JOSÉ EUCLIDES OLIVEIRA DE ARAUJO

A ATUAÇÃO DA DEFESA CIBERNÉTICA NA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DO BRASIL

Trabalho de Conclusão de Curso – artigo científico – apresentado à Comissão de Avaliação de TCC da Escola Superior de Guerra – Campus Brasília, como exigência parcial para obtenção do certificado de Especialista em Altos Estudos em Defesa.

Orientador: Cel R1 EB THADEU LUIZ CRESPO ALVES NEGRÃO

Brasília
2020

Os TCC, nos termos da legislação que resguarda os direitos autorais, são considerados propriedade da Escola Superior de Guerra (ESG). É permitida a transcrição parcial de textos do trabalho ou mencioná-los para comentários ou citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa. Os conceitos expressos nos TCC são de responsabilidade do autor e não expressam necessariamente qualquer orientação institucional da ESG.

JOSÉ EUCLIDES OLIVEIRA DE ARAUJO (Idt 118142703-8)

JOSÉ EUCLIDES OLIVEIRA DE ARAUJO

A ATUAÇÃO DA DEFESA CIBERNÉTICA NA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DO BRASIL

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

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 22 de Outubro de 2020

THADEU LUIZ CRESPO ALVES NEGRÃO (Cel R1 EB)
Orientador

CLÁUDIO ALFREDO CUNHA DORNELLES (Cel R1 EB)
Avaliador 1

Profa. Dra. CINTIENE SANDES MONFREDO MENDES (ESG/RJ)
Avaliador 2

A atuação da Defesa Cibernética na proteção de infraestruturas críticas do Brasil.

José Euclides Oliveira de Araujo[1]

RESUMO

Este artigo trata da atuação da Defesa Cibernética na proteção de infraestruturas críticas do Brasil. A metodologia empregada foi baseada em pesquisa bibliográfica e análise documental. Primeiramente, são apresentadas a Política Nacional de Defesa e a Estratégia Nacional de Defesa, esta última como documento do Estado Brasileiro que define a divisão dos setores estratégicos da Defesa no âmbito das Forças Armadas. Após isso, são apresentados os conceitos de Segurança Cibernética, Proteção de Infraestruturas Críticas e Defesa Cibernética. Finalmente, busca-se apresentar qual seria o papel da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa. Outro aspecto foi o de apresentar o amparo legal para as atividades de Segurança e Defesa Cibernéticas.
Palavras-chave: Infraestruturas Críticas. Setores Estratégicos. Defesa Cibernética

The role of Cyber Defense in protecting critical infrastructure in Brazil.

ABSTRACT

This article deals with the performance of Cyber Defense in protecting critical infrastructure in Brazil. The methodology used was based on bibliographic research and document analysis. First, the National Defense Policy and the National Defense Strategy are presented, the latter as a document of the Brazilian State which defines the division of the Defense strategic sectors within the scope of the Armed Forces. After that, the concept of Cybersecurity, Critical Infrastructure Protection and Cyber Defense are presented. Finally, it seeks to present what would be the role of Cyber Defense in protecting critical infrastructure of interest to Defense. Another aspect was that of to present the legal support for the activities of Cyber Security and Defense addressed in the topic.
Keywords: Critical Infrastructure. Strategic Sectors. Cyber Defense.

[1] Coronel de Comunicações, Oficial do Comando de Defesa Cibernética. Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Guerra (ESG) Campus Brasília, 2020.

1 INTRODUÇÃO

A proteção de infraestruturas críticas é uma das prioridades do Governo Federal, considerando que a interrupção dos serviços de alguma dessas infraestruturas pode colapsar sistemas fundamentais para o funcionamento do país.

A Política Nacional de Defesa (PND) (BRASIL, 2018) e a Estratégia Nacional de Defesa (END) (BRASIL, 2018) tratam desse tema, buscando definir as responsabilidades na proteção das infraestruturas críticas, cujo valor estratégico demandam especial atenção durante o planejamento das ações de proteção.

Em relação à proteção cibernética de infraestruturas críticas, a END trata da responsabilidade no tocante à Segurança Cibernética, deixando este setor a cargo do Gabinete de Segurança Institucional da Presidência da República (GSI). Ao Ministério da Defesa (MD) coube as ações de Defesa Cibernética, buscando manter a proteção dos ativos das Forças Armadas (BRASIL, 2018).

Na definição dos setores estratégicos (espacial, cibernético e nuclear) o MD definiu que o Exército Brasileiro seria o coordenador do Setor Cibernético no âmbito da Defesa Nacional (BRASIL, 2009), devendo o mesmo implementar a sua estruturação, considerando a necessidade de independência tecnológica em relação a outros países.

A Defesa Cibernética estruturou-se na última década, apoiada pelo Programa de Defesa Cibernética na Defesa Nacional (PDCDN), tendo como principal entrega o Comando de Defesa Cibernética (ComDCiber) (BRASIL, 2014).

Mesmo sendo de responsabilidade do GSI, as infraestruturas críticas são, em sua maioria, de interesse da Defesa, demandando especial atenção do MD nas ações de proteção das mesmas. Tal interesse surge da necessidade de se manter o funcionamento dessas infraestruturas com vistas a se manter a capacidade de Defesa do país.

Com o aumento da capacidade de proteção cibernética no âmbito da Defesa, surgiu a necessidade de apoio à proteção cibernética das infraestruturas críticas, uma vez que tais infraestruturas são de interesse da Defesa.

O artigo tem o objetivo de avaliar a atuação da Defesa Cibernética na proteção de infraestruturas críticas sob o ponto de vista das esferas de responsabilidade, num cenário onde o ComDCiber aparece como uma alternativa importante na estrutura do Estado, possuindo capacidade para realizar ações de proteção efetivas.

O trabalho se baseará em pesquisa bibliográfica e análise documental, o que possibilitará a realização do diagnóstico e análise do programa que ampara o desenvolvimento do setor cibernético no âmbito da Defesa.

