DEFESA CIBERNÉTICA NO BRASIL: PRIMÍCIAS DE UMA HISTÓRIA DE SUCESSO

Eduardo Wallier Vianna*
José Ricardo Souza Camelo**

RESUMO
Este artigo descreve a história da defesa cibernética no Brasil entre os anos de 2008 a 2012, apresentando seu processo de constituição com base na Estratégia Nacional de Defesa. A partir da vivência dos autores em instituições da esfera cibernética, narram-se os eventos relevantes que precederam a implantação da defesa cibernética nacional e as interações com nações amigas, introduzindo o pioneirismo do Centro de Defesa Cibernética no Setor Cibernético brasileiro. O trabalho refere-se, ainda, às principais documentações governamentais vigentes, imbricadas com a segurança e a defesa cibernéticas, bem como discorre, em especial, sobre as motivações, os requisitos fundamentais e os objetos dos projetos originais escolhidos pelo Exército Brasileiro para a construção da defesa cibernética na conjuntura da Defesa Nacional.
Palavras-chave: Defesa Nacional. Estratégia Nacional de Defesa. Setor Cibernético. Defesa Cibernética. Centro de Defesa Cibernética.

CYBER DEFENSE IN BRAZIL: THE BEGINNING OF A SUCCESS STORY

ABSTRACT
This article describes the history of cyber defense in Brazil between the years 2008 to 2012, presenting its constitution process based on the National Defense Strategy. Based on the participatory observation of the authors, it narrates the relevant events that preceded the implantation of national cyber defense and interactions with friendly nations, introducing the pioneering spirit of the Cyber Defense Center in the Brazilian Cyber Sector. The work also refers to the main government regulations in force overlapping with cyber security and defense, as well as discuss

---

* Doutor em Ciência da Informação pela Universidade de Brasília (UnB). Atua nos setores público e privado, principalmente nas áreas de proteção digital e gestão estratégica do conhecimento. Ex-integrante do Núcleo do Centro de Defesa Cibernética e relator do Projeto de criação da Escola Nacional de Defesa Cibernética. No presente, assessora a Procuradoria Geral do Ministério Público do Distrito Federal e territórios nas áreas de segurança e inteligência institucional. Contato: eduardowallier@hotmail.com

** Doutorando em Ciência da Informação pela Universidade de Brasília. Desenvolve pesquisa no campo da Consciência Situacional para Defesa Cibernética. Ex-subchefe do Centro de Defesa Cibernética (CDCiber). Atualmente é professor no curso de Ciência da Computação da Universidade Paulista, campus Brasília. Membro do time original dos elaboradores das diretrizes e dos projetos originais do Setor Cibernético no Exército e, na Defe-sa, é um dos pioneiros do Centro de Defesa Cibernética. Contato: ricardo.camelo@gmail.com

especially about the motivations, the fundamental requirements and the objects of the original projects chosen by the Brazilian Army for the construction of the cyber defense in the context of National Defense.
Keywords: National Defense. National Defense Strategy. Cyber Sector. Cyber Defense. Cyber Defense Center.

DEFENSA CIBERNÉTICA EN BRASIL: EL COMIENZO DE UNA HISTORIA DE ÉXITO

RESUMEN
Este articulo describe la historia de la ciberdefensa en Brasil de 2008 a 2012, presentando su proceso de constitución basado en la Estrategia de Defensa Nacional. Basado en la observación participativa de los autores, narra los eventos relevantes que precedieron a la implementación de la ciberdefensa nacional y las interacciones con las naciones amigas, introduciendo el pionero Centro de Ciberdefensa en el Sector Cibernético Brasileño. El trabajo también se refiere a las principales normas gubernamentales vigentes que están imbricadas con la seguridad y la defensa cibernética, así como discute, en particular, las motivaciones, los requisitos fundamentales y los objetos de los proyectos originales elegidos por el ejército brasileño para la construcción de la ciberdefensa en el contexto de la Defensa Nacional.
Palabras clave: Defensa Nacional. Estrategia de Defensa Nacional. Sector Cibernético. Defensa Cibernética. Centro de Defensa Cibernética.

1 INTRODUÇÃO

O presente trabalho tem por objetivo apresentar uma descrição dos movimentos iniciais de implementação da defesa cibernética no Brasil, ocorridos entre 2008 e 2012.

A defesa do espaço cibernético e a necessidade de segurança da informação no meio digital para o desenvolvimento e soberania de um Estado-Nação são, de *per si*, temáticas emergentes e indissociáveis, de elevada complexidade e alcance global. Ao considerar o espaço cibernético de interesse nacional, em particular no campo da defesa, depara-se com um contexto multifacetado, que abrange a criação e a aplicação de processos políticos, estratégicos, operacionais, administrativos, tecnológicos, capacitação de pessoal, jurídicos, normativos, além de outros.

A característica principal do processo histórico do setor cibernético brasileiro na defesa nacional foi o desenvolvimento acelerado e em campos heterogêneos. Isso se deu pela abrangência setorial da defesa cibernética, estabelecida, no final de 2008, na *Estratégia Nacional de Defesa* (END), assim como pelo contexto do país à época, que precipitou a necessidade da realização de operações cibernéticas reais e complexas.

Partindo da total inexistência de meios e agentes para se colocar em prática o estabelecido na END, um período de pouco mais de três anos se passou entre os primeiros estudos da END e a primeira missão operacional. O Comando do Exército, a partir de meados de 2009, buscou recursos e designou uma equipe de pioneiros, que, além de planejar e iniciar os processos e projetos necessários à formação do setor cibernético, tiveram de organizar e colocar em funcionamento uma estrutura capaz de consolidá-lo, provendo-lhe capacidades que iam desde o nível gerencial até o operacional.

Ao término desse primeiro ciclo, a estrutura criada, denominada na sua fase experimental de Núcleo do Centro de Defesa Cibernética (NuCDCiber), teve a sua primeira missão operacional e de grande criticidade ao coordenar e integrar as principais e mais experientes equipes de segurança cibernética do país na composição da segurança do primeiro grande evento internacional, a Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio+20), em junho de 2012.

De modo a evitar uma única narrativa extensa e complexa, devido, particularmente, à diversidade do histórico e, ao mesmo tempo, da necessidade de compactação e melhor estruturação informacional do seu teor, os autores optaram pelo fracionamento do estudo do setor cibernético nacional, limitando discussões teóricas-conceituais. Assim, sem haver a pretensão de esgotar o tema, neste artigo será abrangido o período que vai desde a publicação da *Estratégia Nacional de Defesa*, em 2008, até 2012, com a consolidação da infraestrutura operacional em defesa cibernética nacional, culminando com a participação na Rio+20, bem como dos primeiros marcos normativos, tais como a publicação da *Política Cibernética de Defesa* pelo Ministério da Defesa e a primeira revisão da END em 2012.

Neste trabalho predomina uma abordagem histórico-descritivo, cujas fontes de pesquisa são majoritariamente primárias. Baseia-se na observação participativa (relato de experiência dos autores), no período de 2008 a 2016, em instituições-chave da defesa cibernética e da segurança da informação, nomeadamente o Centro de Defesa Cibernética (CDCiber) e o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores do Governo Federal (CTIR Gov), tanto no âmbito operacional quanto no gerencial, bem como na função de comandantes, coordenadores ou assessores na quase totalidade das operações militares cibernéticas desenvolvidas pelo Ministério da Defesa. Enriquece o contexto metodológico a análise documental realizada em marcos regulatórios da Administração Pública Federal (APF), diretamente relacionados à defesa cibernética e à segurança da informação.

2 DEFESA E CIBERESPAÇO

O Brasil está inserido nos desafios e oportunidades da era digital, também conhecida como a 4ª Revolução Industrial, que vem causando profundas conse-

quências políticas, econômicas e sociais, devido à maneira peculiar de compartilhar, analisar e processar as informações baseadas na acelerada e irreversível interconectividade global. Os avanços dos meios de comunicação e a inovação tecnológica parecem colocar a sociedade, dita globalizada, com responsabilidades desafiadoras no que tange à segurança das informações. Especialmente, quando se trata das informações[1] inerentes ao contexto do ciberespaço ou espaço cibernético, ou seja, aquelas produzidas e armazenadas nos sistemas de informação automatizados ou que trafegam em redes de dados locais e pela Internet (VIANNA, 2019). No contexto doutrinário da defesa nacional, o espaço cibernético é composto de dispositivos computacionais, conectados em redes ou não, em que as informações digitais transitam e são processadas e/ou armazenadas (BRASIL, 2014).

