ESCOLA DE GUERRA NAVAL

CC (T) Alcimar Sanches Rangel

ESTRATÉGIA DE EMPREGO DA GUERRA CIBERNÉTICA EM OPERAÇÕES CONJUNTAS E NA DEFESA DE ESTRUTURAS CRÍTICAS: DESAFIOS PARA ESTRUTURAÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA

Rio de Janeiro

2020

CC (T) Alcimar Sanches Rangel

ESTRATÉGIA DE EMPREGO DA GUERRA CIBERNÉTICA EM OPERAÇÕES CONJUNTAS E NA DEFESA DE ESTRUTURAS CRÍTICAS: DESAFIOS PARA ESTRUTURAÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador(a): CC Rafael Rangel Silva.

Rio de Janeiro
Escola de Guerra Naval
2020

RESUMO

Este trabalho tem por objetivo geral apresentar os principais desafios a serem superados por ocasião do processo de estruturação do Sistema Militar de Defesa Cibernética, em especial, no tocante das ações de proteção cibernética das infraestruturas críticas nacionais de interesse da Defesa em operações conjuntas. Para isso, torna-se importante entender, sob a ótica do Estado, os conceitos de segurança da informação, segurança cibernética, defesa cibernética e guerra cibernética. É necessário, também, identificar as áreas prioritárias de infraestruturas críticas definidas pelo governo federal, identificar os principais ataques cibernéticos ocorridos em infraestruturas críticas e levantar os normativos, nos níveis de decisão político, estratégico, operacional e tático, que orientam a segurança das infraestruturas críticas no espaço cibernético. O nível político é coordenado pela Presidência da República e destina-se à segurança da informação, à segurança cibernética e à segurança das infraestruturas críticas. O nível estratégico está relacionado à defesa cibernética e é conduzido pelo Ministério da Defesa, pelo Estado-Maior Conjunto das Forças Armadas e pelos Comandos das Forças Armadas. Já os níveis operacional e tático estão relacionados à guerra cibernética e restritos no âmbito interno das Forças Armadas. A partir da pesquisa descritiva e da análise de conteúdo dos normativos oficiais de governo, verifica-se a necessidade de ampliação do uso das capacidades cibernéticas destinadas à proteção das infraestruturas críticas. Tal necessidade, visa atender o novo papel do Comando de Defesa Cibernética como um novo comando operacional conjunto. Consequentemente, observa-se que aspectos de ordem financeiro e doutrinário deverão ser superados a fim de possibilitar a implementação das sugestões de aprimoramento do Sistema Militar de Defesa Cibernética.

Palavras-chave: Segurança Cibernética. Defesa Cibernética. Guerra Cibernética. Espaço Cibernético. Infraestrutura Crítica. Operações Conjuntas.

LISTA DE ABREVIATURAS E SIGLAS

AIEA	Agência Internacional de Energia Nuclear
APF	Administração Pública Federal
CDCiber	Comando de Defesa Cibernética
CICTE	Comitê Interamericano Contra o Terrorismo
CIDOC	Comissão Interescolar de Doutrina de Operações Conjuntas
ComDCiber	Comando de Defesa Cibernética
DestGCiber	Destacamento de Guerra Cibernética
DOC	Doutrina de Operações Conjuntas
DMDC	Doutrina Militar de Defesa Cibernética
E-Ciber	Estratégia Nacional de Segurança Cibernética
END	Estratégia Nacional de Defesa
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
EUA	Estados Unidos da América
FCjGCiber	Força Conjunta de Guerra Cibernética
GSI-PR	Gabinete de Segurança Institucional da Presidência da República
IC	Infraestrutura Crítica
ISO/IEC	*International Organization for Standardization and the International Electrotechnical Commission*
LBDN	Livro Branco de Defesa Nacional
MD	Ministério da Defesa
NuComDCiber	Núcleo do Comando de Defesa Cibernética
NuENaDCiber	Escola Nacional de Defesa Cibernética
OEA	Organização dos Estados Americanos
OTAN	Organização do Tratado do Atlântico Norte

PCD	Política Cibernética de Defesa
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
Rede 5G	Quinta Geração de Internet Móvel
SCADA	*System Supervisory Control and Data Acquisition*
SMDC	Sistema Militar de Defesa Cibernética
TO	Teatro de Operações
UE	União Europeia
UIT	União Internacional de Telecomunicações

SUMÁRIO

1 INTRODUÇÃO

O uso do espaço cibernético tornou-se uma questão fundamental nos dias atuais. O rápido avanço tecnológico, evidenciado pelo uso crescente dos meios da tecnologia da informação e da Internet, traz consigo o desafio do desenvolvimento de mecanismos de segurança e defesa que possam permitir, aos cidadãos e instituições públicas e privadas, o uso seguro e democrático desses meios, com respeito às liberdades individuais, mas com responsabilidade e obediência às leis; bem como que confiram proteção oportuna às infraestruturas críticas (IC) do País.

A forte dependência do Estado e da sociedade à tecnologia da informação e à internet geram preocupações de ordem estratégica para o governo. Serviços essenciais prestados pelo Estado e pelo setor privado estão fortemente interligados a sistemas computacionais e expostos às diversas ameaças, internas e externas, presentes no mundo digital. O sucesso dos ataques cibernéticos às IC pode gerar sérios impactos social, econômico, político e à segurança nacional.

Uma vez que as operadoras de IC brasileiras tendem adotar tecnologias emergentes fornecidas por outros países, como a internet das coisas, a quinta geração de internet móvel (rede 5G), a computação em nuvem, aumentam-se as incertezas do uso do espaço cibernético, especialmente, no setor de Defesa.

Dado a complexidade do espaço cibernético, diversas nações estão tentando encontrar uma resposta imediata para esse novo desafio, definindo novas políticas e estratégias para um novo campo de batalha, sendo esse sem fronteiras definidas, minado com artefatos invisíveis e com inimigos desconhecidos. Tais fatores alteram profundamente o pensamento estratégico militar, pois devido às incertezas da origem de um ataque, não há como, de imediato, identificar se foi uma ação de um determinado indivíduo, de uma organização criminosa ou de um outro Estado.