O referencial teórico da pesquisa está relacionado às principais Leis, Decretos, Políticas, Estratégias, Normas e Planos do Ministério da Defesa e do Exército relativos à atividade de Defesa Cibernética, além de autores de trabalhos acadêmicos relacionados a esses temas.

A seguir, serão desenvolvidos argumentos que abordam as esferas de responsabilidade através da PND e END, descrição do Programa Estratégico que norteia o desenvolvimento do Setor Cibernético e a avaliação da capacidade da Defesa Cibernética na proteção de infraestruturas críticas.

2 POLÍTICA NACIONAL DE DEFESA

A Política Nacional de Defesa (PND) (BRASIL, 2018), documento de mais alto nível do planejamento de ações destinadas à Defesa Nacional, trata do conceito de Segurança e Defesa Nacional, analisando os ambientes internacional e nacional, tratando, ainda, dos Objetivos Nacionais de Defesa.

De acordo com a PND, Defesa Nacional refere-se ao conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas.

A Constituição Federal de 1988, em seu artigo 21, inciso II, estabelece que compete à União assegurar a Defesa Nacional. O artigo 142 da CF dispõe que:

> As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.
> §1º - Lei complementar estabelecerá as normas gerais a serem adotadas na organização**,** no preparo e no emprego das Forças Armadas. (BRASIL, 1988)

A Política Nacional de Defesa (PND) (BRASIL, 2018), dispõe que a Defesa Nacional é o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas.

A Lei Complementar n.º 136, de 2010, no artigo 9°, inclui:

> § 2° O Livro Branco de Defesa Nacional deverá conter dados estratégicos, orçamentários, institucionais e materiais detalhados sobre as Forças Armadas, abordando os seguintes tópicos:
> "I - cenário estratégico para o século XXI;
> II - política nacional de defesa;
> III - estratégia nacional de defesa;
> IV - modernização das Forças Armadas (BRASIL, 2010)

A PND estabelece, entre outros, os seguintes Objetivos Nacionais de Defesa:

> II. Assegurar a capacidade de Defesa, para o cumprimento das missões constitucionais das Forças Armadas.
> Refere-se a, em última análise, dotar as Forças Armadas das capacidades necessárias para realizar a vigilância, o controle e a defesa do território, das águas jurisdicionais e do espaço aéreo brasileiros e prover a segurança das linhas de comunicação marítimas. Leva em conta a necessidade de contínuo aperfeiçoamento das técnicas e da doutrina de emprego das Forças, de forma singular ou conjunta, com foco na interoperabilidade; o adequado aparelhamento das Forças Armadas, empregando-se tecnologias modernas e equipamentos eficientes e em quantidade compatível com a magnitude das atribuições cometidas; e a dotação de recursos humanos qualificados e bem preparados. (BRASIL, 2018)

Em relação aos conceitos de Segurança e Defesa Nacional a PND estabelece:

> I. Segurança é a condição que permite ao País preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais; e
> II. Defesa Nacional é o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas. (BRASIL, 2018)

Verifica-se, assim, que a Política Nacional de Defesa busca orientar os setores militar e civil, visando o preparo e emprego com o intuito de atender à Defesa Nacional, assegurando a capacidade de resposta contra potenciais ameaças ao Brasil.

3 ESTRATÉGIA NACIONAL DE DEFESA

A Estratégia Nacional de Defesa (END) (BRASIL, 2018), 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 .

É interessante que seja reforçado o entendimento de que um país que pensa sua Defesa deve buscar desenvolver-se nos diversos setores. A transformação das Forças Armadas passa a ser essencial no entendimento da END.

A Estratégia Nacional de Defesa pauta-se em 25 (vinte e cinco) diretrizes. Dentre elas podemos destacar:

> 6. Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear. Esse fortalecimento assegurará o atendimento ao conceito de flexibilidade.
> Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar.
> Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio País não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço.
> O Brasil tem compromisso – decorrente da Constituição e da adesão a Tratados Internacionais – com o uso estritamente pacífico da energia nuclear. Entretanto, afirma a necessidade estratégica de desenvolver e dominar essa tecnologia. O Brasil precisa garantir o equilíbrio e a versatilidade da sua matriz energética e avançar em áreas, tais como as de agricultura e saúde, que podem se beneficiar da tecnologia de energia nuclear. E levar a cabo, entre outras iniciativas que exigem independência tecnológica em matéria de energia nuclear, o projeto do submarino de propulsão nuclear. (BRASIL, 2018)

A Estratégia Nacional de Defesa trata, ainda, das seguintes considerações sobre o Setor Cibernético:

> 3. No setor cibernético, as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades são as seguintes:
> (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;
> (b) Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à cerificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;
> (c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;

> (d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;
> (e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;
> (f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;
> (g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e
> (h) Estruturar a produção de conhecimento oriundo da fonte cibernética. (BRASIL, 2018)

Em relação à Segurança Nacional, a END trata das esferas de responsabilidade, onde aborda o aperfeiçoamento dos dispositivos e procedimentos de segurança com o intuito de reduzir a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos (BRASIL, 2018).

O Gabinete de Segurança Institucional da Presidência da República fica encarregado de coordenação da Segurança Cibernética em âmbito nacional, buscando atuar de modo amplo, cooperativo, participativo e alinhado com as ações de Defesa Cibernética a cargo do Ministério da Defesa (BRASIL, 2020).

A Diretriz Ministerial nº 0014, do Ministério da Defesa, de 09 de novembro de 2009, definiu as responsabilidades dos setores estratégicos, cabendo ao Exército Brasileiro a responsabilidade pela coordenação e integração do setor cibernético no âmbito da Defesa (BRASIL, 2009).

No capítulo onde trata dos setores estratégicos, a END impõe que a proteção das infraestruturas estratégicas virá de um conjunto de esforços de diversos setores, não apenas das Forças Armadas, onde a coordenação de tais ações será realizada pela Gabinete de Segurança Institucional da Presidência da República (BRASIL, 2018).

