibernética. O item 2.3.5 do Anexo ao Decreto nº 10.222, de 2020, estabelece as seguintes ações estratégicas:

> 2.3.5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais
> Proporcionar às infraestruturas críticas, maior resiliência que possibilite a contínua prestação de serviços essenciais, por meio das seguintes ações:
> - promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à Segurança Cibernética;
> - estimular a adoção de ações de Segurança Cibernética pelas infraestruturas críticas;
> - incentivar que essas organizações implementem políticas de Segurança Cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação, e de revisão periódica;
> - incentivar a constituição de ETIRs;
> - estimular que as infraestruturas críticas notifiquem o CTIR Gov dos incidentes cibernéticos; e
> - incentivar a participação das infraestruturas críticas em exercícios cibernéticos. (BRASIL, 2020d, p.07).

Assim sendo, pode-se inferir que não existe segurança de infraestruturas críticas sem proteção cibernética. Como será demonstrado, a evolução das ferramentas de exploração e ataque no espaço cibernético tem se modificado com o passar do tempo, não respeitando posição geográfica, condição econômica ou importância geopolítica.

3.3 AS INFRAESTRUTURAS COMO ALVO DE ATAQUES CIBERNÉTICOS

O ataque cibernético a infraestruturas críticas, considerado como o marco que despertou o interesse militar sobre o tema, foi realizado, em 2007, contra uma estrutura de redes de computadores do sistema bancário na Estônia. A saturação das páginas provocou a negação deste serviço a uma parcela considerável da população estoniana. O ocorrido levou, também, as páginas do governo local ao colapso. O ataque foi atribuído à Rússia em retaliação à retirada de uma estátua de bronze[3] de um soldado da União Soviética (GÓMEZ, 2018). Até o momento não foi possível comprovar os verdadeiros autores do ataque devido a utilização de técnicas de anonimização, que caracterizam a maioria dos ataques cibernéticos.

Em 2009, ocorreu um ataque cibernético que ficou conhecido como *Stuxnet*. Este ataque infectou, inicialmente, cinco organizações iranianas, afetando, indiretamente, a usina nuclear de *Natanz*. O governo iraniano acusou EUA e Israel pelas hostilidades. Porém, mais uma vez, nada foi comprovado (CLARKE, 2015).

O primeiro ataque cibernético a um sistema de controle de uma concessionária de energia elétrica foi realizado em 2015 na Ucrânia. A ação paralisou 27 (vinte e sete) subestações por cerca de seis horas. Os danos se espalharam, atingindo outros setores e continentes, causando prejuízos incalculáveis (ARAUJO, 2020). Um grupo russo de espionagem cibernética, que operava desde 2009, teria sido responsável pelo ataque denominado *BlackEnergy*, que literalmente desligou os disjuntores da Ucrânia (DAFLON, 2020).

O mais recente ataque de vulto ocorreu em maio deste ano, ao maior oleoduto da Empresa Colonial, nos EUA. Segundo a BBC News (2021), um grupo de *hackers* desconectou completamente a rede e roubou mais de 100 GB de informações. O duto transporta mais de 2,5 milhões de barris de óleo por dia, o que corresponde a 45% do abastecimento de diesel, gasolina e querosene de aviação da costa leste dos EUA. A ação atingiu uma infraestrutura de transporte

[3] Soldado de Bronze de Tallin: estatua localizada próxima aos restos mortais de soldados do Exército Vermelho mortos na Segunda Guerra Mundial

afetando, também, o setor energético e, consequentemente, a economia americana, fazendo o governo declarar estado de emergência.

3.4 A IMPORTÂNCIA DA SEGURANÇA DAS INFRAESTRUTURA CRÍTICAS PARA A DEFESA

A geração de energia, o transporte de cargas e pessoas, o abastecimento de água para a população e a operação do sistema financeiro são vitais para a estabilidade econômica, psicossocial, política e até militar de qualquer estado. Tal fato se comprova desde a Segunda Guerra Mundial, quando a Resistência Francesa explodia as linhas férreas para dificultar o abastecimento logístico das tropas Alemães (TRUEMAN, 2012) ou na Guerra do Golfo, quando Saddam Hussein mandou incendiar poços de petróleo no Kuwait, causando um desastre ambiental de grandes proporções, além de prejudicar o abastecimento e elevar o preço do barril em todo mundo (SOUSA, 2019). Dessa forma, as infraestruturas críticas se tornam um objetivo militar valioso em um conflito declarado.

Como visto no item anterior, o comprometimento dessas estruturas também poderá atingir outro estado mesmo em tempos de paz, tornando-se o centro de gravidade de uma campanha limitada que pode ter o objetivo não o de destruir o inimigo, mas de impingir baixas que o impossibilitem de combater ou que sinalizem que um conflito aberto poderia ter proporções ainda mais devastadoras, retirando a vontade do agredido de se engajar. Além disso, danos às infraestruturas críticas de um País poderão obrigar o Estado a gastar tempo, energia e recursos para o restabelecimento dos serviços, enfraquecendo-o ou mesmo incapacitando-o para uma reação em caso de um conflito de maiores proporções. Há que se falar, também, na segurança interna já que as infraestruturas podem ser alvos de terroristas e até mesmo do crime organizado na intenção de desestabilizar um governo ou ameaçar a população.