Entretanto, em decorrência dos avanços tecnológicos e da velocidade com que os mesmos vêm ocorrendo é possível verificar um movimento acentuado de rearranjo das proposições das nações em termos de segurança e defesa cibernética. Tal está sendo propiciado quer seja por meio da revisão de suas políticas, estratégias, e normas, quer seja pela atualização ou reformulação das competências essenciais de órgãos chave de governo, visando principalmente criar as condições necessárias de segurança e defesa do espaço cibernético,

notadamente no que diz respeito ao entendimento das novas exigências para a proteção das IC de uma nação.

Nesse sentido, considerando as necessidades levantadas para a ampliação das capacidades militares no emprego da guerra cibernética em operações conjuntas, em especial à proteção das IC de interesse da Defesa, esta pesquisa tem como objetivo geral apresentar os principais desafios para a reestruturação do Sistema Militar de Defesa Cibernética (SMDC), para tal, se faz necessário: compreender os principais conceitos de segurança, defesa e guerra cibernética; levantar os normativos de governo que estabelecem diretrizes para a proteção cibernética das IC nacionais; e apresentar os principais fatores críticos de sucesso para a reestruturação do SMDC.

Dada a importância do tema estudado e para melhor compreender as questões impostas no espaço cibernético, torna-se imprescindível que o País estabeleça políticas e estratégias com regras claramente definidas capazes de responder e intervir, prontamente, qualquer evento adverso que possa vir comprometer a segurança da sociedade e do Estado, em especial, os eventos que possam afetar as IC.

Para a construção deste trabalho acadêmico é realizada uma pesquisa descritiva, utilizando-se da técnica de análise de conteúdo dos documentos oficiais do governo federal, como: leis, decretos, instruções normativas, políticas e estratégias. Também se realiza uma pesquisa bibliográfica a fim de contribuir para o levantamento de conceitos na literatura atual.

Após o capítulo de introdução da pesquisa, é apresentado o segundo capítulo que descreve as ações de segurança e defesa no espaço cibernético, contendo os principais conceitos afetos à segurança, defesa e guerra cibernética; o terceiro capítulo analisa os aspectos relevantes para a segurança e defesa cibernética nas IC, descrevendo os setores de IC, os ataques cibernéticos em IC e as políticas públicas de proteção das IC no espaço cibernético; já o quarto capítulo apresenta fatores críticos que podem impactar de forma negativa o processo de reestruturação do SMDC; por fim, é apresentado o quinto e último capítulo de conclusão.

2 AÇÕES DE SEGURANÇA E DEFESA NO ESPAÇO CIBERNÉTICO

Tendo em vista a natureza transversal dos temas abordados nesta pesquisa e considerando os vastos conceitos encontrados na literatura e em arcabouços técnicos e jurídicos, nacionais e internacionais, são descritos neste capítulo os conceitos de segurança da informação, de segurança cibernética, de defesa cibernética e de guerra cibernética adotados no Governo Federal.

2.1 Segurança da Informação

A Segurança da Informação diz respeito a uma atividade abrangente, que congrega uma série de aspectos, desde a segurança física e lógica da informação, em qualquer meio onde ela esteja armazenada, à proteção dos sistemas e redes de informação. Abrange, ainda, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações computacionais destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento, ou seja, um conjunto de ativos de informação.

Nessa direção, o Governo Federal, por iniciativa do Gabinete de Segurança Institucional da Presidência da República (GSI-PR) considerou, como prioridade nas ações de governo, a necessidade do País possuir uma Política de Segurança da Informação, em nível nacional, o que resultou na publicação do Decreto nº 9.637, de 26 de dezembro de 2018, descrevendo que a SI abrange a segurança cibernética, a defesa cibernética, a segurança física, a proteção dos dados organizacionais e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (BRASIL, 2018a).

Os normativos internacionais consideram a segurança da informação como a aplicação e a gestão de controles com vistas a garantir a disponibilidade, integridade e confidencialidade das informações. Tais controles são obtidos por meio da aplicação do processo de gestão de riscos e gerenciados por um sistema de gestão de segurança da informação, os quais se incluem as políticas, os processos, os procedimentos, a estrutura da organização, os hardwares e os softwares (ISO/IEC, 2018).

Diferente do entendimento internacional, as normas do governo brasileiro, além de prever as propriedades da disponibilidade, integridade e confidencialidade, incluíram o requisito da autenticidade das informações, tal iniciativa se deu pela necessidade do fortalecimento e do alinhamento com a infraestrutura de chaves públicas brasileiras, a fim de prover, além das propriedades acima descritas, a validade jurídica de documento eletrônicos, nesse sentido, o glossário de segurança da informação do Gabinete de Segurança Institucional da Presidência da República entende que a segurança da informação visa assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (BRASIL, 2019a).

A disponibilidade da informação está diretamente relacionada ao princípio da oportunidade, ou seja, a informação tem que estar acessível quando desejável, enquanto a integridade dá a garantia de que a informação não foi modificada de forma não autorizada, e é baseado nesse conceito que as normas internacionais entendem que a autenticidade está inserida

na integridade, visto que, por exemplo, se alguém alterar a assinatura de uma pessoa, tal ação estaria quebrando a integridade do documento, e por fim, a confidencialidade da informação que está relacionada à necessidade de conhecer, visto que a informação não poderá ser revelada a alguém não tenha a devida autorização e credenciamento.

Considerando o acima exposto, pode-se observar um forte relacionamento entre os conceitos de segurança da informação e os conceitos dos requisitos básicos das comunicações navais: rapidez, confiança e segurança. Ao se exigir a rapidez para que uma determinada informação esteja acessível e utilizável por uma pessoa, refere-se à disponibilidade da informação. Quanto à confiança exigida para garantir que não houve modificação do conteúdo ou do remetente da informação, refere-se à integridade e à autenticidade da informação respectivamente. Já a sensação de segurança em saber que determinada informação apenas está disponível às pessoas autorizadas e credenciadas, refere-se à confidencialidade da informação.