O Exército Brasileiro está encarregado da coordenação e integração do Setor Cibernético no âmbito da Defesa. Nos casos em que houver necessidade da participação do Exército na proteção de infraestruturas críticas será necessária a coordenação com o Gabinete de Segurança Institucional, uma vez que cabe ao GSI a coordenação de tais ações.

4. NÍVEIS DE ATUAÇÃO DO SETOR CIBERNÉTICO

A partir do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa (BRASIL, 2018), três campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo do Gabinete de Segurança Institucional da Presidência da República , a Defesa Cibernética, a cargo do Ministério da Defesa e a Guerra Cibernética, no âmbito das Forças Armadas.

As ações no Espaço Cibernético passam a seguir, assim, denominações de acordo com o nível de decisão.

Figura 1 - Níveis de atuação do Setor Cibernético

Fonte: Doutrina Militar de Defesa Cibernética – MD31-M-07 (BRASIL, 2014)

De acordo com o Manual de Doutrina Militar de Defesa Cibernética (MD31-M-07) (2014) as ações no espaço cibernético deverão seguir as seguintes denominações de acordo com o nível de decisão:

> **nível político** - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;
> **nível estratégico** - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças

> Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e
> **níveis operacional e tático** - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas. (BRASIL, 2014)

4.1 SEGURANÇA CIBERNÉTICA

Em 2015, o Governo Federal deu publicidade à Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (BRASIL, 2015), com validade até 2018, como um importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, cujo objetivo foi de melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais. Esse documento impulsionou as discussões sobre o tema no âmbito da Administração Pública Federal, e também em outros setores da sociedade.

O Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação (BRASIL, 2018) e dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e entidades da Administração Pública Federal, sob o prisma da governança, previu, para sua implementação, a elaboração da Estratégia Nacional de Segurança da Informação e dos Planos Nacionais. Em virtude da abrangência da Segurança da Informação este documento, indicou, em seu art. 6º, que a Estratégia Nacional de Segurança da Informação seja construída em módulos, a fim de contemplar a Segurança Cibernética, a Defesa Cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados.

A Segurança Cibernética é considerada atualmente a área mais crítica a ser abordada, com isso, o Gabinete de Segurança Institucional da Presidência da República elegeu, em janeiro de 2019, a Estratégia Nacional de Segurança Cibernética (E-Ciber) (BRASIL, 2020) como primeiro módulo da Estratégia Nacional de Segurança da Informação, a seu cargo, a ser elaborada.

Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo Federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.

Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais.

Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão.

De acordo com o Manual de Campanha GUERRA CIBERNÉTICA (EB70-MC-10.232) (2017) as atuações no nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética – são coordenadas pela Presidência da República, abrangendo a Administração Pública Federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais e no nível estratégico a Defesa Cibernética permanece a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA, interagindo com a Presidência da República e a APF (BRASIL, 2017).

Verifica-se, assim, que Segurança e Defesa Cibernética atuam em diferentes esferas de poder, mantendo profunda interação de suas ações, devido à transversalidade do tema em questão.

4.2 DEFESA CIBERNÉTICA

De acordo com o Glossário das Forças Armadas (MD35-G-01) (2015) Defesa Cibernética é definida como o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de 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 (BRASIL, 2015).

O Setor Cibernético contempla o emprego de modernos meios tecnológicos, enfaticamente as redes de computadores e de comunicações destinadas ao trânsito de informações, seja por meio de pessoas, no atendimento de suas necessidades individuais, seja por organizações diversas, inclusive aquelas dedicadas a setores estratégicos do País, como a Defesa Nacional.

O atual Programa da Defesa Cibernética na Defesa Nacional (PDCDN) incluiu o Exército Brasileiro no restrito grupo de organizações, nacionais e internacionais, que possuem a capacidade de desenvolver medidas de proteção e mitigação de ataques no campo cibernético (BRASIL, 2014).

Dentre as potenciais ameaças no campo da Defesa Cibernética, verifica-se o risco de ataques perpetrados por Estados, organizações e pequenos grupos, fruto das mais diversas motivações (BRASIL, 2014).

É nesse contexto que a Defesa Cibernética busca atuar na proteção dos ativos das Forças Armadas, com capacidade para apoiar a proteção de infraestruturas críticas e outros setores do Governo.

4.3 GUERRA CIBERNÉTICA

A "Guerra Cibernética" é uma denominação restrita ao âmbito das Forças Armadas, dentro de um contexto de planejamento militar de nível operacional ou tático (BRASIL, 2014).

Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2.

As ações decorrentes da Guerra Cibernética estarão focadas no nível de dependência do oponente em relação aos seus meios de TIC. A análise desse nível de dependência será fundamental para o planejamento das operações (BRASIL, 2014).

A Guerra Cibernética poderá ser planejada e executada mediante solicitações de efeitos desejados pelo Comando Operacional, por grupos específicos designados para tal, empregando o canal técnico com os órgãos responsáveis pela Defesa Cibernética de cada FA e do Ministério da Defesa (BRASIL, 2014).

5. **O COMANDO DE DEFESA CIBERNÉTICA**

A Diretriz Ministerial nº 14/2009 (MD) (2009) atribuiu a cada Força Armada a liderança das atividades de um setor estratégico, cabendo ao Exército a coordenação do Setor Cibernético no âmbito da Defesa Nacional (BRASIL, 2009).

Após a criação do Centro de Defesa Cibernética (BRASIL, 2010), passando a funcionar dentro da estrutura regimental do Exército Brasileiro a partir de 2012, vários estudos foram realizados com a participação das outras duas Forças Armadas e de instituições públicas e privadas, os quais apontaram para a necessidade de se estabelecer outros projetos, a

fim de promover a expansão e a abrangência das atividades de Defesa Cibernética para toda a Defesa Nacional e instituições a ela relacionadas.