Nesse contexto, as ações cibernéticas se tornam uma ferramenta extremamente compensadora, já que pode ser empregada sem que se arrisque a vida de um soldado sequer, sendo possível, caso se decida e se tenha competência para isso, não revelar quem realmente provocou o dano.

Portanto, pode-se concluir que essas infraestruturas devem estar, também, sob os cuidados do Ministério da Defesa. Esta deverá atuar na colaboração para a proteção cibernética, mesmo que a responsabilidade esteja no nível político. Assim sendo, é mister que se criem procedimentos e estruturas capazes de integrar o SMDC aos órgãos responsáveis pela segurança

das infraestruturas, com o intuito de transformar o que está previsto nos marcos normativos em ações concretas.

4 INICIATIVAS INTERNAS E EXPERIÊNCIAS EXTERNAS DE INTEGRAÇÃO

Esta seção apresentará as ações de integração que já estão sendo realizadas no Brasil. Apresentará, ainda, as estruturas existentes em outros países para coordenar as ações de segurança cibernética.

4.1 CAPACITAÇÃO DE RECURSOS HUMANOS: INTEGRANDO POR MEIO DO ENSINO E DA PESQUISA.

A disseminação e o compartilhamento de conhecimentos e experiências são uma forma de aproximar instituições públicas e privadas, civis e militares. A END, ao colocar o Exército Brasileiro à frente do Setor Cibernético, provocou na Força um primeiro questionamento: como seria feita a capacitação do profissional militar que atuaria no espaço cibernético?

Em 2018, o General Gleuber Vieira, ex-Ministro e ex-Comandante do Exército, definiu que o ensino era a joia da coroa da Instituição. Analisando essas palavras, pode-se inferir que o conhecimento é um bem incomparável, capaz de moldar o maior patrimônio que o Exército pode ter: o seu pessoal. Profissionais, capacitados de maneira correta, não devem se limitar a planejar, executar e fiscalizar tarefas, mas devem atuar como indutores de conhecimento, além disso, sendo capazes de suprir, mesmo que parcialmente, a escassez dos meios existentes, mantendo seu autoaperfeiçoamento para operarem equipamentos no estado da arte, quando estes lhes forem fornecidos.

Assim sendo, era preciso escolher um estabelecimento de ensino capaz de formar os militares nessa nova capacidade. O Centro de Instrução de Guerra Eletrônica (CIGE), pioneiro no ensino de Guerra Eletrônica na América Latina, possuía, desde 2006, um núcleo de estudos de Cibernética conhecido como Projeto *Proteus* (COSTA, 2010). Dessa forma, em 2012, o Exército confiou ao CIGE a missão de capacitar recursos humanos na área de Guerra Cibernética, além de cooperar com a doutrina por meio destes cursos, estágios e programa de pós-graduação.

Hoje o CIGE conta com cursos e estágios voltados para militares, inclusive da Marinha do Brasil e da Força Aérea Brasileira, na área de cibernética. Nesses 11 (onze) anos, já foram formados 312 (trezentos e doze) militares, inclusive 2 (dois) da República Argentina, e 06 (seis) civis.

Os civis supracitados cursaram em caráter excepcional, a pedido de seus órgãos da Administração Pública Federal (APF), que vislumbravam a necessidade imediata de contar com profissionais qualificados para exercer a proteção cibernética de suas estruturas de redes, já que os cursos do CIGE, atualmente, possuem a duração de 24 (vinte e quatro) semanas, com reconhecida qualidade.

Ainda buscando apoiar os órgãos da APF, o CIGE tem a atendido a pedidos de cooperação de instrução extraordinários, com o intuito de promover uma capacitação inicial, particularizada, visando suprir as necessidades dessas instituições, ao mesmo tempo em que promove a integração de especialistas.

No que tange ao ensino em instituições civis, o Catálogo Nacional de Cursos Superiores de Tecnologia, de 2016, editado pelo Ministério da Educação (MEC), padroniza que um curso superior de tecnologia em Defesa Cibernética em uma instituição civil deve ter, pelo menos, 2.000 (duas mil) horas de carga horária, elencando o que egresso pode ser capaz de realizar após a conclusão:

> Analisa a operacionalidade das redes, os sistemas de conexão, e avalia as ameaças de invasão. Planeja, especificar e desenvolver sistemas de proteção de redes e de equipamentos de tecnologia da informação. Investiga e monitorar ataques. Estabelece procedimentos contra invasão de redes e guerra eletrônica. Coordena equipes de trabalho. Vistoria, realiza perícia, avalia, lauda e emiti parecer técnico em sua área de formação. (BRASIL, 2016c, P.54)

Assim sendo, como verificado, o profissional civil deve estar em condições de executar ações mais afetas à proteção cibernética de estruturas civis. Cabe destacar que o MEC especifica, neste mesmo documento, como possibilidades de prosseguimento de estudos para a Pós-Graduação de um curso superior de tecnologia em Defesa Cibernética, as áreas de Ciência da Computação e Ciências Militares.