Por fim, pode-se observar que a segurança da informação não está relacionada apenas na proteção da informação digital, a segurança da informação atua independentemente do ambiente em que o ciclo de vida da informação esteja inserido, quer esteja no ambiente físico, como por exemplo, informações contidas com pessoas, processos, livros, dispositivos de armazenamentos, ou quer esteja no espaço cibernético, sendo esse um aspecto relacionado especificamente à segurança cibernética.

2.2 Segurança Cibernética

A segurança cibernética é considerada como parte integrante da segurança da informação, possuindo controles voltados para à segurança de operações que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e dos serviços gerenciados por sistemas de informações no espaço cibernético (BRASIL, 2019a). Já o Glossário das Forças Armadas define segurança cibernética como ações destinadas a garantir e a proteger os ativos de informação e as IC destinadas à sociedade da informação de uma nação (BRASIL, 2015).

O último levantamento da União Internacional de Telecomunicações (UIT, 2018, p. 56), apresentou o Brasil ocupando a 70ª posição dos países em termo de segurança cibernética, esse cenário é alarmante, visto que, tanto os órgãos de governo, como as empresas privadas utilizam a internet e, em sua maioria, estão conectadas em redes computacionais. Tal fato demonstra as fragilidades brasileiras no espaço cibernético que, além de possibilitar as perdas

diretas geradas pelas ameaças virtuais, também, afastam investidores, ocasionando perdas financeiras.

Por se tratar de uma preocupação de ordem mundial, questões relacionadas ao espaço cibernético foram inseridas nos arcabouços jurídicos dos países, a exemplo, os Estados Unidos da América publicaram a Lei de nº 111-274, de 12 de agosto de 2014, que instituiu o Aprimoramento da Segurança Cibernética, com vistas a proporcionar uma parceria público-privada voluntária e contínua para a melhoria da segurança cibernética, incluída a proteção de IC contra ameaças cibernéticas (EUA, 2014).

Nessa mesma direção, o Japão também promulgou sua lei que, além de abordar os aspectos da segurança cibernética, incorporou em seus artigos a garantia da distribuição gratuita de informações, a fim de contribuir para a criação de uma sociedade japonesa economicamente mais dinâmica e em contínuo desenvolvimento, de modo a contribuir para a segurança nacional daquele país (JAPÃO, 2014).

No Brasil, as atuais políticas do governo federal, tais como, a Estratégia de Governança Digital, a Estratégia Brasileira de Transformação Digital, a Política Nacional de Modernização do Estado, trouxeram para o debate a temática cibernética para o alcance dos atuais objetivos socioeconômicos do País, de maneira a garantir que a prosperidade digital esteja acompanhada pela confiança e pela resiliência do espaço cibernético, que consequentemente, acelerou-se a construção da Estratégia Nacional de Segurança Cibernética (E-Ciber), publicada por meio do Decreto nº 10.222, de 5 de fevereiro de 2020, já prevista como um dos instrumentos na Política Nacional de Segurança da Informação (PNSI), publicada por meio do Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2018a).

Construída com a visão de tornar o Brasil como uma referência em segurança cibernética, a E-Ciber possui 3 objetivos estratégicos: trazer prosperidade e confiança no ambiente digital, aumentar a resiliência às ameaças cibernéticas e projetar o País no cenário internacional nas questões de segurança cibernética (BRASIL, 2020).

Para o atingimento dos objetivos estratégicos previstos na E-Ciber foram propostas 10 ações estratégicas que nortearão a elaboração dos diversos planos de ações das entidades públicas, sendo que uma dessas está especificamente voltada à proteção das IC do País, prevendo, dentre outras, o incentivo da participação dos órgãos e entidades, públicas e privadas, pertencente às IC em exercícios cibernéticos (BRASIL, 2020).

Levando em consideração a dificuldade e o desafio da coordenação da segurança no espaço cibernético, competência essa dada ao GSI-PR, a E-Ciber somente terá resultados

positivos quando realizada de forma coordenada e colaborativa, envolvendo todos órgãos públicos da União, Estados, municípios, pertencentes aos Poderes Executivo, Legislativo e Judiciário, assim como, envolvendo toda a sociedade civil, uma vez que todos fazem parte de um ecossistema complexo – espaço cibernético – carregado de vulnerabilidades e ameaças.

Com isso, conclui-se que cabe a todos o desenvolvimento de ações voltadas ao tratamento das vulnerabilidades encontradas no espaço cibernético brasileiro, tais como atividades de: padronização, normatização, educação, treinamento e desenvolvimento de habilidades, no entanto, cabe ressaltar que as ações de enfrentamento às ameaças dos tipos: ataque, proteção e exploração cibernética, são de competência da Defesa Cibernética, especialmente quando tais ações ultrapassam o espaço cibernético brasileiro, cabendo essa coordenação ao Ministério da Defesa (MD).

2.3 Defesa Cibernética

No contexto nacional e em nível estratégico sob a coordenação do MD, a defesa cibernética consiste do uso do espaço cibernético por meio da execução de ações de caráter ofensivo, defensivo e exploratório, com vistas a: proteger todos sistemas de informação relevante à defesa nacional, levantar dados para a produção de conhecimento destinados à atividade de inteligência e degradar os sistemas de informação do inimigo (BRASIL, 2014a).

A defesa cibernética tem sua atuação voltada diretamente a conter os ataques das ameaças cibernéticas, especialmente aqueles contra as IC, aos sistemas governamentais, podendo inclusive atuar em realizações de ataques e contra-ataques a grupos de pessoas, de organizações governamentais e não governamentais, que realizam indevidamente acessos, extrações, destruições de informações sensíveis, assim como, atentam contra sistemas de informação de governo e da sociedade civil, especificamente aqueles que prestam serviços essenciais ao cidadão e ao Estado (COSTA, 2016). Galinec, Možnik e Guberina (2017) também entendem que a defesa cibernética está concentrada na detecção e na resposta aos ataques cibernéticos a fim de evitar que qualquer dano às informações e às infraestruturas.

A Doutrina Militar de Defesa Cibernética (DMDC) prevê diversas possibilidades de atuação durante um conflito no espaço cibernético, inclusive, atuar por meio de ações ofensivas, defensivas e exploratórias, podendo, inclusive, atacar IC do inimigo, sem limitação de alcance físico e exposição de tropa. Para tal, faz-se necessário que o País tenha SMDC estabelecido em construções adequadas, disposto de tecnologias de ponta, de um efetivo altamente qualificado, de doutrinas e procedimentos bem definidos (BRASIL, 2014a).