Por intermédio da Portaria Normativa nº 2777/MD, de 27 de outubro de 2014 (BRASIL, 2014), o Sr Ministro estabeleceu a Diretriz de Implantação de medidas visando à potencialização da Defesa Cibernética Nacional, com a atribuição dos seguintes encargos:

> 1. Pelo Estado-Maior Conjunto das Forças Armadas (EMCFA):
>
> I - supervisionar a implantação das medidas necessárias, com ênfase nas seguintes iniciativas: criação do Comando de Defesa Cibernética (ComDCiber) na Estrutura Regimental do Comando do Exército, que contará, na forma da legislação, com o exercício de militares das três Forças Armadas, cabendo ao EMCFA as atividades de coordenação nos casos de operações conjuntas, especificando-se, em atos próprios, os aspectos inerentes ao controle operacional;
>
> .....
>
> 3. Pelo Exército Brasileiro (EB), em articulação com o EMCFA, com a SG e com as demais Forças Armadas: I - tomar as providências necessárias à imediata ativação do Núcleo do Comando de Defesa Cibernética (NuComDCiber), subordinado ao Centro de Defesa Cibernética (CDCiber), dotado de pessoal e infraestrutura para os trabalhos de implantação do Comando de Defesa Cibernética (ComDCiber); (BRASIL, 2014)

Em 25 Fev 15, o Ch EME aprovou a Diretriz de Iniciação do Programa da Defesa Cibernética na Defesa Nacional, tendo, como um dos objetivos do Programa:

> a. Criar e implantar o Comando de Defesa Cibernética (ComDCiber), na Estrutura Regimental do Comando do Exército, integrado por militares das três Forças Armadas (FA), para atuar nas atividades de ciência, tecnologia e inovação, doutrina, recursos humanos, operações e inteligência de Defesa Cibernética. O ComDCiber deverá contar com o Centro de Defesa Cibernética (CDCiber), como organização militar diretamente subordinada, para executar as duas últimas atividades mencionadas. (BRASIL, 2015)

O Comando de Defesa Cibernética está estruturado para atender as missões acima previstas de acordo com o seguinte organograma:

Figura 2 – Organograma do Comando de Defesa Cibernética

Fonte: Comando de Defesa Cibernética (2020)

Do acima exposto, verifica-se que o Comando de Defesa Cibernética possui grande desafio pela frente, necessitando capacitar seus quadros e atuar na sua estrutura organizacional, com a finalidade de atender à missão de estruturar o Setor Cibernético de Defesa.

5.1 O SISTEMA MILITAR DE DEFESA CIBERNÉTICA

A atuação de Defesa Cibernética visa atender às necessidades da Defesa Nacional. Nesse contexto, buscou-se a criação do Sistema Militar de Defesa Cibernética (SMDC) visando a integração com órgãos de interesse dentro de uma situação de normalidade institucional, com a finalidade de facilitar as ações decorrentes de uma evolução para situações de crise ou conflitos (BRASIL, 2014).

O Sistema Militar de Defesa Cibernética (SMDC) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades relacionadas à Defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional (MD31-M-07) (BRASIL, 2014).

Uma das próximas medidas a serem adotadas pelo MD é a publicação de uma Portaria para efetivação do ComDCiber como órgão central do SMDC. A referida Portaria seguirá o que já está previsto no Manual de Doutrina Militar de Defesa Cibernética (MD31-

M-07) (2014), considerando a substituição de CDCiber para o ComDCiber como órgão central do SMDC, tendo em vista a criação do ComDCiber em 2016:

> 3.3.3 O órgão central do SMDC é o Centro de Defesa Cibernética (CDCiber), que passa ao controle operacional do MD nas Operações Conjuntas e conta, permanentemente, com um Estado-Maior Conjunto para realizar o planejamento e o controle das ações planejadas, levando em conta as particularidades de cada Força Armada, de modo a obter uma atuação sinérgica (BRASIL, 2014).

Cabe destacar, que a atuação do ComDCiber, no tocante ao SMDC, ocorre sob orientação e supervisão do MD, no nível estratégico, realizando as ações de coordenação e integração do Setor Cibernético nas Forças Armadas e privilegiando, sempre que possível, uma forma de atuação conjunta (BRASIL, 2014).

5.2 PROGRAMA DA DEFESA CIBERNÉTICA NA DEFESA NACIONAL

O Programa da Defesa Cibernética na Defesa Nacional (PDCDN) foi estabelecido com base na Portaria Normativa nº 2.777/MD, de 27 de outubro de 2014, do Ministério da Defesa (MD) (BRASIL, MINISTÉRIO DA DEFESA, 2014), que aprovou a Diretriz de Implantação de Medidas visando à Potencialização da Defesa Cibernética Nacional. Com base nesse documento, foi elaborada, pelo Estado-Maior do Exército, com data de 25 de fevereiro de 2015, a Diretriz de Iniciação do Programa da Defesa Cibernética na Defesa Nacional, a cargo do Exército Brasileiro (BRASIL, 2015).

O Programa foi instituído com recursos do MD, sob a gerência do Exército Brasileiro, coordenador do Setor Cibernético no âmbito da Defesa Nacional, de acordo com o estabelecido na Diretriz Ministerial nº 014, de 9 de novembro de 2009 (BRASIL, 2009).