Fica claro que os ensinos militar e civil podem atuar de maneira colaborativa e complementar, possibilitando uma integração desses meios. Nesse contexto, o Comandante do Exército criou a Escola Nacional de Defesa Cibernética (ENaDCiber), tendo sido ativada como Núcleo pela Portaria nº 002-Cmt Ex, de 02 de janeiro de 2015. A ativação como OM do Exército

Brasileiro, subordinado ao ComDCiber, seria efetivada 4 (quatro) anos mais tarde pela Portaria nº 099-Cmt Ex, de 30 de janeiro de 2019.

A nova escola tem como missão capacitar recursos humanos para atender às necessidades do setor cibernético de interesse da Defesa Nacional (ENADCIBER, 2021). É possível verificar que não existe apenas o foco em capacitar o pessoal militar ou exclusivamente da APF, mas todo aquele profissional que possa contribuir para a defesa cibernética. À ENaDCiber foi atribuído:

> - Atuar como centro polarizador de ensino e pesquisa em Segurança e Defesa Cibernética no âmbito nacional.
> - Ministrar cursos de graduação superior de tecnologia, de pós-graduação lato sensu (especialização) e stricto sensu (mestrado e doutorado), estágio de pós-doutorado e outros estágios em Segurança e Defesa Cibernética para militares e civis.
> - Conduzir treinamentos em atividades de Segurança e Defesa Cibernética.
> - Promover a pesquisa nas áreas de Segurança e Defesa Cibernética, inclusive com a participação de instituições congêneres militares e civis, nacionais e estrangeiras.
> - Cooperar com o desenvolvimento da doutrina de Segurança e Defesa Cibernética.
> - Fomentar a pesquisa na área de Segurança e Defesa Cibernética.
> - Incrementar a base de conhecimento do setor cibernético, no que tange à Segurança e à Defesa Cibernética, por meio de programas de extensão, treinamentos, congressos, seminários e outras atividades afins.
> - Capacitar recursos humanos para proporcionar pronta resposta às ameaças cibernéticas.
> - Promover a sensibilização e a conscientização quanto à Segurança e à Defesa Cibernética Nacional. (ENADCIBER, 2021)

Pelo que foi apresentado sobre a ENaDCiber é possível assegurar que este estabelecimento de ensino atua gerando capacidades ao SMDC, bem como a setor cibernético, incluindo as infraestruturas críticas. O caráter dual dessa Escola poderá proporcionar a disseminação de conhecimento e doutrina, gerando uma mentalidade de busca pela segurança de ativos cibernéticos em todos os setores, proporcionando a integração fundamental para a defesa da Pátria.

4.2 O USO DE SIMULADORES: SOLUÇÃO PARA INTEGRAÇÃO NA CAPACITAÇÃO E NO PREPARO.

Segundo BARFORD (2009), o espaço cibernético é profundamente distinto e, por esse motivo, as ferramentas e processos utilizados em outros espaços, como o físico e o

eletromagnético, podem não funcionar, adequadamente, com o ambiente cibernético. Como já citado, o CIGE, desde 2012, é o responsável pelos cursos de formação dos guerreiros cibernéticos dentro do SMDC. Dessa forma, com o intuito de melhorar o processo ensino-aprendizagem, vislumbrou-se a adoção de novas ferramentas, capazes de simular ações no espaço cibernético. Assim sendo, em 2013, foi entregue ao CIGE o Simulador de Operações Cibernética (SIMOC). Idealizado no próprio Centro, que já havia adquirido uma vasta experiência na utilização de simuladores para o ensino de Guerra Eletrônica, e desenvolvido pela empresa *Decatron*, o SIMOC foi projetado com tecnologia 100% nacional (EXÉRCITO BRASILEIRO, 2013). Operando com uma solução de uso dual, integra ativos de redes virtuais e componentes reais e permite o acompanhamento e a avaliação de todas as atividades executadas pelo aluno em tempo real, otimizando o resultado dos treinamentos. Baseado em cenários criados pelos instrutores, simula situações reais de ataques cibernéticos a infraestruturas, capacitando os alunos em análises de vulnerabilidades de redes, permitindo a execução de ações, em ambiente controlado, de proteção cibernética e defesa ativa, além do treinamento baseado em cenários reais de catástrofes e comprometimentos de infraestruturas críticas nacionais (EXÉRCITO BRASILEIRO, 2021). O SIMOC permite, ainda, a integração com equipamentos reais, proporcionando testes de vulnerabilidades de hardwares ligados em rede. O simulador tem sido utilizado em instruções e avaliações nos cursos e estágios de Cibernética no CIGE, ao longo de mais de 8 (oito) anos, tornando-se uma ferramenta desse Centro no ensino de Guerra Cibernética

Cabe ressaltar, ainda, que a importância do uso desses simuladores pode ser sentida não apenas na capacitação como já citado. O SIMOC também pode ser utilizado no preparo, em exercícios como o Guardião Cibernético; na certificação de estruturas de rede, simulando cenário afetos à cada instituição, com o intuito de avaliar seu grau de proteção; e, até mesmo, na seleção de pessoal, medindo o conhecimento e a competência de profissionais para executarem ações no ambiente cibernético.