Nessa direção, foi conferido ao Exército Brasileiro na Estratégia Nacional de Defesa (END), a competência, junto ao Ministério da Defesa, de conduzir as ações de defesa cibernética no Brasil (BRASIL, 2008a), para isso, foi criado o Centro de Defesa Cibernética do Exército (CDCiber), por meio da Portaria nº 666, de 4 de agosto de 2010, com a missão de prover a proteção dos sistemas de informações, bem como anular as ações de ataques cibernéticos provindas de fontes de ameaças internas e externas do País (BRASIL, 2010).

Diante da amplitude e da complexidade da defesa cibernética no País, considerando suas dimensões continentais e diversidades regionais, além do crescente número de ataques cibernéticos identificados nas redes computacionais da administração pública federal (APF), foram ativados, subordinados ao (CDCiber), o Núcleo do Comando de Defesa Cibernética (NuComDCiber) e o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), compostos por militares das três Forças Armadas (FA), compartilhando das mesmas instalações, com vistas a potencializar o emprego da guerra cibernética em operações conjuntas e a fortalecer a atuação colaborativa entre os órgãos de governo e o setor privado (BRASIL, 2014b).

Um exemplo de operação conjunta realizado em prol da defesa cibernética é o "Guardião Cibernético", um exercício realizado anualmente, coordenado pelo Comando de Defesa Cibernética (ComDCiber) e conta com a participação de representantes militares e civis, pertencentes aos setores de Defesa e das IC. Durante o exercício são geradas diversas situações de crises onde seus participantes são levados a analisar e identificar soluções para os incidentes cibernéticos apresentados.

Sendo assim, é possível observar o forte alinhamento entre as ações governamentais de defesa cibernética e de segurança cibernética, especificamente, entre a END e a E-Ciber, a primeira no tocante da realização de operações conjuntas e da atuação colaborativa entre os entes federativos e a sociedade civil, e a segunda no cumprimento das ações estratégicas previstas de realização de exercícios cibernéticos com a participação de múltiplos atores e de incentivo à participação das IC em exercícios cibernéticos.

Diante do exposto, fica, portanto, realçada a importância das ações de segurança cibernética e de defesa cibernética na proteção das IC nacionais, visto que proporciona maior resiliência dos sistemas, e consequentemente, possibilita a ininterrupta prestação de serviços essenciais ao cidadão, assim como, a salvaguarda dos interesses nacionais.

2.4 Guerra Cibernética

A história da humanidade demonstra que nem sempre os conflitos entres os povos foram solucionados de forma diplomática e pacífica. Fatores de ordem política, racial, religiosa, econômica motivaram povos a declararem guerra em terra, no mar e no ar.

Até o início do século XX, as guerras se desenvolviam apenas sob os domínios marítimo e terrestre. Com a invenção do avião, durante a Primeira Guerra Mundial (1914-1918), ações militares foram empregadas no domínio aéreo. Ao término da Segunda Guerra Mundial, durante o período da "Guerra Fria", iniciou-se a corrida para a exploração do espaço, sendo esse considerado, pelos EUA, como o 4º domínio para o emprego de operações militares. Até então, os demais países, não consideram o espaço como um domínio de guerra.

O aumento significativo de ataques cibernéticos às redes governamentais e do setor privado fizeram com que diversos países estabelecessem políticas e estratégias nacionais com vistas a minimizar os impactos das ameaças virtuais no espaço cibernético. A Estratégia Cibernética Nacional norte-americana reconhece, mesmo em tempo de paz, que suas IC são vulneráveis frente aos ataques cibernéticos provenientes de estados rebeldes e de organizações terroristas e criminosas, nesse sentido, os EUA definiu o espaço cibernético como seu quinto domínio para operações militares (EUA, 2018a) e nessa mesma direção seguiram os países membros da Organização do Tratado do Atlântico Norte (OTAN), considerando o espaço cibernético com seu quarto domínio (OTAN, 2016).

A guerra cibernética, além de incorporar os clássicos princípios da guerra convencional, também reúne outros princípios específicos do espaço cibernético, tais como o princípio do efeito, da dissimulação, da rastreabilidade e da adaptabilidade. As principais características da guerra cibernética que a diferencia da guerra convencional, estão relacionadas ao seu alcance global e as fronteiras geograficamente indefinidas, ou seja, na guerra cibernética não há limitação física de distância entre os oponentes, podendo cada um atuar de qualquer lugar do planeta. Em resumo, tanto a defesa cibernética quanto a guerra cibernética possuem as mesmas características, sendo essa última adaptada para os níveis operacional e tático (BRASIL, 2017a).

3 SEGURANÇA E DEFESA CIBERNÉTICA NAS INFRAESTRUTURAS CRÍTICAS

Há uma similaridade de conceito entre os termos: estrutura estratégica, estrutura crítica e IC. Denomina-se estrutura estratégica ou IC: toda instalação, serviço, bem ou serviço

que, uma vez destruído ou interrompido, pode provocar sérios impactos à segurança do Estado ou da sociedade (BRASIL, 2018b, 2019b). Já Silva (2014) traz esse conceito para a proteção das estruturas críticas nacionais no contexto da guerra cibernética.

Considerando que as atuais políticas do governo convergem para a intensificação do intercâmbio de informações entre os órgãos públicos, e da mesma forma, deles com os órgãos privados do país e considerando, também, que os serviços essenciais prestados à sociedade são fornecidos por instituições das diferentes esferas do Poder Público e por empresas privadas, o termo IC adotado na Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) tornou-se o mais adequado para o desenvolvimento desta pesquisa, no entanto, cabe ressaltar que a criticidade de uma determinada infraestrutura não está relacionada com fragilidade e vulnerabilidade, e sim por necessitar de atenção especial e de controles rígidos de proteção, aqui no caso, de segurança e defesa cibernética.