O PDCDN possui, dentre outros, os seguintes objetivos:

> a. Promover a inserção política e estratégica do setor cibernético da Defesa Nacional.
>
> b. Dotar o Ministério da Defesa (MD) e as Forças Armadas (FA) da estrutura de defesa necessária para desenvolver eficazmente todo o espectro das ações cibernéticas, visando proteger e defender os ativos de informação do MD e das FA, possibilitando atuar com liberdade de ação no espaço cibernético de interesse da Defesa Nacional e negando essa possibilidade aos oponentes.
>
> c. Implantar o Sistema Militar de Defesa Cibernética (SMDC), estruturando-o, definindo sua concepção e processos de integração com outros sistemas, órgãos e agências.
>
> d. Implantar o Comando de Defesa Cibernética

> (ComDCiber), na Estrutura Regimental do Comando do Exército, como órgão central do SMDC, integrado por militares das três Forças Armadas (FA), para atuar nas atividades de ciência, tecnologia e inovação, doutrina, recursos humanos, operações e inteligência de Defesa Cibernética.
>
> e. Promover a capacitação dos recursos humanos do Setor Cibernético, por meio da formação de massa crítica inicial e da implantação da Escola Nacional de Defesa Cibernética (ENaDCiber), subordinada ao ComDCiber, para fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão de Defesa Cibernética e para a melhoria da qualificação da mão de obra nacional para o setor.
>
> f. Otimizar a gestão, retenção e mobilização de recursos humanos imprescindíveis à condução das atividades cibernéticas necessárias à Defesa Nacional. (BRASIL, 2014)

Atualmente está sendo realizado um trabalho de readequação, reavaliação e reorientação do escopo do PDCDN. O objetivo principal é adequá-lo às necessidades de desenvolvimento do setor no âmbito da Defesa, verificadas ao longo dos últimos quatro anos, desde a criação do ComDCiber.

6. ATAQUES CIBERNÉTICOS CONTRA INFRAESTRUTURAS CRÍTICAS

Com o setor digital em ascensão e sendo utilizado em larga escala para fins pessoais, empresariais e governamentais, existe o risco de roubo de informações e de ataques por hackers. Assim, é perceptível o crescimento da quantidade de ataques cibernéticos ao longo dos anos (MARSH e McLENNAN, 2019).

Da mesma forma que o acesso à internet e seu uso vêm crescendo na sociedade, empresas e governo, os ataques hackers também. Esses ataques podem causar diversas consequências, tanto para o setor privado quanto para o setor público.

Em análise realizada em 2019, somente o crime cibernético custa aos países mais de US$ 1 trilhão globalmente, um múltiplo do recorde de US $300 bilhões de danos devido a desastres naturais em 2017 (MARSH e McLENNAN, 2019).

Em relação aos ataques cibernéticos contra infraestruturas críticas podem ser citados alguns exemplos marcantes que caracterizam o potencial de dano que pode ser causado nessas situações.

6.1 ESTÔNIA (2007)

Em abril de 2007, uma série de ataques cibernéticos à Estônia deixou sites do governo fora do ar. Na Estônia, quase todos os serviços são integrados à Internet, o que torna o país vulnerável a esses ataques. Esse foi considerado o primeiro ciberataque de grandes proporções (CLARKE, 2015).

As ações iniciaram logo no dia da remoção do Soldado de Bronze de Tallinn, no dia 27 de abril de 2007, o que significava uma afronta para os russos, prováveis autores do ataque, de acordo com o Governo da Estônia (CLARKE, 2015).

Após os ataques em DDoS, vários sites ficaram indisponíveis por algumas horas, não causando danos permanentes aos serviços da Estônia. Os ataques mostraram como os sistemas ligados à Internet são vulneráveis e deixou em alerta vários países com serviços virtuais que podem ser futuros alvos de ataques (CLARKE, 2015).

6.2 UCRÂNIA (2015)

Em 2015 um “mau funcionamento” do sistema elétrico da Ucrânia paralisou 27 subestações de energia durante seis horas. Após o evento, uma investigação identificou evidências de que vários sistemas de controle de energia regionais da Ucrânia tinham sido comprometidos por ataques cibernéticos (EECSP, 2017).

Este foi o primeiro ataque cibernético efetuado com sucesso ao sistema de controle de uma concessionária de energia elétrica que foi publicamente documentado. O ransomware apelidado de “NotPetya” deixou, aproximadamente, 225 mil pessoas sem energia (EECSP, 2017).

O prejuízo do ataque NotPetya não é restrito ao sistema elétrico ucraniano, e se alastrou para portos em 3 continentes, o que torna o cálculo exato do dano gerado pelo ataque uma tarefa difícil. No entanto, é possível estimar ao menos os danos diretos. No caso deste ataque, a Casa Branca estimou os custos totais em 10 bilhões de dólares (EECSP, 2017).

6.3 PORTO DE FORTALEZA / CE / BRASIL (2019)

Em outubro de 2019 um ataque cibernético permitiu que hackers invadissem o controle do Porto de Fortaleza e exigiram o resgate em Bitcoins, moeda virtual. A Polícia Federal foi acionada para solucionar o caso e não foi informado qual foi o valor do pedido de

resgate. A ação não só derrubou o site da Companhia, como também atrapalhou as operações dentro do Porto, que seguiu realizando o trabalho em Mucuripe de forma manual e off-line (BRASIL, 2020).

Para fins de avaliação dos prováveis prejuízos, cabe destacar que o porto movimenta em média 4.400 toneladas de mercadoria por dia. O prejuízo pode ser calculado pelo custo de um navio parado no porto por dia, que fica entre 25 e 60 mil dólares (BRASIL, 2020).

7. A DEFESA CIBERNÉTICA NA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

A proteção de infraestruturas críticas é fundamental para o funcionamento e existência de qualquer Estado, considerando o potencial de dano a ser causado caso uma infraestrutura que seja de vital importância venha a ser impedida de funcionar (BRASIL, 2020).

A proteção de infraestruturas críticas é de responsabilidade do GSI, onde busca-se analisar os riscos e o impacto de ações hostis que possam ser realizadas contra as infraestruturas.

Em relação a esse assunto, o Ministério da Defesa mantém estreita colaboração com o GSI, uma vez que diversas infraestruturas críticas são fundamentais para a Defesa. A interrupção em serviços prestados por tais infraestruturas pode causar sérios impactos nas ações de Defesa, o que torna necessária a participação do MD nas ações de proteção.

Um ataque cibernético que cause degradação nos reatores de uma usina nuclear, por exemplo, pode causar sério impacto ambiental, além de apresentar elevado potencial de dano ao bem-estar da população. Uma situação dessa natureza acarretaria o emprego das Forças Armadas, orientadas pelo Ministério da Defesa, com o intuito de mitigar os danos e proteger os cidadãos.