Do exposto, pode se inferir que simuladores de emprego dual que possam ser utilizados pelo SMDC e pelas infraestruturas críticas, podem ser ferramentas de ensino e de apoio ao preparo confiáveis e seguras. Ademais, podem servir para testes de vulnerabilidades de redes e equipamentos, além de processo de seleção para o desempenho de funções no setor cibernético.

4.3 O EXERCÍCIO GUARDIÃO CIBERNÉTICO (EGC)

O Guardião Cibernético é um exercício focado na ação de proteção cibernética de infraestruturas críticas de interesse da Defesa Nacional. A atividade é planejada, coordenada e conduzida pelo ComDCiber nas instalações do CIGE, na cidade de Brasília-DF, e do Comando Militar do Sudeste (CMSE), na cidade de São Paulo-SP.

A concepção do exercício é baseada em um cenário realista de simulação, virtual e construtiva, que envolve a participação de líderes e especialistas de tecnologia da informação de setores estratégicos de interesse da Defesa Nacional. Os participantes precisam tomar decisões em tempo real para defender as infraestruturas críticas instaladas no cenário, por meio de atuação colaborativa e compartilhada.

O EGC é um exercício de alto nível, equiparado aos principais exercícios internacionais, como por exemplo o *Locked Shields* (OTAN) e *Ciber Perseu* (Portugal).

O principal objetivo do treinamento é desenvolver a coordenação e integração entre setores da Segurança e Defesa Cibernética, envolvendo áreas do Governo, Defesa, Academia e setor privado, com interesses e responsabilidades correlatas, com a finalidade de buscar a elevação do nível de proteção das infraestruturas críticas nacionais. Dentre outros objetivos, o EGC visa fortalecer a aproximação e estabelecer um ambiente colaborativo com os integrantes do ecossistema cibernético brasileiro, particularmente com as infraestruturas estratégicas críticas do País.

Na fase da simulação construtiva são empregados gabinetes de crise das áreas de tecnologia da informação, comunicação social, jurídica e alta administração dos setores Elétrico, Financeiro, Nuclear, Transporte, Água e Telecomunicações, com a missão de apresentar soluções para os eventos cibernéticos com impacto nas suas organizações. Já na fase da simulação virtual é utilizado o SIMOC, onde são reproduzidos sistemas computacionais utilizados pelos especialistas dos órgãos e empresas participantes.

As discussões nos gabinetes de crise demandam ações nos níveis decisório-gerencial (gestão de crise) e técnico (resposta a incidentes).

O EGC ocorre desde 2018, e atualmente é o único exercício cibernético no âmbito nacional. Para o ano de 2022, além do hub remoto na cidade de São Paulo, que está sendo desdobrado em 2021, haverá um hub remoto na cidade do Rio de Janeiro. A intenção do

ComDCiber é proporcionar essa oportunidade a mais participantes, com o objetivo precípuo de cooperar e colaborar com uma efetiva resiliência cibernética brasileira.

A Figura 4 apresenta a estrutura de participantes do Exercício Guardião Cibernético 3.0 que está previsto para ocorrer no período de 05 a 07 de outubro do corrente ano.

Figura 4 – Exercício Guardião Cibernético 3.0 (EGC 3.0)

Fonte: Adaptado de ComDCiber (2021)

O EGC está alinhado com a PNSI e a Estratégia Nacional de Cibernética (E-Ciber) ambas as legislações produzidas pelo GSI/PR, as quais preconizam a elevação da proteção cibernética no âmbito do governo e das infraestruturas críticas, por meio de ações baseadas na cooperação e integração.

Das muitas lições aprendidas no Guardião Cibernético, a que mais fica evidente é a necessidade de integração urgente entre o SMDC e os órgãos que proporcionam a proteção cibernética das infraestruturas críticas nacionais.

Apesar da proposta de integração entre os 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. Falta, em nível nacional, uma estrutura que normatize e integre as capacidades cibernéticas existentes no SMDC com as já existentes nas estruturas estratégicas do país.

Abordar-se-á, no item 4.4, algumas iniciativas e experiências externas de estruturas de Segurança Cibernética que integram o setor cibernético de Defesa e as estruturas críticas de interesse da Defesa Nacional de seus países.