3.1 Setores de infraestruturas críticas

Ainda não há no arcabouço jurídico brasileiro, em nível nacional, quais são os serviços essenciais que deverão ser priorizados e protegidos frente aos ataques cibernéticos, por outro lado, a Lei nº 7.783, de 28 de junho de 1989, conhecida como a Lei da Greve, serve como um norte, descrevendo uma lista de serviços essenciais que não podem ser interrompidos ou paralisados, pois tais serviços são de necessidades inadiáveis, ou seja, podem colocar em perigo a sobrevivência, a saúde e a segurança da população, como por exemplo, o tratamento e abastecimento de água; a produção e a distribuição de energia elétrica, de gás e de combustíveis; as telecomunicações; a guarda, o uso e o controle de substâncias radioativas; os equipamentos e materiais nucleares; o controle de tráfego aéreo e navegação aérea (BRASIL, 1989).

No Brasil, a Portaria nº 2 de 08 de fevereiro de 2008 do GSI-PR considera como áreas prioritárias de IC, os setores de energia, transporte, água, comunicações e finanças, e define IC como: “as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional” (BRASIL, 2008b). A interrupção ou destruição de uma IC é causada por ameaças que podem ser de ordem natural, acidental ou intencional, no entanto, pelo fato das atuais IC serem largamente controladas e gerenciadas por sistemas autônomos, informatizados e em redes, as ameaças cibernéticas tem sido uma das maiores preocupações para as nações, exigindo cada vez mais a intensificação das ações de segurança e defesa cibernética nas IC.

Os EUA, país que possui um elevado nível de proteção de IC, estabeleceram uma lista de 16 setores considerados como IC, aos quais se destacam as bases industriais de defesa, as instalações de governo e o setor nuclear, isto porque, tais setores, além de estarem estritamente relacionados à defesa nacional daquele país, constituem-se como principais alvos de ameaças terroristas (EUA, 2020). O governo alemão também incluiu em sua lista de 9 setores de IC, a segurança das instituições de Estado e de Governo, incluído o setor de defesa e de segurança interna (ALEMANHA, 2020).

Como visto, a definição dos setores de IC e áreas prioritárias se distinguem em cada país, no entanto, pode-se verificar que, diferente de outros países que já possuem uma cultura de proteção elevada de suas IC, o Brasil não considerou como uma área de interesse, as instalações de governo como IC, especialmente, as instalações de segurança e de defesa. Há que se considerar por exemplo que, um determinado sistema militar de defesa, uma vez interrompido ou destruído por um ataque cibernético, conforme definido, pode provocar sério impacto à segurança nacional (BRASIL, 2008b). Há que se considerar também a relação de interdependência entre os diversos setores de IC. Por exemplo, um ataque cibernético em um sistema de proteção do espaço aéreo pode paralisar o setor de transporte aéreo, assim como, um ataque em um sistema de produção e distribuição de energia pode impactar os sistemas de defesa nacional.

Sendo assim, devido ao considerado espaço temporal transcorrido de 2008 até os dias atuais, quando foram definidas as áreas prioritárias de IC e, também, devido os avanços das tecnologias embarcadas nos sistemas de controle e operação das IC, torna-se importante revisar o conceito dessas áreas prioritárias de IC brasileiras, a exemplo de outras nações que incluíram as áreas de segurança, de defesa e de Tecnologia da Informação no rol de suas IC.

3.2 Ataques cibernéticos em infraestruturas críticas

Com a evolução e a expansão da internet, aumentaram-se os ataques cibernéticos em escala global. Inicialmente, os ataques destinavam-se a obter informações e dados de forma não autorizada de pessoas, empresas e governos, mas com o passar do tempo, assim como houve avanços das tecnologias, os ataques cibernéticos também se tornaram cada vez mais sofisticados, pois além da obtenção de informações privilegiadas, tornaram-se armas de destruição e paralização de sistemas críticos de empresas e de governos. Para Lima e Silva (2018), o espaço cibernético, além de sustentar a sociedade moderna, fornece suporte crítico à economia global, por outro lado, é permeado por diversas vulnerabilidades que não só afetam

a privacidade pessoal, com também, prejudicam as operações de IC, impactando cidades, estados e até mesmo um país inteiro.

Os ataques cibernéticos podem ser direcionados para as três camadas que compõem o espaço cibernético definas por Ltabansky (2011), ou seja, o ataque pode danificar a camada física composta por circuitos integrados, cabeamentos, fontes de energia, dispositivos de armazenamento, transmissores e receptores, assim como, alterar os comandos e as instruções de programas computacionais que correspondem a segunda camada, e por fim, atacar a terceira camada, por meio da obtenção e do sequestros de dados e informações armazenados.

A facilidade de obtenção de artefatos maliciosos na internet faz com que qualquer pessoa se torne um eventual propagador de ataques cibernéticos. A motivação, normalmente, define o perfil dos agentes de ameaças no espaço cibernético, podendo ser, inclusive, uma criança, grupos de ativistas político, organizações criminosas, grupos terroristas e, até mesmo, um Estado-nação. Os atacantes amadores tendem a explorar as vulnerabilidades típicas dos usuários inexperientes e sem cultura de segurança, ou seja, aqueles que ainda usam senhas fracas, não atualizam seus sistemas e programas computacionais e aceitam todos tipos de mensagens. No entanto, os ataques destinados às IC, geralmente, são originados de fontes especializadas, possuidoras de grandes recursos computacionais e financeiros e, até mesmo, são financiados por grandes organizações e Estados.

Um dos primeiros casos de ataque cibernético às IC de um país ocorreu em 2007, quando a Estônia, reconhecida como o maior país digital do mundo, sofreu um ataque de grande proporção em seu espaço cibernético, os seus serviços essenciais prestados pelo governo e pelo setor privado foram paralisados, gerando grande impacto de ordem social e financeiro. Até hoje não há confirmação da origem do ataque, especula-se que pode ter vindo de grupos ativistas ou do próprio governo russo em represália à decisão do governo da Estônia em retirar a estátua do soldado de bronze fixada na principal praça de Tallinn e transferi-la para às proximidades do cemitério militar da mesma cidade. Para a Rússia, a estátua representava sua vitória na 2ª Segunda Guerra Mundial contra o nazismo, já para a Estônia, a mesma estátua representava o domínio soviético em seu território (LIMA e SILVA, 2018).