Um exemplo de ataque cibernético a uma usina nuclear foi o ataque sofrido pelo Irã nas instalações nucleares de Natanz, em 2010, através de um programa de computador, conhecido como “Stuxnet”, cujo efeito foi o aumento de 40% na velocidade de rotação das centrífugas, causando rachaduras nas mesmas (CLARKE, 2015).

Além disso, o “Stuxnet” foi capaz de manter as centrífugas em funcionamento, sendo destruídas, sem que soasse nenhum alarme para os operadores. Tal ação demonstra o potencial de dano de um ataque dessa natureza (CLARKE, 2015).

A característica do ataque acima descrito demonstra a necessidade de atuação colaborativa da Defesa na proteção de infraestruturas críticas, uma vez que o dano causado a

uma dessas instalações pode envolver diretamente o Ministério da Defesa e as Forças Armadas.

7.1 PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

Infraestrutura crítica é um termo usado por governos para descrever ativos e serviços que são essenciais para o funcionamento da sociedade e da economia (BRASIL, 2020).

Em fevereiro de 2008 foi publicada a Portaria nº 2 do GSI, a qual definiu, em seu artigo 2º, infraestrutura crítica como sendo "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional" (BRASIL, 2008).

A infraestrutura crítica é, de forma geral, integrada pelos seguintes setores: sistemas de geração e distribuição de energia elétrica; comunicações e tecnologia da informação; sistema financeiro; transporte; sistemas de captação, armazenamento e distribuição de água; serviços de emergência (médicos, polícia, bombeiros, defesa civil, etc).

Na Era da Informação os ataques em infraestruturas críticas são cibernéticos. A infraestrutura de informações está progressivamente sob ataque de “cibercriminosos”. A quantidade, o custo e a sofisticação dos ataques estão crescendo a taxas alarmantes. Algumas formas infligem, também, uma crescente ameaça às pessoas e infraestruturas nacionais críticas (SOFAER; GOODMAN, 2001).

Os grupos terroristas têm utilizado computadores, a fim de facilitar suas tradicionais formas de atuação. Hackers com motivações políticas ou religiosas, os chamados “hacktivistas”, são recrutados por extremistas. Nesse cenário, surge o terrorismo cibernético ou “ciberterrorismo” (CLARKE, 2015), modalidade de perpetrar o terror, entendida como ataques contra computadores e suas redes, informações armazenadas, serviços essenciais ou infraestrutura, telecomunicações, sistema bancário, fornecimento de água e energia elétrica, usinas nucleares, refinarias de petróleo e outras infraestruturas que impliquem pânico, mortes, acidentes, contaminação ambiental ou perdas econômicas.

O Brasil deve possuir capacidade de proteção contra ataques cibernéticos na suas infraestruturas críticas, aumentando a sua capacidade de resiliência através da estruturação do Setor Cibernético e da interação entre os diversos atores, governamentais ou não, que sejam importantes para o fortalecimento dessa capacidade.

7.2 ATUAÇÃO DA DEFESA CIBERNÉTICA

O Ministério da Defesa possui uma ligação direta com o tema relacionado à proteção de infraestruturas críticas, uma vez que é cliente de muitos serviços e produtos oriundos da indústria para ter sua plena capacidade operativa, bem como, poderá ser acionado para restabelecer a lei e a ordem no caso de ataque cibernético de grande envergadura que comprometa a segurança interna, conforme prevê o Sistema Militar de Defesa Cibernética (BRASIL, 2014).

Em meio a esse ambiente interconectado, de ações no mundo virtual que podem gerar efeitos cinéticos, a atuação colaborativa envolvendo governo, defesa, academia e setor privado, aliada à cooperação internacional, mostra-se como um caminho desejável para garantir a unidade de esforço necessária ao incremento da resiliência cibernética.

A atuação da Defesa Cibernética na proteção de infraestruturas críticas está alinhada com a Política Nacional de Segurança da Informação (PNSI) (BRASIL, 2018) e com a Estratégia Nacional de Segurança Cibernética (ECiber) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) (BRASIL, 2020), as quais preveem a elevação do nível de proteção do Governo e das infraestruturas críticas por meio de ações baseadas na cooperação.

Dentre as ações estratégicas estabelecidas na Estratégia Nacional de Segurança Cibernética podemos destacar:

> 2.3.2. Estabelecer um modelo centralizado de governança no âmbito nacional. Estabelecer um modelo centralizado de governança para o País, por meio da criação de um sistema nacional de segurança cibernética, com as seguintes atribuições: - promover a coordenação dos diversos atores relacionados com a segurança cibernética, além da esfera federal; - promover a análise conjunta dos desafios enfrentados no combate aos crimes cibernéticos; - auxiliar na formulação de políticas públicas; - criar um conselho nacional de segurança cibernética; - criar grupos de debate sobre segurança cibernética, em diferentes setores, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, para fomentar discussões sobre o tema, por meio de mecanismos informais de participação; -estabelecer rotina de verificações de conformidade em segurança cibernética, internamente, nos órgãos públicos e nas entidades privadas; e - permitir a convergência dos esforços e de iniciativas, e atuar de forma complementar para receber denúncias, apurar incidentes e promover a conscientização e a educação da sociedade quanto ao tema. Para viabilizar a sua implementação, ficará a cargo do Gabinete de Segurança Institucional da Presidência da República a coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa.

> 2.3.3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade. Promover um ambiente participativo, colaborativo e seguro, entre as organizações públicas, as instituições privadas, a academia e a sociedade, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos, com o objetivo de: - estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas; - realizar exercícios cibernéticos com participação de múltiplos atores; - estabelecer mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis;- fortalecer o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) e mantê-lo atualizado em pessoal e material; - ressaltar o papel dos Centros de Tratamento e Resposta a Incidentes Cibernéticos (CSIRTs) nacionais; - aperfeiçoar a infraestrutura nacional de investigação de crimes cibernéticos;- incentivar a criação e a atuação de equipe de tratamento e resposta aos incidentes cibernéticos (ETIRs), com ênfase no uso de tecnologias emergentes; - emitir alertas e recomendações; e - estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis (BRASIL, 2020).