Como preâmbulo da definição de defesa cibernética, cabe ressaltar que, para fins deste artigo, considera-se a aplicação do conceito de defesa como uma ação episódica, notadamente militar, mas que carece de planejamento e preparação diuturnos, suportados pela sociedade de um Estado-Nação. Ou seja, não é uma sensação adquirida ou um sentimento perceptível, como a segurança, mas um constante "estar em condições de", que exige treinamento e conhecimento das possíveis forças adversas.

Não faz parte do escopo deste trabalho apresentar confrontações e interpretações entre conceituações genéricas de defesa cibernética, uma vez que, para uso das Forças Armadas (FA), está disponível apenas a definição contida na doutrina sobre defesa cibernética brasileira. Dessa forma, no âmbito do Ministério da Defesa, a definição constante da *Doutrina Militar de Defesa Cibernética* (MD31-M-07) estabelece defesa cibernética como sendo

> [...] 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, 2014).

O conjunto das ações que compõem a defesa cibernética possui objetivos distintos, portanto faz-se necessário pontuar as categorias principais. Essas ações podem ser de três naturezas, designadas doutrinariamente, no âmbito da Defesa Nacional, como: proteção cibernética, exploração cibernética e ataque cibernético.

Neste contexto, as ações de proteção cibernética preservam a segurança

1 Os autores consideram informação como um ativo básico para a tomada de decisões, desenvolvimento da sociedade e preservação da soberania nacional.

dos dados digitais que sejam de interesse da defesa nacional, dos respectivos sistemas que os processam e das redes por onde trafegam no espaço cibernético. As ações de exploração cibernética buscam, no ciberespaço, obter informações que provejam consciência situacional e apoio à decisão nos vários níveis de comando e controle das operações cibernéticas. Por fim, as ações de ataque cibernético têm por alvo os sistemas informacionais digitais localizados no espaço cibernético, cujo comprometimento neutralizaria ou degradaria a capacidade ofensiva de um agente ameaçador à soberania nacional (BRASIL, 2014).

3 ANTECEDENTES

Esta seção provê um relato sobre os eventos relevantes, nacionais e globais, que antecederam a formalização e a estruturação da Defesa Cibernética brasileira.

3.1 Instituições Civis Governamentais

Os anos 1990 e início dos anos 2000 foram para grande parte do mundo uma década de perplexidade devido à "explosão" de acessos do grande público à *internet*. Ao mesmo tempo, ocorreu expressiva proliferação de atividades maliciosas nas redes de computadores, cujos implementadores e gerentes priorizavam muito mais a conectividade que a segurança.

Para fazer frente a esse cenário, os padrões de segurança vigentes, com particular destaque para a norma *BS7799-1:1995*, oriunda do governo britânico, passaram a consolidar-se com base em lições aprendidas das equipes técnicas de grandes empresas de tecnologia da informação e de comunicações[2], métodos provenientes da inteligência militar, modelos de referência conhecidos como *frameworks* gerados por pesquisadores, além de atos normativos de organizações governamentais, concebendo uma nova forma de proteção da informação que se tornaria conhecida mundialmente pela terminologia "segurança da informação".

Nesse sentido, a atualização da norma *BS7799*, ocorrida em 1999, foi adotada *ipsis litteris* como padrão internacional, publicada como *ISO/IEC 17799:2000 - Information technology — Code of practice for information security management*. Em 2001, uma versão brasileira foi publicada pela Associação Brasileira de Normas Técnicas (ABNT), a NBR ISO/IEC 17799:2001: *Tecnologia da Informação – Código de prática para gestão da segurança da informação.*

No Brasil, em 1995, uma iniciativa do Ministério de Ciência e Tecnologia e do Ministério das Comunicações criou o Comitê Gestor da *Internet* no Brasil (CGI.br) para coordenar e integrar as iniciativas relacionadas à rede mundial de computado-

2 Neste trabalho, considera-se Segurança da Informação sinônimo de Segurança da Informação e Comunicações (SIC), bem como Tecnologia da Informação (TI) equivalente à Tecnologia da Informação e Comunicações (TIC).

res no país. Entre as atribuições do CGI.br, destacavam-se a promoção de estudos e as recomendações de procedimentos, normas e padrões técnicos e operacionais para a segurança das redes e serviços de *internet*, assim como para a sua crescente e adequada utilização pela sociedade (BRASIL, 1995). Desse modo, o Brasil passou a contar com uma equipe de tratamento de incidentes de rede de credibilidade internacional, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br), criado em 1997, uma peça-chave no suporte às redes do país no tocante à gestão de incidentes de redes de computadores.

Na mesma época, foi criado pela Rede Nacional de Ensino e Pesquisa (RNP) o Centro de Atendimento a Incidentes de Segurança (CAIS), que passou a atuar na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

No âmbito da Administração Pública Federal, as ações relativas à proteção das informações passaram a ter uma referência legal e de nível estratégico com a "Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal", publicada por intermédio do Decreto n. 3505, de 13 de junho de 2000. Em consequência, o Comitê Gestor de Segurança da Informação (CGSI), instituído pelo referido Decreto e coordenado pelo Gabinete de Segurança Institucional (GSIPR), nomeou grupos de trabalho para estudo das diretrizes apontadas na Política, em busca das soluções para sua efetiva implementação e gestão (BRASIL, 2000).

No ano de 2001, deu-se início à implantação do sistema nacional de certificação digital da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), com a edição da Medida Provisória n. 2.200, de 24 de agosto de 2001, elemento vital para realizar transações eletrônicas com garantia de autenticidade de autoria (elemento básico da segurança da informação), uso de criptografia de chaves públicas e validação jurídica dessa modalidade de comunicação. Cabe ao Instituto Nacional de Tecnologia da Informação (ITI) manter, em suas instalações físicas, os Sistemas da ICP-Brasil (BRASIL, 2001).

Outros elementos precursores da defesa cibernética foram concretizados no âmbito da Presidência da República, nomeadamente no GSIPR. O primeiro deles foi a implementação, no ano de 2004, em caráter emergencial, do Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da APF (CTIR Gov), que, em 2009, consagrar-se-ia como a segunda equipe de tratamento de incidentes, brasileira, a atingir credibilidade internacional. Com a finalidade de prosseguir a implantação dos objetivos e diretrizes definidos pelo Decreto Presidencial n. 3.505, foi criado o Núcleo do Departamento de Segurança da Informação e Comunicações, devidamente formalizado como Departamento de Segurança da Informação e Comunicações (DSIC), em 8 de maio de 2006, enquadrando o CTIR Gov em uma das suas três coordenações gerais.

Em 2008, ainda no âmbito do GSIPR, têm-se: (i) a criação da Rede Nacional de Segurança da Informação e Criptografia (RENASIC) , com o objetivo principal

de promover o avanço científico-tecnológico, no país, da segurança da informação, em geral, e da criptografia e da defesa cibernética em particular, integrando as atividades no país de grupos de pesquisa; e (ii) o início da publicação de uma série de normas de segurança da informação, cuja documentação original, a Instrução Normativa 01 (IN 01GSIPR), disciplinou a gestão da informação e comunicações, na Administração Pública Federal (APF) (BRASIL, 2008b).

Ainda no contexto da Administração Pública Federal, o Tribunal de Contas da União (TCU) iniciou, em 2007, a aplicação de levantamentos de governança de Tecnologia da Informação, com o objetivo de avaliar a situação de governança de TI nos órgãos e instituições do poder executivo e afins, permitindo-se mapear diversos problemas e vulnerabilidades inerentes ao ciberespaço da APF.

No fim do ano de 2010, a Secretaria de Assuntos Estratégicos (SAE) da Presidência da República, principal fomentadora da END/2008, organizou a Reunião Técnica sobre Segurança e Defesa Cibernética. O evento foi registrado em uma publicação sob o título *Desafios estratégicos para segurança e defesa cibernética*, o que contribuiu para a conscientização dos integrantes dos órgãos governamentais, além de reforçar o esforço nacional em constituir sua defesa cibernética[3].

3.2 Forças Armadas brasileiras

Com a consolidação da aplicação da Tecnologia da Informação como elemento essencial ao negócio de qualquer grande organização, as Forças Armadas, cujas redes corporativas cruzavam o território continental brasileiro, investiram na adoção das melhores práticas de segurança da informação para seu ambiente computacional. Esse esforço evoluiu lentamente, devido à dimensão da rede e ao seu alto custo, abrangendo desde soluções específicas, tais como uso de criptografia para dados sensíveis, até projetos de segurança e defesa cibernética com base em publicação da END.