Em 2008, novamente a Rússia estava envolvida em questões de ataques cibernéticos, nesse caso contra a Geórgia, outra república da extinta União Soviética. Diferente do caso Estônia, dessa vez o ataque cibernético ocorreu em uma operação militar conjunta de tropas russas antes mesmo de invadir o espaço terrestre da Geórgia. Um dia antes de a tropa e os tanques russos adentrarem no terreno inimigo, todo serviço de comunicação e da mídia da

Geórgia haviam sido paralisados a fim de evitar represálias de outras nações. Em seguida, o ataque cibernético evoluiu para outras IC como os setores de finanças, de transporte marítimo e instalações de armazenamento e abastecimento de petróleo e gás.

Nesse mesmo contexto envolvendo possíveis conflitos no campo diplomático e bélico, em 2010, especialistas da Agência Internacional de Energia Atômica (AIEA), órgão vinculado às Nações Unidas, identificaram uma anomalia no processo de enriquecimento de urânio em uma usina nuclear iraniana. Tratava-se dos resultados provocados pelo vírus Stuxnet[1], que consiste de um programa malicioso destinado exclusivamente a danificar sistemas SCADA[2], que são amplamente utilizados em controles de dados de equipamentos industriais em tempo real, como por exemplo nos sistemas de controle e monitoramento das centrífugas.

Considerado como uma arma cibernética, o *Stuxnet* é um exemplo do uso da cibernética para provocar efeitos cinéticos e não cinéticos nas capacidades do inimigo. Ao se instalar no sistema operacional, o vírus alterou as instruções e os comandos programados para controlar a velocidade de rotação das centrífugas, assim como, alterou o sistema de monitoramento de alarme e emergência, produzindo assim um efeito não cinético por meio da quebra da integridade das informações dos sistemas. Em consequência da alteração das linhas de comando do sistema operacional, os valores alterados produziram instruções indevidas que aceleraram a velocidade de rotação das centrífugas, danificando-as fisicamente, possibilitando inclusive a geração de incêndios e de explosões em toda usina iraniana, sendo esse caso, um exemplo do efeito cinético da cibernética em uma IC.

Além dos ataques cibernéticos destinados, diretamente, a degradar as capacidades militares ou destruir IC de uma determinada nação, existem aqueles projetados a auferir ganhos financeiros a grupos e organizações criminosas por meio de sequestro de base de dados pessoais e organizacionais.

A título de exemplo, no ano de 2017, aproximadamente 300.000 computadores de 150 países foram infectados pelo código malicioso *WannaCry*. Este código foi criado para explorar as vulnerabilidades do sistema operacional *Windows* desatualizados, fazendo com que os atacantes pudessem criptografar todos dados armazenados nas máquinas atacadas. Após criptografar os dados, a organização criminosa exigia o pagamento do resgate em troca da chave de acesso. Pesquisadores do setor de segurança cibernética atribuíram a origem desse código à

[1] STUXNET – apelido do vírus criado a partir das letras no nome do arquivo mrxnet.sys e de outra parte do código malicioso.
[2] SCADA – acrônimo de *Supervisory Control and Data Acquisition* (Controle Supervisório e Aquisição de Dados).

organização criminosa “Lazarus”, que supostamente estaria ligado ao governo norte-coreano. Em 2018, a polícia federal dos EUA emitiu nota oficial acusando um cidadão norte-coreano chamado Park Jin Hyok como responsável direto pelo vírus *WannaCry* e outros ataques cibernéticos (EUA, 2018b).

Não há relatos de sequestro de dados de IC brasileiras durante o ataque do *WannaCry*, no entanto, devido à falta de informação e das incertezas, diversas organizações públicas e privadas, naquela ocasião, desligaram seus computadores e retiraram seus serviços da internet do ar e, em consequência, alguns serviços essenciais foram indisponibilizados ao cidadão.

Decorridos 2 anos do ataque do *WannaCry*, esse mesmo padrão de ataque cibernético obteve êxito no sequestro de dados da Companhia de Docas do Estado do Ceará, empresa responsável pela operação do porto de Mucuripe em Fortaleza, sendo que dessa vez, toda infraestrutura de transporte aquaviário daquele porto ficou prejudicada, fazendo com que operações fossem realizadas de forma manual, gerando atrasos e perdas financeiras.

Como visto, os ataques cibernéticos contra as IC se tornaram uma preocupação de ordem mundial, a exemplo, a Declaração sobre Proteção da Infraestrutura Crítica assinada pelos Estados membro do Comitê Interamericano Contra o Terrorismo (CICTE) da Organização dos Estados Americanos (OEA), por ocasião de sessões plenárias realizadas no período de 28 de fevereiro a 2 de março de 2007 na República do Panamá, estabeleceu como compromisso dos países signatários: a necessidade de formulação de políticas e doutrinas de segurança e defesa cibernética para a proteção de IC; a necessidade de promover o intercâmbio voluntário de experiências, de informações e de melhores práticas entre os Estados membros; e a necessidade de cooperação hemisférica entre de grupos de peritos, com o objetivo de prevenir, mitigar e dissuadir ameaças à IC, harmonizando, caso seja apropriado, os esforços nacionais e regionais (OEA, 2007). Nessa mesma direção, diretivas da União Europeia (UE) estabeleceram a necessidade dos seus países membros adotarem ações coordenadas para responder os ataques cibernéticos direcionados às IC, reforçando com isso, a segurança e a resiliência dos serviços essenciais gerados e processados por tecnologias da informação (UE, 2020).

No Brasil, coube ao GSI-PR, no cumprimento de sua competência legal de acompanhar os assuntos atinentes às IC e de coordenar as atividades de segurança cibernética (BRASIL, 2019c), e ao MD, na competência de estabelecer diretrizes e procedimentos relacionados à defesa nacional contra ataques cibernéticos (BRASIL, 2018a), elaborarem políticas e estratégias destinadas à proteção das IC no espaço cibernético.