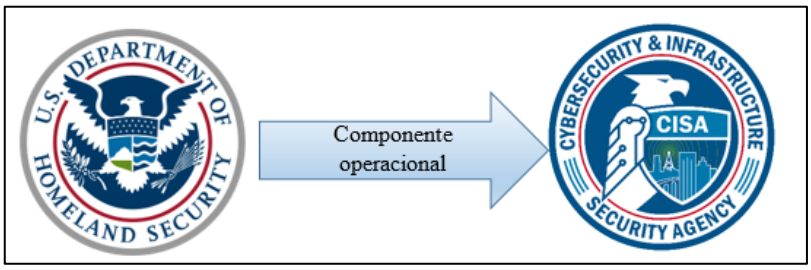
4.4 ESTRUTURAS DE SEGURANÇA CIBERNÉTICA INTERNACIONAIS

Nesta seção abordar-se-á as estruturas implantadas de Segurança Cibernética nos Estados Unidos (EUA) e Reino Unido. Essas organizações servem de referência para proposta de estrutura que desejamos implantar no Brasil, que atende à demanda crescente de coordenação entre a Defesa Cibernética e as estruturas estratégicas de interesse da Defesa Nacional

4.4.1 Estrutura de Segurança Cibernética dos EUA

No plano interno dos EUA, a Segurança Cibernética é planejada e coordenada pelo Departamento de Segurança Interna (DHS), que tem como seu componente operacional a Agência de Segurança Cibernética e Infraestrutura (CISA) como descrito na Figura 5, uma agência federal autônoma que tem por missão liderar o esforço nacional para entender e gerenciar o risco cibernético e físico para as infraestruturas críticas americanas.

Figura 5 - Responsabilidade da Segurança Cibernética interna dos EUA



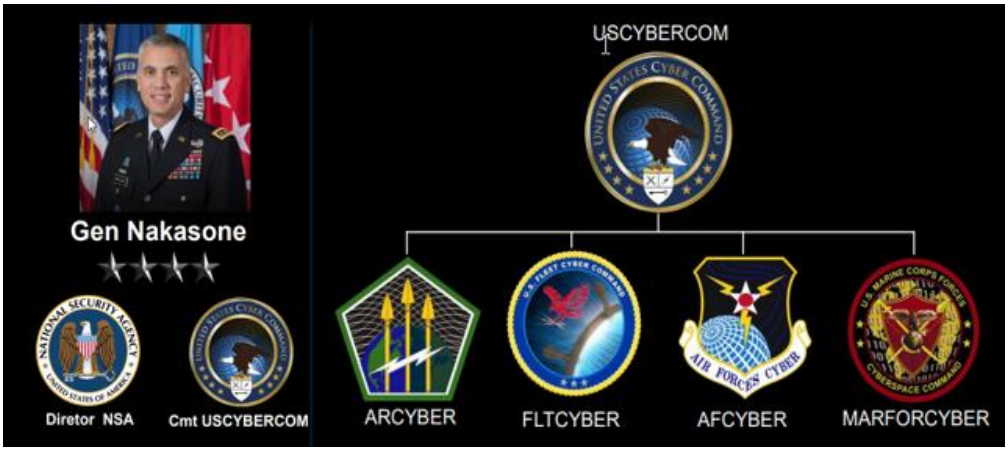
Fonte: Os autores

A CISA desenvolve a capacidade nacional de defesa contra ataques cibernéticos e trabalha com o governo federal para fornecer ferramentas de Segurança Cibernética, serviços de resposta a incidentes e recursos de avaliação para proteger as redes com a extensão .gov que suportam as operações essenciais de departamentos e agências parceiras dos EUA.

A CISA aprimora as comunicações interoperáveis de segurança pública em nos níveis do governo para ajudar os parceiros em todo o país a desenvolver suas capacidades de comunicação de emergência dentro do domínio cibernético.

No plano militar dos EUA, as atividades cibernéticas são de responsabilidade do *United States Cyber Command* (*USCYBERCOM*), que é o comando operacional cibernético das forças armadas, subordinado diretamente ao Departamento de Defesa (DoD). O comando cibernético é composto de vários componentes das Forças Armadas americanas, sendo guarnecido de forma conjunta. O comando projeta, coordena, integra, sincroniza e conduz atividades para direcionar as operações no domínio cibernético de forma a permitir ações em todos os domínios operacionais. Sua missão é garantir a liberdade de ação dos EUA no espaço cibernético e negar o mesmo aos seus adversários. Atualmente o comandante do *USCYBERCOM* é o Gen Nakasone, que acumula a função de diretor da Agência Nacional de Segurança (NSA), conforme pode ser visualizado na Figura 6.

Figura 6 – Estrutura do *United States Cyber Command (USCYBERCOM)*



Fonte: *USCYBERCOM*, (2019)

4.4.2 Estrutura Cibernética do Reino Unido

Em outubro de 2016, o governo britânico criou o *National Cyber Security Center* (NCSC) como uma das diretrizes da Estratégia de Segurança Cibernética (2016-2021) que estabelecia um conjunto de metas, ações e métricas mapeadas com a finalidade de proporcionar as suas próprias defesas no ambiente cibernético. A concepção do novo centro era integrar em um único órgão governamental as funções de Segurança Cibernética, incluindo o Centro de Tratamento de Incidentes de Rede do Reino Unido.

A Figura 7 apresenta imagem aérea do *National Cyber Security Center* (NCSC) em Londres na Inglaterra.

Figura 7 - National Cyber Security Center (NCSC)

Fonte: *National Cyber Security Center (NCSC)*, (OWASP 2021)

O NCSC tem como missão realizar parcerias de Segurança Cibernética entre o governo, a indústria e o público. O compromisso do NCSC de direcionar o engajamento da indústria, busca fornecer muitos elementos da estratégia nacional. Assim, o NCSC gerencia incidentes cibernéticos nacionais, fornece conhecimentos e oferece suporte personalizado e assessoria ao governo e à indústria (GUIMARÃES, 2017).