Na Marinha do Brasil (MB), entre alguns trabalhos precursores da defesa cibernética, destacaram-se os estudos referentes ao emprego da criptografia, realizados pelo Centro de Análise e Sistemas Navais (CASNAV), em particular, sua participação na especificação dos requisitos do Programa João de Barro, no ano de 2005[4]. Em paralelo, o tema guerra cibernética evoluiu na MB de modo conjunto

3 Informações adicionais sobre a Reunião Técnica. Disponíveis em: http://www.biblioteca.presidencia.gov.br/presidencia/dilma-vana-rousseff/publicacoes/orgao-essenciais/secretaria-de-assuntos-estrategicos/deafios-estrategicos-para-a-seguranca-e-defesa-cibernetica/view. Acesso em: 27 abr. 2020.

4 O objetivo inicial do Programa João de Barro, coordenado pelo ITI, era desenvolver uma nova plataforma criptográfica (módulo de segurança), composta por *hardware* e *software* desenvolvidos com tecnologia nacional para a Autoridade Certificadora Raiz da ICP-Brasil e para os responsáveis pelo gerenciamento dos certificados das Autoridades Certificadoras de primeiro nível.

no seu Comando de Operações Navais (ComOpNav) e nos órgãos técnicos de TI, em particular na Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), reunindo, assim, aspectos operacionais e técnicos. Entre os destaques da época, podem ser relacionados exercícios de guerra cibernética no âmbito das organizações da Marinha do Brasil e a elaboração e aplicação de um conjunto de documentos normativos para disciplinar a segurança da informação no ambiente informacional da instituição.

Na Força Aérea Brasileira (FAB), destacaram-se os estudos realizados pelo Instituto Tecnológico de Aeronáutica (ITA), também na área de criptografia, sendo que, no ano de 2006, igualmente participou do Programa João de Barro do ITI, iniciando o projeto do *hardware.* Não obstante, o estudo do tema guerra cibernética na FAB ganhava especial atenção de especialistas da Força, especialmente no campo da inteligência militar.

No Exército Brasileiro (EB), destacam-se, cronologicamente, as seguintes ações:

a) 2001: publicação das *Instruções Gerais de Segurança da Informação para o Exército Brasileiro*, equivalentes à política de segurança da informação em organizações civis;

b) 2003/2004: instituição da fusão Grupo Finalístico de Segurança da Informação, voltado para a pesquisa, desenvolvimento e fomento para produção de soluções de segurança da informação no âmbito do EB, com início dos trabalhos em 2003 na Secretaria de Ciência e Tecnologia (SCT) e consolidação em 2004, no Departamento de Ciência e Tecnologia (DCT), resultante da fusão da SCT com a Secretaria de Tecnologia da Informação (STI);

c) 2004: publicação da diretriz do Secretário de Tecnologia da Informação sobre segurança da informação e estudos a serem desenvolvidos sobre a guerra cibernética;

d) 2006: implantação de uma estrutura de seções de tratamento de incidentes de redes, equivalentes aos modelos internacionais de "Computer Security Incident Response Teams" (CSIRT) em treze localidades do país, para proteção da intranet corporativa do Exército;

e) 2007: primeiras publicações das normas sobre gestão de riscos, auditoria e segurança para os ambientes de redes do Exército;

f) 2007: ativação do Estágio Setorial de Guerra Cibernética no Centro de Instrução de Guerra Eletrônica (CIGE); e

g) 2009: início da implantação da infraestrutura de chaves públicas do Exército, por meio do projeto do Centro de Desenvolvimento de Sistemas (CDS) e implementação no Centro de Telemática do Exército (CITEx).

No MD, em 2008, foi levantada a possibilidade de ser criado um Grupo de Estudos de Defesa Cibernética no âmbito do Estado-Maior de Defesa. Reuniões preliminares foram realizadas e metas relativas à confecção de manuais de doutrina e

à realização de seminários foram estabelecidas. O trabalho foi descontinuado, provavelmente, devido à edição da END e ao consequente rearranjo das prioridades, em particular no direcionamento da gestão dos setores estratégicos para cada Força. Cabe, no entanto, ressaltar que o esforço propiciou a disseminação do conhecimento sobre o tema e o consequente impulso à conscientização de decisores sobre a relevância da defesa cibernética e a necessidade de sua consolidação na Defesa Nacional.

3.3 Contexto Internacional

Foram inúmeros os eventos governamentais globais a respeito da segurança e da defesa cibernética, refletindo a crescente preocupação mundial sobre os potenciais impactos destrutivos do uso da cibernética como meio para: (i) espionar; (ii) cometer crimes, realizar ações ativistas; (iii) apoiar o terrorismo; e (iv) atos de guerra.

Menos frequentes, mas severamente graves, foram as ações relacionadas a atos de guerra e ataques às infraestruturas críticas (IC)[5]. Relevante é mencionar que tais "atos bélicos" não foram realizados em um contexto de declaração formal de guerra entre países, mas sim por ações contra a soberania de nações, sem que nenhum inimigo, explicitamente declarado, houvesse assumido os ataques, o que, até os dias atuais, é uma característica do emprego ofensivo da cibernética entre nações. Três eventos que alcançaram proporções mundiais e obtiveram notoriedade no período foram os ataques cibernéticos em grande escala, sofridos pela Estônia em 2007, a Guerra da Geórgia em 2008 e, em 2010, a revelação da mais sofisticada das armas cibernéticas descobertas até então, o *worm Stuxnet*.

Especial destaque para a linha histórica teve o ataque contra a Estônia, pois, como consequência imediata e de impacto global, tem-se a criação, em Tallin, do *North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), Centro de Excelência e Cooperação de Defesa Cibernética da Organização do Tratado do Atlântico Norte, com o objetivo de apoiar as nações-membros com competências cibernéticas nas áreas de tecnologia, estratégia, operações e direito.

Entre as ações governamentais de diversos países ocorridas no período, podem-se destacar alguns exemplos, dada a relevância do tema mundialmente:

a) entrada em vigor da Convenção de Budapeste, em 2004, envolvendo um tratado internacional sobre crimes perpetrados pela *internet*;

b) publicação, entre 2005 e 2012, de estratégias nacionais de segurança cibernética de diversos países da Europa, tais como: Estônia, 2005; Finlândia, 2008; Eslováquia, 2008; República Tcheca, 2011; França, 2011; Alemanha, 2011; Lituânia, 2011; Luxemburgo, 2011; Países Baixos, 2011; e Reino Unido, 2011; e

5 Também conhecidas como infraestruturas estratégicas/nacionais, as IC afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (BRASIL, 2015).

c) criação, em junho de 2009, do U.S. Cyber Command (USCyberComm), órgão subordinado ao Comando Estratégico norte-americano, responsável pela coordenação das ações de prevenção e defesa cibernéticas.

Cabe ressaltar que, no período aqui destacado, houve diversos outros eventos e ações de vários governos e organismos internacionais, em especial, no ocidente, sendo registrados neste artigo apenas alguns de relevância e notoriedade que, com maior força, impulsionaram os eventos no Brasil. No oriente, especial destaque tiveram as atuações da Rússia e da República Popular da China. Os chineses, por exemplo, constituíram grupos militares especializados em guerra da informação, com forte emprego da cibernética.

Na conjuntura dos organismos internacionais, ainda que à época não se tivessem obtido avanços sobre aplicação significativamente sentida na esfera da Defesa Nacional, ocorreram discussões nos âmbitos da Organização das Nações Unidas (ONU) por grupo de peritos governamentais com ênfase em crimes e atos terroristas por meios cibernéticos entre 2004 e 2005 e da Organização dos Estados Americanos (OEA) em 2004 - ênfase em crimes cibernéticos e segurança cibernética nos países-membros. Ainda em relação à OEA, entre 2008 e 2011, evidenciam-se as atividades promovidas pelo Comitê Interamericano contra o Terrorismo (CICTE/OEA), objetivando o compartilhamento de melhores práticas sobre segurança cibernética no âmbito da América Latina e Caribe, com destaque para o *Joint* OAS *Hemispheric Workshop Developing a National Framework for Cyber Security*[6], organizado pelo DSIC/CTIR Gov, em 2009.