Verifica-se, com isso, que a Defesa Cibernética deverá colaborar na proteção de infraestruturas críticas por meio de atuação colaborativa com os demais entes, governamentais ou não, que sejam importantes para a proteção do Setor Cibernético.

8. EXERCÍCIO GUARDIÃO CIBERNÉTICO

O Exercício Guardião Cibernético é considerado um excelente exemplo de cooperação interagências, com o intuito de buscar soluções e treinar o pessoal envolvido na proteção de infraestruturas críticas.

Atualmente conduzido pelo Comando de Defesa Cibernética, tem por finalidade contribuir para o incremento do nível de proteção do espaço cibernético nas infraestruturas críticas de interesse para a Defesa Nacional nos seguintes setores: elétrico, financeiro, nuclear e telecomunicações. Para o cumprimento do seu propósito, foram estabelecidos os seguintes objetivos:

> a) coordenar e integrar, em ambiente interagências, a segurança e defesa cibernéticas para a proteção de infraestruturas críticas;
>
> b) exercitar o processo decisório em diferentes níveis de responsabilidade e de competência, incentivando a atuação colaborativa na prevenção, solução e mitigação de danos causados por ameaças existentes no espaço cibernético;
>
> c) verificar a efetividade de procedimentos para a solução de incidentes em infraestruturas críticas;
>
> d) contribuir para a integração do governo, defesa, comunidade acadêmica e setor privado, por meio de simulações virtual e construtiva, bem como propondo contribuição de normativas;

> e) aplicar boas práticas de proteção cibernética nas ações preventivas e reativas frente a incidentes cibernéticos;
> f) empregar ferramentas para o compartilhamento de informação; e
> g) proporcionar ambiente favorável para que as empresas e organizações simulem incidentes que permitam colher ensinamentos para o aprimoramento de processos e protocolos internos (SILVA, 2019).

O exercício conta com a participação de representantes de diversos setores de interesse para o ecossistema cibernético, conforme descrito a seguir (SILVA, 2019):

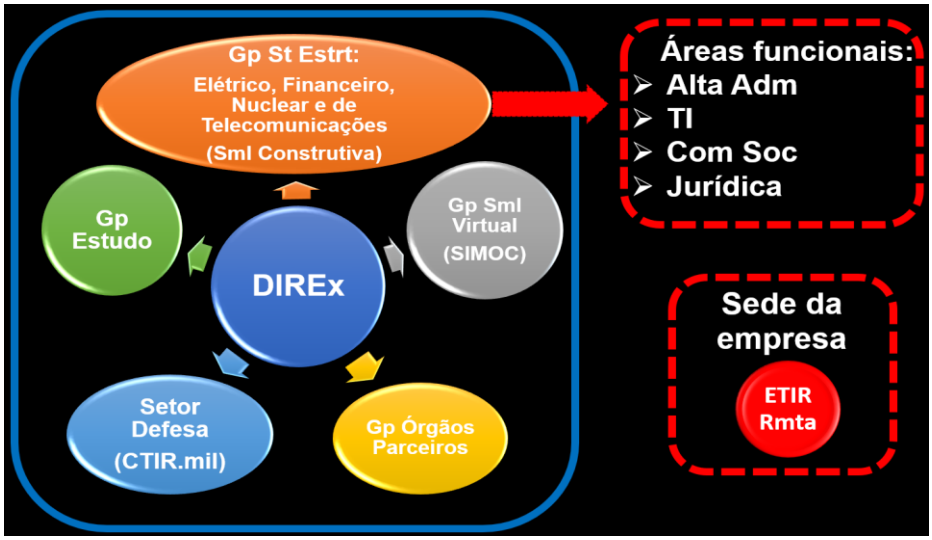
- Defesa;
- Setor Elétrico;
- Setor Financeiro;
- Setor Nuclear;
- Setor de Telecomunicações;
- Órgãos Parceiros;
- Comunidade Acadêmica; e
- Observadores Internacionais.

O Exercício está alinhado com a Política Nacional de Segurança da Informação (PNSI) (BRASIL, 2018) e com a Estratégia Nacional de Segurança Cibernética (ECiber) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) (BRASIL, 2020), as quais preveem a elevação do nível de proteção do governo e das infraestruturas críticas por meio de ações baseadas na cooperação.

Em julho de 2019 foi realizada a segunda edição do Exercício Guardião Cibernético (EGC 2.0), onde houve a participação de 215 representantes de 41 empresas e organizações de interesse para a Defesa no tocante à proteção de infraestruturas críticas (SILVA, 2019).

O EGC adotou técnicas de simulação virtual e construtiva de forma integrada através da simulação virtual com o objetivo de identificar e difundir as melhores práticas das equipes de tratamento de incidentes de rede.

Figura 3: Concepção do EGC



Fonte: SILVA (2019)

O formato adotado no EGC contribui para incrementar a resiliência cibernética, por meio do estímulo à unidade de esforço entre os diversos atores civis e militares que constituem o ecossistema cibernético.

Figura 4: Direção do Exercício Guardião Cibernético 2.0

Fonte: acessado pelo portal <https://ftp.registro.br/pub/gts/gts34/01-ExercicioGuardiao2019.pdf> (14/09/2020)

O EGC tem evoluído ao longo de suas edições, buscando agregar novos atores e reforçar a sinergia entre os envolvidos. O exercício representa a materialização da cooperação e integração entre o Sistema Militar de Defesa Cibernética e a proteção de infraestruturas críticas de interesse para a Defesa Nacional (SILVA, 2019).