3.3 Políticas e estratégias brasileiras para a proteção das infraestruturas críticas no espaço cibernético

Dada a importância para o fortalecimento do setor cibernético conforme estabelecido na END, a construção dos instrumentos normativos destinados a nortear o uso do espaço cibernético, em especial para a proteção das IC, foi realizada de acordo com os seguintes níveis de decisão: político, estratégico, operacional e tático.

O nível político, coordenado pela Presidência da República, destina-se à segurança da informação, à segurança cibernética e à segurança das IC; já o nível estratégico, relativo à defesa cibernética, é conduzido pelo MD, pelo Estado-Maior Conjunto das FA e pelos Comandos das FA; e por fim, os níveis operacional e tático, restritos no âmbito interno das FA, destinados a condução das ações de guerra cibernética (BRASIL, 2014a).

3.3.1 Nível político

Com vistas a endereçar as necessidades de proteção das IC, o GSI-PR criou grupos de trabalho, compostos por representantes da APF, para realizar levantamentos sobre cada área prioritária e, também, propor um marco legal para o setor de IC. Como resultado, foi publicado o Decreto nº 9.573, de 22 de novembro de 2018, aprovando a PNSIC (BRASIL, 2018b).

Para a execução da PNSIC, estão previstos como instrumentos: a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), o Plano Nacional de Segurança de Infraestruturas Críticas e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. Consideram-se fatores críticos para o sucesso da ENSIC, a previsão de planos setoriais, sob a responsabilidade dos Ministérios e agências reguladoras de cada área prioritária, contendo mecanismos de acompanhamento das ações executadas e metas atingidas. Outro fator importante para a construção da ENSIC é a previsão de um sistema central de gestão de informação que possibilite a tomada de decisão em tempo oportuno e que seja baseado na visão integrada dos diversos cenários.

Para alcançar os objetivos propostos na PNSIC, espera-se que, com a publicação da ENSIC, alguns desafios sejam superados como: o reconhecimento da IC como uma política de Estado; o comprometimento da alta administração das organizações, pública e privada, para o fomento de ações preventivas; o fomento da cultura de segurança para os colaboradores, interno e externo, das IC, assim como para a sociedade; o estabelecimento de canais estratégicos e técnicos para maior compartilhamento e fluidez das informações.

Ressalta-se ainda que a operação e o controle das IC são de responsabilidades de organizações privadas e públicas e para que haja o comprometimento de todos, torna-se imprescindível que a PNSIC seja editada em forma de lei e não por decreto, com vistas a abarcar sob o seu mandato todo setor privado e todas as esferas de governo estaduais e municipais.

Em relação às competências destinadas a assegurar o espaço cibernético, a PNSI e a E-Ciber constituem, também, como orientações exclusivas ao Poder Executivo Federal, uma vez que foram publicados em forma de decretos e aqui, novamente, percebe-se a necessidade de ser editada uma Lei Nacional de Segurança Cibernética para atender os objetivos nacionais, incluindo todos os Poderes, as outras esferas de governo, o setor privado e a sociedade.

Destarte, torna-se oportuno que o GSI-PR faça um alinhamento entre as duas estratégias, E-Ciber e a ENSIC, no tocante da proteção das IC contra ataques cibernéticos. Uma vez que tais estratégias necessitam de planos setoriais, a elaboração de um plano nacional de segurança cibernética para as IC atenderia os anseios dos dois normativos.

Além da PNSI e da E-Ciber, o GSI-PR possui um arcabouço normativo destinado à gestão de segurança da informação dos órgãos e entidades da APF que aborda temas, entre outros, afetos à gestão de riscos em segurança da informação, ao tratamento de incidentes em redes de governo, ao controle de acesso físico e lógico, ao uso de recursos criptográficos.

3.3.2 Nível estratégico, operacional e tático

Os principais documentos, em nível de decisão estratégico, que abordam aspectos relativos à defesa cibernética e à proteção de IC de interesse da Defesa são: a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END), o Livro Branco de Defesa Nacional (LBDN), a Política Cibernética de Defesa (PCD) – MD31-P-02, a Doutrina Militar de Defesa Cibernética (DMDC) – MD31-M08.

Em resumo, a PND e a END incluem o setor cibernético como um setor estratégico tecnológico essencial para a Defesa Nacional, já o LBDN acrescenta que para proteger o espaço cibernético torna-se necessário incluir outras áreas como: capacitação, doutrina, pessoal, preparo, emprego e pesquisa (BRASIL, 2017b).

A garantia o uso efetivo do espaço cibernético pelas FA constitui um dos objetivos da PCD que são desdobrados na DMDC, documento pelo qual o MD promove um entendimento estratégico sobre a atuação das FA, de forma conjunta, em defesa dos interesses nacionais no espaço cibernético. As diretrizes estabelecidas na DMDC têm por finalidade trazer às FA brasileira vantagens estratégica, operacional e tática no espaço cibernético frente às ações do

inimigo, em especial, contra as ações que venham a comprometer IC de interesse à Defesa Nacional. Em síntese, o nível estratégico fornece as principais diretrizes e orientações necessárias para o emprego da guerra cibernética em operações conjuntas das FA definidas nos níveis operacional e tático.

No que se refere aos documentos de níveis de decisão operacional e tático, destaca-se a Doutrina de Operações Conjuntas (DOC) – MD30-M-01 que estabelece os fundamentos doutrinários necessários a orientar as Forças Singulares, durante o processo da construção dos seus planos operacionais e táticos, em ações de exploração, ataque e proteção no espaço cibernético (BRASIL, 2011).

Tendo em vista a necessidade de implementar os objetivos previstos na PCD e na DMDC, considerou-se importante aperfeiçoar o uso da capacidade cibernética em operações conjuntas, nesse sentido, em 2018 foi publicada a Nota Escolar nº 004 da Comissão Interescolar de Doutrina de Operações Conjuntas (CIDOC) contendo "orientações para a elaboração do componente conceitual do planejamento operacional, a fim de servir como convenção didática e uniformizar os trabalhos escolares executados nas Escolas de Altos Estudos Militares" (BRASIL, 2018c).