4 ESTRATÉGIA NACIONAL DE DEFESA - A PEDRA ANGULAR

A *Estratégia Nacional de Defesa* foi publicada por meio do Decreto n. 6703, de 18 de dezembro de 2008, tendo como principal alicerce o reconhecimento de setores considerados estratégicos para a Defesa Nacional e, assim, prover o país de referências a serem seguidas para justificar, priorizar e focar o esforço do desenvolvimento em termos da segurança e da defesa nacionais.

O texto da END estabeleceu uma série de elementos basilares, sobre os quais a estratégia é estruturada. Dentre esses elementos, podem-se citar: (i) princípios de desenvolvimento; (ii) eixos estruturantes; (iii) diretrizes gerais; (iv) objetivos específicos para cada uma das Força Armadas; (v) Setores Estratégicos; (vi) Indústria Nacional de Material de Defesa; e (vii) Serviço Militar Obrigatório (BRASIL, 2008a).

Deste modo, foram estabelecidos três setores estratégicos de defesa: o espacial, o nuclear e o "cibernético". A *Estratégia Nacional de Defesa* não definiu tais setores estratégicos de modo a responder diretamente ao que é cada um deles, limitando-se a discorrer sobre aspectos de relevância, tais como: especificidades

6 Workshop hemisférico de desenvolvimento de uma estrutura nacional para segurança cibernética.

dos setores e interação de uns com os outros. No que se refere à abrangência e à importância do setor cibernético, a END alertou que

> Todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com ênfase sobre [...] o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos;
> O setor cibernético é essencial à defesa do país e as suas capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares;
> As capacitações cibernéticas 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 (BRASIL, 2008a).

A partir da publicação da END, houve diversas mobilizações internas nas Forças Armadas no sentido de assimilar o conteúdo do documento e promover seus desdobramentos práticos. No âmbito do Exército, a principal iniciativa foi a decisão de abordar as demandas da END, no se referisse ao setor cibernético, por uma perspectiva de "projetos".

Em consequência, durante o primeiro semestre de 2009, o Departamento de Ciência e Tecnologia reuniu o primeiro grupo de especialistas do Exército com maior afinidade em relação às temáticas de segurança e guerra cibernéticas, advindos do CITEx, CIGE, CDS e do próprio DCT, sob a supervisão do Estado-Maior do Exército (EME), a fim de apresentarem uma proposta de escopo de projeto ao Ministério da Defesa para implementação do Setor Cibernético no Exército. Dessa forma, a referida proposta viabilizou que o Comando do Exército formalizasse a sua disposição em assumir a gestão do setor cibernético no âmbito da Defesa.

Em novembro de 2009, o MD oficializou a atribuição da condução dos setores para cada uma das Forças. Assim, o Setor Espacial ficou a cargo da Força Aérea, o Setor Nuclear passou a ser gerido pela Marinha do Brasil e o setor cibernético teve por Força líder o Exército Brasileiro. A Diretriz Ministerial n. 0014/2009 – MD estabeleceu, ainda, que cada Força Singular elaborasse uma proposta de ações e diretrizes para cada setor (BRASIL, 2009).

Ao analisar a referida Diretriz, o Estado-Maior do Exército extraiu do seu texto algumas premissas básicas para o setor cibernético, destacando-se

a) capacitar pessoal para as ações de médio e longo prazos;

b) interagir e cooperar com outras áreas governamentais e de pesquisa;

c) realizar os trabalhos, conjuntamente, com representantes do MD e das FA;

d) considerar trabalhos e projetos em andamento e sistemas existentes, realizando intercâmbio de pesquisadores no âmbito do MD;

e) criar ambientes laboratoriais específicos; e

f) considerar que não existem tratados e controles internacionais sobre o tema cibernético.

Ressalta-se, também, a criação de um grupo de trabalho interforças, conduzido pelo DCT e supervisionado pelo EME, com representantes das três Forças Armadas e do MD, a fim de definir os objetivos e ações para a estruturação do setor cibernético.

Ainda em relação ao setor cibernético, o EME ponderou estudar a criação de um centro de coordenação e integração das atividades, concentrando militares das três Forças Armadas em um mesmo ambiente de atuação, assunto a ser tratado na próxima seção.

5 O NÚCLEO DO CENTRO DE DEFESA CIBERNÉTICA

A designação do Exército pelo Ministério da Defesa, como Força responsável pela condução do setor cibernético, teve resultados práticos imediatos, como a decisão de criar uma estrutura administrativa para supervisão dos projetos e assessoramento nas deliberações técnicas e administrativas para o tema.

Em princípio, a linha de ação que parecia mais natural aos envolvidos na elaboração do planejamento original era a formação de um escritório de projetos. A abordagem por projetos na implementação do setor cibernético, por si só, era um fator que impunha essa necessidade. Ao mesmo tempo, no nível estratégico do Exército, os fatores analisados apontavam como premente a necessidade de se criar uma Organização Militar especializada que pudesse tanto gerir as questões técnicas quanto se tornar, no devido tempo, capacitada a responder às demandas operacionais da Defesa no campo cibernético.

A necessidade de se criar uma estrutura que atuasse tanto no nível gerencial quanto no operacional advinha de um outro fator fundamental. Diferente dos Setores Espaciais e Nuclear, cujas especializações técnicas e compartimentalização de fato não prejudicavam sua evolução, o setor cibernético, por definição, necessitava de graus de maturidade semelhantes ou, no mínimo, complementares entre as três Forças. Um desbalanceamento nesses níveis poderia implicar vulnerabilidades graves ao ambiente informacional digital das FA e do MD, com a possibilidade de gerar consequências severas para a estrutura de Defesa.

Assim sendo, um eventual vácuo ou pulverização na condução do setor cibernético poderia gerar desgastes técnicos, operacionais, estratégicos e até políticos na implementação da *Estratégia Nacional de Defesa*. Em consequência, no mês de agosto de 2010, foi ativado, no âmbito do Exército, o Núcleo do Centro de Defesa Cibernética (NuCDCiber), subordinado ao Departamento de Ciência e Tecnologia, como organização experimental e precursora do Centro de Defesa Cibernética.

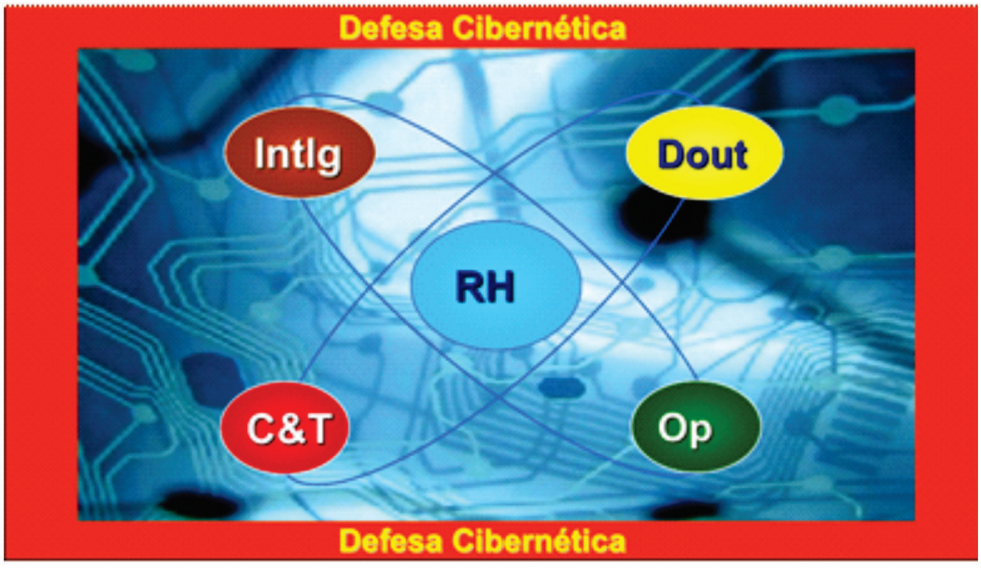
Na criação do NuCDCiber, a diretriz do EME destacava a coordenação das atividades do Setor Cibernético no Exército e a promoção de ações que atendessem o preconizado na Estratégia Nacional de Defesa, com ênfase na atuação em rede e na redução das vulnerabilidades contra ataques cibernéticos.

A ativação do NuCDCiber resultou imediatamente na obtenção de recursos humanos para preencher os cargos necessários, além da designação de um Comandante. O grupo pioneiro de militares, que viriam compor o primeiro time do CDCiber, foi consolidado em várias etapas, contando com pouco mais de dez militares ao final de 2010 e atingindo aproximadamente 25 integrantes em meados de 2011.