A estratégia atual visa prevenir e mitigar o impacto dos ataques cibernéticos no Reino Unido, refletida em um programa denominado *Active Cyber Defense* que visa fornecer proteções automatizadas aos cidadãos que acessam os serviços governamentais on-line e afirma que, sempre que possível, que tecnologias similares devem ser oferecidas ao setor privado e ao cidadão. A estratégia apoia o compartilhamento de informações, de forma que as organizações governamentais do Reino Unido tenham fácil acesso às informações sobre ameaças cibernéticas e melhorem o compartilhamento entre governo e indústria (GUIMARÃES, 2017).

O objetivo principal do NCSC é garantir que os cidadãos, empresas, organizações e instituições do setor público e privado tenham acesso à informação certa para se defender.

O compartilhamento da inteligência de ameaças sobre ataques cibernéticos avançados, motivações de cibercriminosos e táticas de atores mal-intencionados é essencial para defender redes e evitar ataques bem-sucedidos. Aumentando os objetivos de resiliência cibernética, a estratégia enfatiza que, tanto na indústria quanto no governo, a Segurança Cibernética precisa ser vista como uma preocupação de nível nacional, não apenas uma questão de TI.

5 SOLUÇÕES PARA INTEGRAÇÃO E COORDENAÇÃO DENTRO DO ECOSSISTEMA CIBERNÉTICO BRASILEIRO

Nesta seção será apresentada a avaliação do cenário, fruto da pesquisa bibliográfica realizada, e uma proposta de estrutura de segurança cibernética nacional que atenda às necessidades de integração entre o SMDC e as estruturas estratégicas de interesse da Defesa Nacional.

5.1 AVALIAÇÃO DO CENÁRIO JÁ APRESENTADO NESSE ESTUDO

Pode-se perceber que as normatizações para a proteção das infraestruturas críticas já estão bem definidas. Nessas políticas e estratégias também está clara a interdependência para que se atinjam os objetivos, particularmente no setor cibernético, ou seja, o "o que fazer" já é do conhecimento dos diversos segmentos interessados. Destaca-se, ainda, que existem exemplos positivos de integração entre o SMDC e as infraestruturas críticas no setor.

Além disso, países que se encontram no "estado da arte" em termos de proteção cibernética já possuem estruturas governamentais capazes de multiplicar as ações de Segurança e Defesa Cibernética por meio de uma coordenada integração. Porém, é importante verificar que as iniciativas de integração no Brasil, têm seguido um modelo de gestão diferente dos exemplos citados na seção 4 deste estudo. Neles é percebido um modelo *top down* ou seja, uma governança do nível mais alto para o nível mais baixo.

Nesse viés, faz-se necessário no Brasil, a criação de uma estrutura capaz integrar o SMDC às infraestruturas críticas, suprindo lacunas nos setores e promovendo novas iniciativas de integração.

5.2 PROPOSTA DE CRIAÇÃO DE UM CENTRO NACIONAL DE SEGURANÇA CIBERNÉTICA

A proposta de implementação de um Centro Nacional de Segurança Cibernética BRASIL (CNSC-BRASIL) tem por finalidade garantir a utilização segura e coordenada do espaço cibernético à população brasileira, bem como salvaguardar as estruturas estratégicas de interesse da Defesa Nacional de ataques cibernéticos.

O espaço cibernético é uma área de responsabilidade que obedece as mesmas lógicas, competências e ameaças que caracterizam a segurança e defesa do Estado, sendo essa garantia essencial a sobrevivência do País. Em diversas situações não é possível dissociar a Segurança Cibernética da Defesa Cibernética, pois a segunda, além de estar contida na primeira, possui interesses exógenos a sua área de atuação. Dessa forma, esse centro integraria ações de níveis hierárquicos diferentes, porém com interesses comuns, e teria a seguinte missão:

- orientar políticas e estratégias, bem como coordenar e gerir ações e parcerias nos setores civil e militar do Estado, da iniciativa privada e da academia, para a Segurança e a Defesa Cibernética, proporcionando a prevenção e a pronta resposta a ataques que possam vir a afetar o espaço cibernético de interesse.

A proposta de posicionamento do CNSC-BRASIL, dentro da estrutura governamental, seria vinculado ao GSI/PR, utilizando como embrião a estrutura já existente do Departamento de Segurança da Informação (DSI) do GSI/PR que tem sob sua subordinação o Centro de Tratamento de Incidentes de Redes do Governo Federal (CTIR-GOV). Tendo em vista que atualmente o DSI não possui ligações institucionais regulamentadas com as infraestruturas estratégicas de interesse da Defesa Nacional, o CNSC-BRASIL passaria a ter o papel de vincular as Equipes de Tratamento de Incidentes de Redes (ETIR) das infraestruturas estratégicas.