Figura 5: Exercício Guardião Cibernético 2.0

Fonte: acessado pelo portal https://agenciabrasil.ebc.com.br/geral/noticia/2019-07/governo- faz-simulacoes-de-ataques-estruturas-estrategicas (14/09/2020)

O conhecimento alcançado através da realização do EGC, nas suas duas versões, deixa clara a importância da simulação virtual para criar o ambiente de crise em situações de ataques às infraestruturas. Os diversos agentes representantes dos setores que englobam as infraestruturas críticas têm, nesse exercício, uma excelente oportunidade de exercitar a pronta resposta dentro de um contexto de crise.

Cabe ressaltar, que o fato de estarem operando no mesmo ambiente favorece a cooperação entre as agências, tendo em vista as situações reais que possam ocorrer no futuro. Dividindo as mesmas preocupações oriundas de problemas similares, os diversos agentes passam a se conhecer e trocar informações, criando o ambiente colaborativo necessário para o desenvolvimento do Setor Cibernético no Brasil.

A proteção cibernética, nos seus diversos níveis, torna-se mais eficaz dentro de um ambiente colaborativo. A troca de experiências favorece o conhecimento das possíveis ameaças, aumentando a capacidade de resposta contra possíveis ataques.

O EGC cria oportunidade para que as pessoas envolvidas com a atividade de proteção cibernética, oriundas das mais diversas instituições, possam se conhecer, facilitando coordenações futuras e diminuindo o tempo de reação frente a ataques cibernéticos.

O Exercício Guardião Cibernético pode ser considerado como o principal exemplo de integração entre os diversos atores, civis e militares, que atuam na proteção do Setor

Cibernético. Por meio de sua execução, é possível verificar que apenas a cooperação e o trabalho em conjunto serão capazes de mitigar as ameaças que se apresentam cada vez mais frequentes no ambiente cibernético.

9. CONSIDERAÇÕES FINAIS

A proteção cibernética de infraestruturas críticas é uma atividade que demanda grande esforço por parte dos entes, governamentais ou não, que atuam na área. A necessidade de manter o funcionamento de tais infraestruturas leva a uma necessária cooperação entre diversas instituições.

A Defesa Cibernética, responsável pela proteção dos ativos no âmbito do MD, também participa da proteção de infraestruturas críticas de interesse da Defesa, pois a interrupção de algum desses serviços essenciais pode causar impacto na Defesa Nacional.

Após o lançamento da Estratégia Nacional de Defesa, em 2008, o Ministério da Defesa definiu o desenvolvimento do Setor Cibernético de Defesa como sendo de responsabilidade do Exército Brasileiro. Cabe ressaltar, que dentro das esferas de responsabilidade na atuação da proteção cibernética, o Gabinete de Segurança Institucional ficou como responsável por conduzir a segurança cibernética dos ativos do governo, abarcando a proteção de infraestruturas críticas.

A partir da evolução do Setor Cibernético de Defesa com a criação do Centro de Defesa Cibernética (2012) e do Comando de Defesa Cibernética (2016), as ações de coordenação com o GSI foram incrementadas, visando a participação da Defesa Cibernética na proteção de infraestruturas críticas.

A atuação colaborativa da Defesa Cibernética com os demais entes, governamentais ou não, mostrou-se favorável para a proteção de infraestruturas críticas, uma vez que tal atividade foge da esfera de responsabilidade do MD, porém é de vital importância para a Defesa.

O maior exemplo dessa atuação colaborativa é o Exercício Guardião Cibernético (EGC), coordenado pelo ComDCiber. Contando com a participação de diversos setores, o EGC deixa claro que apenas a cooperação pode mitigar as ameaças existentes no setor cibernético. A expertise alcançada através da realização do EGC mostra a necessidade de se ampliarem as ações interagências, com o intuito de integrar todos os atores envolvidos na proteção cibernética de infraestruturas críticas.

Como conclusão, verifica-se que a proteção cibernética de infraestruturas críticas é uma atividade fundamental também para a Defesa, demandando atuação colaborativa com os diversos entes envolvidos para que os objetivos de proteção sejam alcançados.

REFERÊNCIAS

BARWISE, MIKE. **What is an internet worm?, 2010**. BBC. Disponível em http://www.bbc.co.uk/webwise/guides/internet-worms. Acesso em 19 de agosto de 2020.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília: Imprensa Nacional, 1988.

BRASIL. Comando de Defesa Cibernética. **Organograma.** Brasília, DF, 2020.

BRASIL. Exército Brasileiro. **EB70 – MC-10.232. Guerra Cibernética.** 1.Ed. Brasília, DF, 2017.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Política Nacional de Segurança da Informação**. Brasília, DF: GSI, 2018.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de Segurança Cibernética**. Disponível em: http://participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca- cibernetica-e-ciber. Acesso em 10 de agosto de 2020.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2018.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília: Ministério da Defesa, 2018.

BRASIL. Ministério da Defesa. **MD31-M-07. Doutrina Militar de Defesa Cibernética.** 1.Ed. Brasília, DF, 2014.

BRASIL. Ministério da Defesa. **MD35-G-01. Glossário das Forças Armadas.** 4.Ed. Brasília, DF, 2007.

BRASIL. Presidência da República. **Política Nacional de Defesa**. Brasília: Ministério da Defesa, 2018.

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

ESCOLA SUPERIOR DE GUERRA (Brasil). **Manual de Procedimentos da Atividade de EnsinoTrabalho de Conclusão de Curso**. Brasília: ESG Campus Brasília, 2019.

EECSP. **Cyber Security in the Energy Sector (2017).** Disponível em <https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf> Acesso em 25 de setembro de 2020.

MARSH e McLENNAN. **Cyber Handbook 2019 da MMC.** Disponível em <file:///C:/Users/Samsung/AppData/Local/Temp/Cyber_Handbook_2019_MMC-1.pdf>. Acesso em 03 de julho de 2020.

SILVA, Walbery Nogueira de Lima e. **Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional.** Brasília, 2019.

SOFAER/GOODMAN. **The Transnational Dimension of Cyber Crime and Terrorism**. United States of America, 2001.