5.1 Projetos Estruturantes

Uma das primeiras missões do Núcleo do CDCiber foi elaborar o plano de projeto de defesa cibernética relativo ao escopo enviado ao MD em 2009, qual seja, a sua criação e ativação. Nessa oportunidade, o projeto teve a abrangência atualizada para compor os alicerces do que seria o Setor Cibernético no âmbito do Exército/MD, conforme ilustrado na figura 1.

Figura 1 - Visão sistêmica do Setor Cibernético – Exército Brasileiro /Ministério da Defesa



Fonte: *NÚCLEO DO CENTRO DE DEFESA CIBERNÉTICA, - apresentação oral no ano de 2012.*

Para cumprir o estabelecido na END, o Comando do Exército decidiu, por razões de viabilidade, que o passo inicial para materializar o setor seria realizar

as primeiras entregas do projeto no âmbito do próprio Exército. Essa escolha continha, pelo menos, três pressupostos importantes: (i) todo resultado gerado pelo projeto do Exército, por definição, seria componente da estrutura de Defesa; (ii) como Força líder do setor cibernético e, portanto, pioneiro nas ações a serem efetuadas, o Exército acumularia as preciosas "lições aprendidas" e, assim, expandiria as atividades e projetos para a Defesa e demais Forças com maior maturidade; e (iii) durante a evolução do setor, um permanente diálogo com as demais Forças e o MD sobre as principais atividades e decisões seria realizado por intermédio de um grupo de trabalho, que foi designado como GT interforças.

Inicialmente, convém esclarecer o motivo de todo o trabalho inicial ter sido voltado para uma abordagem de projeto. Houve, fundamentalmente, duas razões para tal. Primeiro, todo e qualquer trabalho para edificar as fundações do setor cibernético, um campo novo do combate em todo o mundo, destinava-se à produção de novos produtos, o que, por si só, já requeria um tratamento por projeto. Segundo, havia no Ministério da Defesa, em consolidação e aplicação, uma cultura de priorizar propostas advindas das Forças que tivessem um formato de projeto, de tal modo que elementos como viabilidade, orçamento, objeto e cronograma fossem mais facilmente avaliáveis.

Por diversas razões relacionadas, principalmente, aos prazos exíguos e às injunções políticas-estratégicas, oriundas do governo federal, impostos à época, não foi possível elaborar formalmente os requisitos operacionais que balizariam os projetos, permanecendo esses apenas de modo tácito entre os membros da equipe de elaboradores. Na prática, as atividades necessárias para que esses requisitos fossem satisfeitos foram consolidadas diretamente no corpo dos documentos derivados dos projetos.

Nesta seção, considerada a ausência de registros a respeito, este trabalho apresenta o esforço inédito de agregar, ao histórico da Defesa Cibernética brasileira, o registro dos três "requisitos fundamentais" que nortearam a construção do setor cibernético, assim como os diversos "porquês" da escolha dos objetos de cada um dos projetos que se tornaram as colunas de sustentação da construção original do Setor Cibernético da Defesa Nacional.

O primeiro requisito fundamental levantado foi: o setor cibernético deve ser materializado por uma estrutura que proveja capacidade operacional à Defesa Nacional nesse setor. Esse requisito depreendia-se diretamente da END, uma vez que o setor cibernético não existia como tal e foi definido como prioritário na Defesa.

O segundo requisito fundamental identificado foi: a efetivação do setor cibernético deve considerar os trabalhos já existentes no Exército ligados ao campo cibernético. Esse requisito era derivado do primeiro e explicitava o re-

conhecimento de que era necessário identificar e organizar o legado relativo à cibernética existente no Exército como ponto de partida da constituição do setor. Isso possibilitou a racionalização de recursos e fundamentou decisões baseadas no conhecimento já adquirido, indo ao encontro da premência imposta pela natureza tempestiva da área cibernética. Como exemplos desse legado, citam-se

a) os trabalhos de segurança cibernética desempenhados na proteção da rede corporativa pelo CITEx;

b) os projetos de segurança da informação implementados pelo CDS;

c) o esforço de pesquisa e formação desenvolvido no CIGE em guerra cibernética, com destaque para o Núcleo Protheus e o Estágio Setorial de 2007;

d) as pesquisas científicas fomentadas pelo Grupo Finalístico de Segurança da Informação do DCT, realizadas majoritariamente no Instituto Militar de Engenharia (IME) e gerenciadas pelo CDS;

e) os esforços realizados no setor de Inteligência da Força para tornar a fonte cibernética em mais uma fonte de conhecimento; e

f) os trabalhos realizados na Assessoria de Tecnologia da Informação do DCT, relativos à elaboração de normas técnicas de segurança da informação, à representação em projetos e aos trabalhos conjuntos com as demais Forças Armadas e MD ou outros ministérios e a Presidência da República, além da supervisão das ações realizadas nas áreas supracitadas.

Derivado dos dois primeiros, o terceiro requisito fundamental discernido: a constituição do Setor Cibernético no Exército Brasileiro deverá ser implantada por meio de uma abordagem de projetos, tendo por objetos os temas prioritários que refletissem as boas práticas mundiais, as recomendações da Estratégia Nacional de Defesa (END) e o legado de cibernética no Exército. Sendo o tema da cibernética uma nova perspectiva da Defesa brasileira e distinta da segurança cibernética já praticada pelos especialistas da instituição, era necessário identificar as boas práticas para a defesa cibernética, o que foi possível pelos trabalhos correntes no Exército, listados na descrição do segundo requisito fundamental, indo ao encontro do legado existente na época[7].

A partir dos três requisitos fundamentais, passou a ser clara a necessidade de que os produtos dos projetos originais deveriam se complementar mutuamente, contribuindo para que três objetivos fossem atingidos: (i) potencializar

7 Cabe reforçar que as informações sobre os três requisitos fundamentais são advindas da experiência dos pesquisadores em instituições nacionais envolvidas com o ciberespaço.

a capacidade de proteção das redes corporativas; (ii) proporcionar capacidade ofensiva e, assim, agregar valor à atividade-fim das Forças Armadas; e (iii) proporcionar capacidade de consciência situacional, apoio à decisão e contrainteligência no espaço cibernético de interesse. Posteriormente, no alinhamento com a *Doutrina Militar de Defesa Cibernética*, os três objetivos citados seriam cobertos, respectivamente, pelas ações de proteção, ataque e exploração cibernéticas.

Arquitetou-se, então, uma proposta de estruturação do setor cibernético, inicialmente contemplando seis áreas que viriam a se tornar os objetos dos projetos originais:

a) normas e doutrina;

b) segurança cibernética;

c) aplicação de soluções tecnológicas de curto prazo;

d) pesquisa científica;

e) guerra cibernética; e

f) recursos humanos.

Cabe destacar-se que a estruturação do "portfólio" de projetos propostos, com o amadurecimento dos trabalhos, evoluiu de modo a agregar novos projetos ou mesmo desmembrar outros existentes. Por exemplo, a área "guerra cibernética" foi desdobrada em formação de pessoal com capacidades de guerra cibernética (capacitações específicas da área) e Inteligência, gerando, em marcos históricos posteriores, os projetos "Capacitação, Preparo e Emprego Operacional" e "Inteligência Cibernética", respectivamente.

Outro exemplo, não contemplado nas áreas primordiais, foi a criação de uma Organização Militar (o futuro CDCiber) especificamente voltada para a ação cibernética. Embora, hoje, possa parecer óbvia essa necessidade, naquele tempo, ainda havia dúvidas quanto criar uma organização nova ou aproveitar uma já existente, além de dificuldades administrativas e de recursos financeiros para colocar a cabo tal intento.

Neste ponto, resta clarificar o porquê da escolha de cada área ou, de modo equivalente, que contribuição operacional cada uma delas poderia trazer, recordando que todas as áreas (e seus projetos) deveriam convergir para o primeiro requisito fundamental e serem compatíveis e alinhadas com os dois decorrentes. O quadro 01 representa as áreas originais que deram origem aos primeiros projetos e seus porquês, ou seja, a contribuição operacional esperada.