5.3 ATRIBUIÇÕES DO CNSC-BRASIL

O CNSC-BRASIL teria as seguintes atribuições:

a) coordenar as estruturas dos centros de tratamento de incidentes de redes governamentais;

b) integrar, por meio de sistemas de comunicações seguros, as ETIR das infraestruturas estratégicas, os CTIR da Defesa e o CTIR-GOV;

c) regular a capacitação dos RH das estruturas estratégicas estatais e privadas nos setores essenciais (Energia, Transportes, Saúde, Telecomunicações, Bancário e Defesa);

d) planejar a padronização na capacitação de RH, junto ao MEC e ao MD, contra o cibercrime, a ciberespionagem, o ciberterrorismo e o hackitivismo dentro dos ambientes acadêmicos civis e militares, facilitando a obtenção de conhecimento tanto no SMDC quanto nas estruturas estratégicas críticas de interesse da Defesa Nacional;

e) apoiar o desenvolvimento da ENaDCiber para atender as demandas do CNSC, com o intuito de intensificá-la como um centro polarizador de ensino e pesquisa em Segurança e Defesa Cibernética no âmbito nacional;

f) propor e coordenar exercícios entre setores da Segurança e Defesa Cibernética, envolvendo entes do governo, iniciativa privada e academia, multiplicando a capacidade de proteção e a resiliência cibernética para as infraestruturas críticas nacionais;

g) padronizar os procedimentos para definição dos níveis de alerta para o setor cibernético nacional;

h) regular a aquisição e o desenvolvimento de *hardwares* e *softwares*, definindo requisitos técnicos e operacionais mínimos necessários a proporcionar a proteção das estruturas estratégicas de interesse da segurança e da Defesa Nacional;

i) propor a alocação de recursos governamentais e fomentar a captação de recursos da iniciativa privada para capacitação de RH, preparo e emprego dentro do setor cibernético;

j) fomentar parcerias com agências similares de outros países, buscando a inserção na rede de proteção cibernética internacional; e

k) propor a criação de marcos normativos de interesse nos níveis da Defesa e Segurança Cibernética, bem como a atualização dos existentes.

6 **CONSIDERAÇÕES FINAIS**

O Setor Cibernético brasileiro permanece em constante evolução. Diariamente observa-se pelos meios de comunicações o aumento das ameaças cibernéticas em países ao redor do planeta. O Setor Cibernético de Defesa, vigilante a este cenário, tem elaborado uma regulamentação sólida e desenvolvido diversas iniciativas, destacando-se, a criação do SMDC.

Paralelamente, diversos entes, tanto da APF, como da iniciativa privada, têm desenvolvido seus próprios setores de proteção dos seus ativos cibernéticos, porém de forma desarticulada quando se pensa em uma proteção cibernética nacional. Como se verificou neste estudo, os interesses do SMDC avançam além dos limites da Defesa Cibernética, particularmente quando se trata de infraestruturas estratégicas críticas em setores tão caros à nação como os de energia, telecomunicações, financeiro, saúde dentre outros.

Conforme foi demostrado, a integração entre o SMDC e às infraestruturas críticas é fundamental não apenas para a sensação de segurança, mas prioritariamente na defesa da Pátria.

Essa integração existe por ações bilaterais entre o SMDC e as infraestruturas, carecendo de um impulso e uma coordenação nacional. Assim, surge a proposta da criação de um Centro capaz de integrar e coordenar as necessidades das infraestruturas críticas com o SMDC, no nível da Defesa Cibernética. Portanto, terá por finalidade promover ações organizadas em um ambiente colaborativo dentro do espaço cibernético de interesse da nação brasileira.

A proposta de criação do CNSC-BRASIL segue uma tendência de outros países, tais como EUA e Reino Unido que já possuem uma estrutura capaz de propiciar a sinergia necessária para a proteção de ativos cibernéticos de interesses da Defesa Nacional.

É importante destacar que este Centro poderá ser um marco na estruturação da Segurança Cibernética em nível nacional. Após consolidar-se nesse cenário, em um segundo momento, vislumbra-se que ele passe a ser uma agência reguladora nos moldes das já existentes na APF, tendo uma missão mais abrangente e independente, não restringindo-se a única tarefa de realizar a integração entre o SMDC e as infraestruturas críticas. Esta agência reguladora será o ponto de coordenação, gestão e fiscalização da Segurança Cibernética e, por conseguinte, de orientação para a Defesa Cibernética.

Por fim, pode-se concluir que a proteção cibernética das infraestruturas críticas, vitais para a existência do Estado brasileiro, quer em tempo de paz ou de guerra, deve ser uma prioridade para o SMDC, porém, na atual realidade, se faz necessária a criação da estrutura em nível nacional, com a finalidade de prover o uso mais racional e distribuído destes recursos, evitando redundâncias ou lacunas.

REFERÊNCIAS

ARAUJO, Jose Euclides Oliveira de. **A Atuação da Defesa Cibernética na Proteção de Infraestruturas Críticas do Brasil**. Artigo (Trabalho de Conclusão de Curso, Brasília) – Escola Superior de Guerra, Brasília, 2020.

BARFORD, P. *et al*. **Cyber situational awareness**: issues and research. Nova York. 2009.