Quadro 01 - Contribuição operacional dos projetos originais

ÁREAS ORIGINAIS	PROJETO ORIGINAL	CONTRIBUIÇÃO OPERACIONAL (PORQUÊS)
Normas e Doutrina	Projeto Arcabouço Documental	Normas**:** servir de referência para implementar e aferir a segurança cibernética nas redes do Exército. Doutrina**:** servir como referência primordial para preparo, emprego, geração de lições aprendidas e manutenção das capacidades operacionais a serem desenvolvidas.
Segurança Cibernética	Projeto Defesa Cibernética (Escudo Cibernético)	Necessidade de mapeamento e minimização da superfície de ataque às redes corporativas do Exército, protegendo toda a informação sensível, de caráter administrativo ou operacional, nos sistemas digitais e redes corporativos da Força.
Aplicação de soluções tecnológicas de curto prazo	Apoio Tecnológico	Prover ferramentas cibernéticas conhecidas à atividade operacional, passíveis de aquisição, integração ou adaptação para emprego em curto e médio prazos (em relação à criação do setor cibernético na Força).
Pesquisa Científica	Pesquisa Científica	Prover à atividade operacional ferramentas cibernéticas de alta complexidade e majoritariamente de desenvolvimento próprio, por envolver campos sensíveis e negados por outras nações, para emprego em médio e longo prazos.
Guerra Cibernética	Núcleo Experimental de Guerra Cibernética (Preparo e Emprego Operacional)	Desenvolver as capacidades operacionais necessárias para realizar atividades de ataques e exploração cibernéticas
Recursos Humanos	Gestão de Pessoal	Descobrir, fomentar, atrair, capacitar e manter talentos para atuação no campo operacional.

Fonte*: O AUTOR, 2020.*

Após a complementação do escopo inicial com o acréscimo do plano de projeto, o Projeto de implementação do setor cibernético passou a alicerçar-se em oito

áreas, constituindo-se, cada uma, em um projeto[8] específico. O quadro 02 sintetiza os objetivos, as justificativas e o gestor de cada projeto, refletindo o proposto pela Força Terrestre ao Ministério da Defesa.

Quadro 02 - Projetos de implementação do setor cibernético

PROJETO	OBJETIVO	JUSTIFICATIVA	GESTOR ORIGINAL
Arcabouço Documental	Elaborar o primeiro conjunto de documentos conceituais, normativos e doutrinários necessários para guiar e regular o emprego do setor cibernético no EB/ MD, bem como definir e implementar o processo de gestão do conhecimento.	Estabelecer um primeiro grupo de referências que esclarecesse ao público interno o que era o setor cibernético (conceitos), como deveria ser gerenciado, em particular no aspecto da segurança da informação (normas), como deveria agregar valor ao poder de combate da Força (doutrina) e como acompanhar, promover e atualizar a aplicação do conhecimento gerado (gestão do conhecimento).	Núcleo do Cen-tro de Defesa Cibernética
Pesquisa Científica	Instituir a pesquisa sobre defesa cibernética, organizando as condições necessárias para iniciar e manter as investigações científicas de interesse do setor cibernético.	Existência de temas de extrema importância e complexidade no âmbito da defesa cibernética, como, por exemplo, a criptologia ou a supercomputação, cujo domínio, em geral, não é compartilhado por quem o detém, além do fato de que esses tipos de estudos serem de longo prazo.	Instituto Militar de Engenharia

8 Em consonância com a Diretriz de Implantação do Setor Cibernético no EB, de 22 de junho de 2010, expedida pelo Comando do Exército. As terminologias usadas para designar cada área, seja nas suas versões originais ou nas suas variantes adotadas no decorrer das atualizações do projeto, foram omitidas aqui por mera simplificação do relato, assim como para que fossem usadas expressões de apreensão mais simples pelo leitor.

PROJETO	OBJETIVO	JUSTIFICATIVA	GESTOR ORIGINAL
Gestão de Pessoal	Identificar, selecionar, capacitar e manter os talentos que desenvolveriam a sua carreira no setor cibernético.	Os profissionais de defesa cibernética tinham de ser recrutados com critérios muito específicos, que variavam desde aspectos gerenciais relacionados à carreira até aspectos subjetivos relacionados ao pendor para área, sendo este fator especialmente crítico no nível operacional.	Núcleo do Cen-tro de Defesa Cibernética
Defesa Cibernética	Atualizar e adequar toda a estrutura de segurança da rede corporativa do Exército (EBNet).	A rede corporativa do Exército, assim como ocorre com as demais FA, é uma infraestrutura crítica para a manutenção do poder de combate da Força. Além disso, à época, havia sistemas ainda não adequadamente protegidos, causando, assim, vulnerabilidades diversas.	Centro de Telemática do Exército
Núcleo Experimental de Guerra Cibernética	Formação e emprego, em caráter experimental, de célula operacional de guerra cibernética.	Iniciar o desenvolvimento da capacidade de guerra cibernética em curto prazo, uma vez que, à época, tinha-se poucas fontes para capacitação e o seu exercício, em operações reais, demandava um amadurecimento muito expressivo e confiável.	Núcleo do Cen-tro de Defesa Cibernética

PROJETO	OBJETIVO	JUSTIFICATIVA	GESTOR ORIGINAL
Inteligência Cibernética	Adequar e atualizar a doutrina e os procedimentos de Inteligência, abrangendo a defesa cibernética, bem como estruturar a produção de conhecimento oriundo da fonte cibernética.	A atividade de Inteligência é elemento fundamental na consciência situacional e na tomada de decisão dos comandantes envolvidos, seja em operações ou na atividade do dia-a-dia, devendo estar capacitada para, sistematicamente, ser capaz de usar da fonte cibernética para alimentar seus processos e atividades.	Núcleo do Centro de Defesa Cibernética
Apoio Tecnológico	Prover soluções tecnológicas de cibernética viabilizadas em curto e médio prazo para emprego operacional.	Necessidade de contar com uma estrutura de avaliação a respeito de possíveis adoções, integrações, adaptações ou, até mesmo da criação de soluções de defesa cibernética a partir de conhecimentos e ferramentas existentes na área.	Centro de Desenvolvimento de Sistemas
Construção do CDCiber	Prover um local adequadamente construído e organizado para abrigar o CDCiber.	Necessidade de uma estrutura física capaz de suportar as atividades operacionais, normativas e administrativas do Centro de Defesa Cibernética.	Núcleo do Centro de Defesa Cibernética

Fonte*: O AUTOR, 2020.*

O "portfólio" dos projetos de implementação do setor cibernético recebeu, em 2011, o reforço da Rede Nacional de Segurança da Informação e Criptografia, oriunda do GSIPR. De acordo com Vianna (2019), o Projeto RENASIC era composto de dez subprojetos ou áreas de atuação, gerenciados por um Laboratório Virtual:

a) VIRTUS - Técnicas Simétricas - Criação de um sistema de criptoanálise nacional e de ferramentas para a proteção de sistemas móveis;

b) ASTECA - Técnicas Assimétricas - Desenvolvimento de um produto de segurança corporativa;

c) PROTO – Protocolos Criptográficos Seguros – Desenvolvimento de sistemas de criptografia por chave única;

d) LATIM – Implementações Seguras - Desenvolvimento de um sistema de gestão de identidades e outro de defesa contra ataques laterais;

e) LAPAD - acesso ao processamento de alto desempenho à comunidade científica nacional;

f) QUANTA - Computação, Informação e Criptografia Quânticas;

g) LAPROJ - Acompanhamento de Projetos e Desenvolvimento de componente básico (*hardware*) do Sistema KeyBITS;

h) LABIN – Inteligência de Redes – Análise do tráfego de redes e proteção de pacotes sigilosos;

i) SALTAR - Sistema de Análise de Link e Tráfego de Dados em Redes de Comunicações; e

j) LASEC2 – Desenvolvimento de ferramentas para Segurança Eletrônica, de Comunicações e Cibernética. (VIANNA, 2019, p. 159).

Cabe ressaltar que, à época da elaboração deste artigo, os projetos ainda estavam em execução e títulos, objetivos e alguns outros elementos sofreram atualizações diversas. Essas adequações foram realizadas de modo a refletir a realidade corrente, uma vez que o contexto de execução do projeto passou por mudanças muito expressivas em praticamente todas as áreas, desde limitações orçamentárias até eventos de âmbito internacional, como, por exemplo, o escândalo Snowden[9].

5.2 Atividades desenvolvidas

O período entre os anos de 2009 a 2011 abrangeu atividades de impacto significativo para a construção do setor cibernético brasileiro. Entre elas, destacam-se:

a) participação de comitiva de oficiais do Exército Brasileiro no Cyber Security for National Defense Summit 2009, nos EUA;

9 Esclarecimentos complementares sobre o 'caso Snowden' podem ser encontrados na Revista do Senado Federal - Em Discussão! Disponível em: http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/. Acesso em: 22 abr. 2020.

b) realização de um encontro para intercâmbio de informações sobre cibernética, entre representantes do Ministério da Defesa brasileiro e dos EUA, em Washington, 2010;

c) realização do I Seminário Internacional de Defesa Cibernética, em 2010;

d) visita à República Popular da China para entendimentos sobre segurança da informação;

e) envio de observador para a Operação Amazônia 2011, do MD; e

f) realização de duas Jornadas de Trabalho de Defesa Cibernética, em 2011.

5.2.1 Participação no Cyber Security for National Defense Summit 2009

O simpósio Cyber Security for National Defense - SUMMIT 2009 e os *workshops* concomitantes ("Information Assurance" e "Information Security Management") poderiam ter representado apenas mais um evento com palestras e cursos de teor tecnicamente relevantes, com algumas oportunidades de *networking*, como ocorre com a maioria desses eventos. No entanto esse simpósio em particular teve pelo menos duas características-chave para a construção do setor cibernético brasileiro.

A primeira característica foi o fato de que o encontro, embora aberto mundialmente para inscrições, reunia poucas dezenas de pessoas e, excetuada a equipe dos oficiais brasileiros, era composta por estadunidenses representantes de diversos setores do governo dos EUA. Em consequência, a abordagem dos palestrantes e participantes era muito aberta no tocante a problemas causados por ações cibernéticas nas redes norte-americanas. Foram abordados temas relativamente sensíveis, tais como: (i) ataques à infraestrutura crítica de energia elétrica, considerando como suposição mais provável a autoria chinesa; (ii) desenvolvimentos científicos sensíveis, que demandavam cidadãos estadunidenses natos para manuseio dos sistemas, mas que, segundo o professor chefe da equipe de pesquisa e palestrante, contavam na maior parte com mão de obra estrangeira, em particular de origem indiana e chinesa; e (iii) capacitação de pessoal, apresentando-se estimativas de recursos financeiros e quantitativo de pessoal para trabalhar na área. Tal abordagem, até certo ponto transparente, das dificuldades dos EUA para construirem seu equivalente do nosso setor cibernético, serviu como importante referência à equipe brasileira, toda ela composta por integrantes do grupo original que especificara os projetos seminais e que se tornariam supervisores de alguns desses projetos.

A segunda característica, provavelmente a mais importante do SUMMIT 2009, foi a grande semelhança das áreas prioritárias para construção das capacidades cibernéticas nos EUA, expostas nas palestras com as escolhas equivalentes brasileiras já estabelecidas no escopo de projeto enviado ao MD. Todas, sem exceção, encontravam correspondentes nos projetos brasileiros para construção do setor cibernético nacional, do arcabouço documental até a existência de uma estrutura de defesa que comandasse os esforços.

Cabe ressaltar que não se está afirmando, aqui, que os desenvolvimentos dos EUA e os projetos brasileiros eram semelhantes em forma, mas nos seus fins, ressalvadas as devidas proporções no tocante a orçamento, número de agências envolvidas, quantitativo de pessoal empregado etc. Considerado o fato de que a estrutura de defesa dos EUA é constantemente empregada e testada, a constatação das semelhanças observadas pela equipe reforçou a convicção da pertinência das escolhas iniciais que serviriam de alicerces e pontos de partida para os trabalhos no Brasil.

Importante destacar que o projeto brasileiro foi estruturado sem que houvesse nenhum modelo disponível de outro país para servir de ponto de partida e ser objeto de adaptação. Ao contrário, para que se materializasse a concepção dos alicerces do desenvolvimento brasileiro, foi preciso juntar referências diversas e, muitas vezes, dispersas e desconectadas, no Brasil e em outros países, fossem acadêmicas ou de lições aprendidas, experiências pessoais dos poucos especialistas na Força, além da necessária aderência à realidade da Defesa Nacional.

5.2.2 Intercâmbio de informações sobre cibernética nos EUA

No ano de 2010, o encontro para intercâmbio de informações sobre cibernética entre o Ministério da Defesa brasileiro e o *Department of Defense* dos EUA (US DoD) teve grande relevância no tocante a conhecer os pontos não classificados da estratégia do DoD para cibernética. Nessa estratégia, destacavam-se cinco pilares: (i) ciberespaço como um domínio; (ii) o combate no espaço cibernético, implicando novos conceitos operacionais no campo da defesa; (iii) extensão da defesa cibernética aos órgãos de governo e parte do setor privado, em especial as infraestruturas críticas; (iv) parcerias internacionais, tecnologia e inovação; e (v) a P, D&I na área de ciência e tecnologia sendo prioridades para o setor cibernético.

Outro ponto importante da missão foi a visita ao *Department of Homeland Security* (US DHS), quando se pôde interagir com a equipe do US-Cert (*United States Computer Emergency Response Team*), principal CSIRT do governo dos EUA à época, e ter ideia das dificuldades de avançar com um programa de conscientização extensivo às áreas governamentais civis sobre o tema. Ainda no DHS, houve uma videoconferência com o CCIRC (*Canadian Cyber Incident Response Centre*), principal CSIRT Canadense, por meio da qual foi transmitida uma palestra sobre lições aprendidas nos Jogos de Inverno de Vancouver. Também houve uma visita ao *Department of Cyber Crime Center* (DC3), onde se observaram trabalhos de perícia forense e áreas de capacitação técnica de pessoal. Outro ponto de destaque foi a visita à *National Defense University* (NDU), onde a delegação brasileira conheceu laboratórios e propostas de formação acadêmica para a área de defesa cibernética.

5.2.3 Realização do I Seminário Internacional de Defesa Cibernética

O I Seminário sobre defesa cibernética do Ministério da Defesa, realizado no período de 21 a 24 de junho de 2010, foi desenvolvido em dois momentos. O primeiro de caráter político-estratégico, com palestras e participação de setores públicos e privados relacionados particularmente às infraestruturas críticas, à comunidade acadêmica e ao MD. O segundo voltado especificamente à área militar, tratando da situação do setor cibernético nas Forças Armadas, bem como debatendo sobre os temas: pessoal, doutrina, estruturas e tecnologia. Com base nessas discussões, foi gerada uma "nota de coordenação doutrinária", documento interno ao Exército que serviu como uma das referências para implantação do setor cibernético.

5.2.4 Visita de comitiva à República Popular da China

A visita à República Popular da China, em 2010, teve por objetivo intensificar o intercâmbio bilateral para consultas nas áreas de segurança do espaço informacional, em 2010, contando com a participação de um membro da equipe original, que especificou o setor cibernético brasileiro e que supervisionou um dos seus projetos. A principal contribuição para o setor cibernético brasileiro foi o conhecimento, ainda que ocorrido com restrições, da forma de gestão da segurança da informação exercida pelo governo chinês, uma vez que a visita cobriu as áreas de gestão de nível governamental, pesquisa e desenvolvimento, infraestrutura de TI, indústria de segurança da informação e formação de especialistas.

5.2.5 Envio de observador para a Operação Amazônia 2011

Em 2011, ainda durante os trabalhos de constituição do Centro de Defesa Cibernética, o NuCDCiber enviou um observador para analisar e avaliar como, em operações futuras, equipes de defesa cibernética poderiam tomar parte para agregar valor às atividades de combate simulado e estar em condições adequadas para um emprego real. A partir de 2012, o CDCiber pôde integrar de forma permanente os exercícios de adestramento do MD, nos quais, segundo a metodologia empregada à época, buscava-se testar tanto a capacidade do Estado-Maior Conjunto em tomar decisões, diante de situações simuladas de conflito, quanto da tropa no terreno em realizar operações o mais próximo de uma situação real.

5.2.6 Jornadas de Trabalho de Defesa Cibernética

No segundo semestre de 2011, destaca-se a realização de duas jornadas de trabalho, respectivamente em julho e setembro de 2011. Organizadas pelo Exército Brasileiro/MD e pela Secretaria de Política de Informática/MCTI, as jornadas con-

taram com ampla participação dos órgãos da Administração Pública Federal (APF), da comunidade acadêmica, bem como de entidades/empresas envolvidas com a segurança das informações em meio digital. A primeira jornada recebeu tamanha relevância por parte das autoridades governamentais que, em sua abertura, compareceu o então Ministro da Ciência, Tecnologia e Inovação, o qual não só enalteceu retoricamente o evento, mas realçou a intenção do Ministério em investir recursos nos trabalhos do setor. Entre as premissas norteadoras das jornadas, elencavam-se

a) contemplar multidisciplinaridade e a dualidade das aplicações;

b) fomentar a indústria nacional de Defesa;

c) induzir a indústria nacional a produzir sistemas inovadores; e

d) produzir componentes críticos nacionalmente.