BBC NEWS. **O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência,** 10 de maio 2021. Disponível em: https://www.bbc.com/portuguese/internacional-57055618/. Acesso em: 14 jul. 2021.

BRASIL, Decreto nº 6703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 19 dez 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm#:~:text=DECRETO%20N%C2%BA%206.703%2C%20DE%2018,que%20lhe%20confere%20o%20art.&text=1o%20Fica%20aprovada%20a,Defesa%20anexa%20a%20este%20Decreto. Acesso em: 29 abr. 2021.

BRASIL. Ministério da Defesa. **MD31-M-07. Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília, DF, 2016a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 26 abr. 2021

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF, 2016b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 26 abr. 2021

BRASIL. Ministério da Educação. **Catálogo Nacional de Cursos Superiores de Tecnologia.** Brasília, DF, 2016c.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança das Infraestruturas Críticas. **Diário Oficial da União**, Brasília, DF, 23 nov. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm Acesso em: 29 abr. 2021.

BRASIL, Decreto nº 9637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. **Diário Oficial da União**, Brasília, DF, 27 dez 2018b. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938. Acesso em: 29 abr. 2021.

BRASIL. Ministério da Defesa. **Portaria Normativa nº 3781 GM/MD**, de 17 de novembro de 2020a. Cria o Sistema Militar de Defesa Cibernética e dá outras providências. Brasília, DF, 2020.

BRASIL. Ministério da Defesa. **MD30-M-01. Doutrina de Operações Conjuntas**. 2.ed. Brasília, DF, 2020b.

BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança das Infraestruturas Críticas. **Diário Oficial da União**, Brasília, DF, 10 dez. 2020c. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357. Acesso em: 26 abr. 2021.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, DF, 06 fev. 2020d. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 10 abr. 2021.

CLARKE, Richard. **Guerra Cibernética**: a próxima ameaça e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

COSTA, Angelo Giusepp Amaral da. **O Exército Brasileiro e a Guerra cibernética**: situação atual e perspectivas. Escola de Comando e Estado-Maior do Exército. Rio de Janeiro. 2010.

COMDCIBER. **Apresentação no Comando Militar do Sudeste sobre o Exercício Guardião Cibernético 3.0 (EGC 3.0).** São Paulo, 2021.

DAFLON, Marlon Anderson Santiago. **Modelos de Dominação do Espaço Cibernético**: As Abordagens Brasileira e Russa à Guerra Cibernética**,** Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro, 2020.

ENADCIBER. **Apresentação para o Estágio de Adaptação ao Setor Cibernético.** Brasília, 2021.

EXÉRCITO BRASILEIRO. **Centro de Instrução de Guerra Eletrônica – Exército Apresenta Simulador Nacional de Operações Cibernéticas.** 2013. Disponível em: http://www.eb.mil.br/o-exercito. Acesso em: 08 ago. 2021.

EXÉRCITO BRASILEIRO. **Exército assina contrato de licenciamento de Simulador de Operações Cibernéticas,** 2013. Disponível em: http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/id/13829063. Acesso em: 08 ago. 2021.

FERREIRA, António Carlos dos Santos. **A Vulnerabilidade em Infraestruturas Críticas: Um Modelo de Análise.** Dissertação (Mestrado em Ciências Militares – Segurança e Defesa) - Instituto Universitário Militar, Pedrouços, 2020.

GOMEZ, Mariano Oscar. **Como construir sistemas cibernéticos resilientes avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN.** Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2018.

GUIMARÃES, Flávio de Queiroz. **Análise Comparativa da Estruturação do Setor Cibernético Nacional em Função das Doutrinas Cibernéticas Internacionais.** Centro de Instrução de Guerra Eletrônica, Brasília, 2017

HENRIQUES, Henrique de Queiroz. **Os desafios da capacitação de recursos humanos para a Defesa Cibernética**. Observatório Militar da Praia Vermelha, Escola de Comando e Estado Maior do Exército, Rio de Janeiro, 2021.

OWASP. **Introduction to the National Cyber Security Centre**. Disponível em: https://owasp.org/www-chapter-cambridge/presentations/prev/NCSC_slides.pdf. Acesso em 26 de agosto de 2021.

SOUSA, Ferdinando de. **A invasão do Kuwait pelo Iraque em 1990, o incêndio de poços e o despejo proposital de 500 milhões de barris de petróleo no mar.** 2019. Disponível em: https://ferdinandodesousa.com/2019/11/21/a-invasao-do-kuwait-pelo-iraque-em-1990-o-incendio-de-pocos-e-o-despejo-proposital-de-500-milhoes-de-barris-de-petroleo-no-mar/. Acesso em: 10 ago. 2021.

TRUEMAN, C N. **The French Resistance**. 2012. Disponível em: https://www.historylearningsite.co.uk/world-war-two/resistance-movements/the-french-resistance/. Acesso em: 10 ago. 2021.

USCYBERCOM. **Apresentação da estrutura do setor cibernético americano para comitiva ComDCiber.** Fort George G. Meade-Odenton: Maryland, 2019.