Como resultado das jornadas, estruturaram-se quatro programas de trabalho: (i) Sistema Modular de soluções de TI; (ii) Supercomputação (computação de alto desempenho - CAD); (iii) Escola Nacional de Defesa Cibernética (ENaDCiber); e (iv) Sistema de Proteção (segurança em ambientes computacionais).

Em paralelo com algumas das atividades citadas anteriormente, o Núcleo de Centro de Defesa Cibernética, a partir do segundo semestre de 2011, iniciou os preparativos administrativos e operacionais para que a equipe de defesa cibernética das Forças Armadas compusesse, em junho de 2012, a segurança cibernética da Rio +20. Nessa nova conjuntura de atuação, foram realizadas reuniões preparatórias para a configuração da Central de Monitoramento Cibernético/CDCiber com o Comitê Nacional de Organização (CNO/Rio+20) e demais parceiros externos.

5.3 Arcabouço normativo - consolidação inicial

Coube, ainda, ao Núcleo do CDCiber participar ativamente da concepção de uma política do Ministério da Defesa para o emergente e incipiente setor cibernético.

Em consequência, por intermédio da Portaria n. 3389/MD, de 21 de dezembro de 2012, foi publicada a *Política Cibernética de Defesa* (PCD/MD), com a finalidade de orientar as atividades de defesa cibernética, no nível estratégico e de guerra cibernética, nos níveis operacional e tático. Entre seus pressupostos básicos, destacam-se

a) A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa;

b) As atividades de Defesa Cibernética no MD são orientadas para atender as necessidades da Defesa Nacional;

c) As ações cibernéticas de caráter ofensivo deverão estar em conformidade com o planejamento elaborado em atendimento às Hipóteses de Emprego (HE);

d) A capacitação tecnológica do setor cibernético deve ser buscada de maneira harmônica com a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional (C, T&I);

e) A eficácia das ações de Defesa Cibernética no MD depende, diretamente, do grau de conscientização alcançado junto às organizações e pessoas, acerca do valor da informação que detêm ou processam;

f) A Segurança da Informação e Comunicações é a base da Defesa Cibernética e depende diretamente das ações individuais [...]; e

g) As ações cibernéticas, no contexto do MD, visam a assegurar o uso do espaço cibernético, impedindo ou dificultando seu uso contra os interesses do País e garantindo, dessa forma, a liberdade de ação (BRASIL, 2012).

A PCD/MD estabeleceu nove objetivos principais, cada qual desdobrado em uma série de diretrizes que orientavam suas realizações. Como síntese da Política Cibernética de Defesa destacaram-se: (i) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da Defesa Nacional; (ii) capacitar e gerir talentos humanos necessários à condução das atividades do setor cibernético no âmbito do MD; e (iii) definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no setor cibernético.

Importante ressaltar que, até o surgimento da *Doutrina Militar de Defesa Cibernética*, em novembro de 2014, a *Política Cibernética de Defesa* foi a única referência normativa específica de defesa cibernética para orientar ações do setor.

6 CONSIDERAÇÕES FINAIS

O panorama da segurança cibernética mundial provoca mudanças urgentes na forma de pensar a defesa de um Estado-Nação, com destaque para as necessárias mudanças de paradigmas advindas da inserção da dimensão cibernética no campo de batalha.

Este artigo buscou "mapear os principais movimentos" nacionais (Forças Armadas e Instituições civis) que contribuíram para o desenvolvimento do setor cibernético no Brasil, a partir da *Estratégia Nacional de Defesa*. A END, de 2008, fomentou a discussão sobre a inexorável necessidade de se estruturar, no Brasil, a defesa do espaço cibernético de interesse nacional, reconhecendo as potencialidades da cibernética e a forte tendência desse novo ramo do combate de se tornar um elemento decisivo no campo de batalha.

As estratégias e medidas adotadas no âmbito do Ministério da Defesa e operacionalizadas pelas Forças Armadas, lideradas pelo Exército Brasileiro, propiciaram a evolução e o incremento substancial da segurança no setor cibernético nacional.

Para guiar esse esforço, foram levados em conta requisitos nas áreas de: (i) operações militares e interagências; (ii) boas práticas de segurança da informação nacionais e internacionais; (iii) capacitação; (iv) inteligência; (v) ciência e tecnologia; (vi) acordos ou entendimentos com nações amigas ou órgãos internacionais na área de segurança cibernética; e (vii) lições aprendidas nas Forças Armadas no campo cibernético.

A operacionalização das diretrizes da defesa brasileira, para construção do setor cibernético, foi possível em curto prazo devido, particularmente, à ocorrência de cinco fatores primordiais:

a) a priorização "de fato" do Setor dada pelas autoridades envolvidas, em particular o Comandante do Exército à época;

b) o capital intelectual existente nas três Forças Armadas brasileiras, composto, em especial, por pessoal técnico especializado em segurança cibernética;

c) as estruturas já existentes com atribuições de segurança da informação voltadas para a proteção das redes corporativas das Forças e que se encontravam em expansão;

d) a crescente sinergia nas atividades de proteção cibernética, em especial advinda de trabalhos conjuntos interforças e interagências; e

e) a expressiva onda global que demandava, de forma explícita e urgente, a reação dos países no que se referia às suas próprias seguranças cibernéticas, bem como ao desenvolvimento de capacidades de defesa cibernética para preservação de suas soberanias.

A inclusão definitiva da defesa cibernética como nova dimensão de combate na Defesa Nacional impõe desafios diuturnos e complexos ao Ministério da Defesa.

O Centro de Defesa Cibernética, unidade precursora da defesa cibernética brasileira, prossegue no desenvolvimento dos seus projetos e ações operacionais. Atualmente, integra o Comando de Defesa Cibernética e dispõe do suporte acadêmico da Escola Nacional de Defesa Cibernética, ativados em 2016 e 2019, respectivamente.

Aos fatores primordiais abordados neste trabalho, seguiram-se as demandas em segurança cibernética impostas ao Brasil, como, por exemplo, a sequência dos grandes eventos internacionais ocorridos no país, iniciados em 2012 com a Rio+20 até os Jogos Olímpicos, em 2016.

Nesse contexto, devido a sua complexidade e diversidade de ações, os grandes eventos, a criação de organizações imbricadas com a defesa cibernética no país, entre outras ações e atividades cibernéticas realizadas no âmbito do MD, devem ter sua narrativa específica, documentada em trabalhos futuros similares a este.

REFERÊNCIAS

BRASIL. *Decreto n. 3.505, de 13 de junho de 2000.* Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF: Presidência da República, 2000.

BRASIL. *Decreto n. 6.703, de 18 de dezembro de 2008.* Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, DF: Presidência da República, 2008a.

BRASIL. *Medida Provisória n. 2.200-2, de 24 de agosto de 2001*. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF: Presidência da República, 2001.

BRASIL. Ministério da Defesa. *Diretriz Ministerial n. 14, de 09 de novembro de 2009*. Diretriz de Integração e Coordenação dos Setores Estratégicos de Defesa**.** Brasília, DF: MD, 2009.

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

BRASIL. Ministério da Defesa. *Glossário das Forças Armadas – MD35-G-01*. Brasília, DF: MD, 2015.

BRASIL. Ministério da Defesa. *Portaria Normativa n. 3.389, de 21 de dezembro de 2012*. Dispõe sobre a Política Cibernética de Defesa. Brasília, DF: MD, 2012.

BRASIL. Ministério das Comunicações. *Portaria n. 147, de 31 de maio de 1995*. Cria o Comitê Gestor Internet do Brasil. Brasília, DF: MD, 1995.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Instrução Normativa GSI n. 1, de 13 de junho de 2008*. Disciplina a gestão da segurança da informação e comunicações na administração pública federal, direta e indireta e dá outras providências. Brasília, DF: Presidência da República, 2008b.

VIANNA, Eduardo Wallier. *Segurança da informação digital*: proposta de modelo para a Ciber Proteção nacional. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, DF, 2019. Disponível em: https://repositorio.unb.br/handle/10482/35253. Acesso em: 22 abr. 2020.

Recebido em: 26 maio 2020
Aceito em: 27 out. 2020