Dentre as diversas orientações da referida Nota Escolar, destaca-se uma proposta de estrutura da guerra cibernética no Teatro de Operações (TO), em especial, o emprego operativo do ComDCiber atuando como órgão central do SMDC em nível de decisão operacional e o emprego da Força Conjunta de Guerra Cibernética (FCjGCiber) e de Destacamentos de Guerra Cibernética (DestGCiber) em nível de decisão tático.

Por fim, há que se considerar que o modelo de SMDC previsto na DMDC deverá ser reestruturado e para tal, torna-se importante identificar quais são os desafios a serem superados, em especial, no tocante da proteção de IC de interesse para a Defesa Nacional.

4 DESAFIOS PARA A ESTRUTURAÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA

O modelo de SMDC apresentado na DMDC, na época, foi considerado a forma mais adequada de estrutura militar necessária a assegurar, de forma conjunta, o uso efetivo do espaço cibernético contra ameaças que venham afetar os interesses nacionais e a segurança do Estado, no entanto, devido à grande velocidade com que surgem as novas tecnologias e, também, devido ao ritmo exponencial com que os novos tipos de ataques se potencializam no

espaço cibernético, fazem com que o SMDC desenvolva novas capacidades de defesa e guerra cibernética, impondo constantes atualizações em seu modelo.

Por se tratar de um modelo sistêmico que envolve diversos atores em diversos níveis de decisão, torna-se importante identificar os principais fatores críticos que podem impactar de forma negativa o processo de reestruturação do SMDC.

Hoje, tanto no setor público quanto no privado, pode-se dizer que a continuidade de qualquer serviço essencial destinado ao cidadão ou ao Estado depende da forma como é gerenciada a segurança cibernética. A má gestão da segurança cibernética, quer seja no que tange à segurança da informação, quer seja no que tange à segurança da IC, pode afetar à condução das ações afetas aos órgãos integrantes do SMDC. O nível de decisão político coordenado pela Presidência da República necessita ampliar o seu escopo de atuação por meio de leis gerais de segurança cibernética e de segurança de IC. Para que os decretos que publicaram a PNSI, a E-Ciber e a PNSIC tenham efeitos além do escopo da APF, se faz necessário incluir tais temas como assuntos privativos à União na Constituição Federal, por meio de Emenda Constitucional.

Nota-se também que o Brasil ainda não possui um órgão central que concentre todas as atividades necessárias para regular o setor cibernético. A criação de uma Agência Nacional de Segurança Cibernética possibilitaria uma melhoria no processo de comunicação entre os órgãos que compõem os setores de IC e o SMDC, possibilitando um melhor compartilhamento de informações para a prevenção e reação oportuna a incidentes cibernéticos. Isso não significa que o SMDC será responsável pela proteção cibernética de todas as IC, mas sim daquelas que caso venha a ser atacada possa comprometer, direta ou indiretamente, a Defesa Nacional.

Como por exemplo, um ataque cibernético que venha a comprometer o sistema de abastecimento de água da cidade de Angra dos Reis, inicialmente teria o impacto social à população daquela cidade, no entanto, caso esse ataque evolua e venha a comprometer o sistema de resfriamento das usinas nucleares de Angra do Reis, essa IC passou a ser de interesse da Defesa.

Há que se considerar também os desafios a serem superados por ocasião da transformação do ComDCiber em um comando operacional conjunto, permanentemente ativado. Para atender as sugestões já apresentadas na Nota Escolar nº 004/CIDOC, deverão ser considerados diversos aspectos de ordem financeira e doutrinária.

Questões financeiras podem impactar os projetos de implantação e de melhorias do setor de defesa cibernética, visto que o Programa de Defesa Cibernética da Defesa Nacional

(PDCDN) do orçamento federal previa entregas imediatas, tais como, a estruturação do SMDC e a adequação das instalações do ComDCiber para as demandas operacionais, já para uma segunda fase, a construção das instalações do futuro centro de operações. Um estudo preliminar estimou-se que orçamento deveria ser na ordem de R$ 60.000.000,00 para o ano de 2020 e de R$ 120.000.000,00 para os anos de 2021, 2022 e 2023, no entanto, apenas somente R$ 6.334.725,00 foram destinados ao ComDCiber para o ano de 2020 (BRASIL, 2019d).

Atualmente, o ComDCiber não possui em sua estrutura um centro de operações capaz de funcionar ininterruptamente, para tal, iniciaram-se diversos projetos destinados à construção das instalações, à aquisição de tecnologia e à capacitação de especialistas. Sendo assim, o corte orçamentário se tornou um grande desafio para a continuidade dos projetos previstos para a reestruturação do SMDC e de transformação do ComDCiber num comando operacional conjunto.

Ressalta-se que algumas questões de ordem doutrinária, também, constituem-se como desafios para o novo modelo de SDMC. Uma vez considerado o setor cibernético como um novo domínio da guerra, as FA deverão rever e repensar suas atuais doutrinas e seus *Modus operandi,* a fim de atender essa nova modalidade de atuação no TO.

Considerando que a área de conflito da guerra cibernética não possui fronteira definida e não requer a presença física da tropa, torna-se necessário rever as doutrinas, operacional e tática, com a finalidade de definir claramente o campo de atuação do Comando do TO e do ComDCiber, para que não haja conflitos e superposições de atribuições.

Cabe ressaltar que o ComDCiber, além de exercer a função de Estado-Maior em operações conjuntas, deverá também fornecer um contingente de especialistas militares, devidamente preparados e equipados às demais estruturas de Comandos Operacionais e Forças Conjuntas quando ativadas. Aqui, novamente, identificam-se, além das necessidades de revisão doutrinária, novos desafios de ordem financeira para o SMDC.

Por fim, há que se prever na DOC a possibilidade de ações cibernéticas ofensivas contra IC do oponente localizados fora do TO, no entanto, as peculiaridades da guerra cibernética trazem outros desafios que ultrapassam o cenário da guerra convencional. Ao se decidir degradar uma infraestrutura que provê serviços à força oponente, as ações de ataque cibernético deverão ser precedidas de autorização seguindo a cadeia de comando, até chegar ao Presidente da República, como Comandante Supremo das FA.

5 CONCLUSÃO

A partir do exposto, fica claro que, no mundo, são crescentes os debates e as discussões acerca do espaço cibernético e os seus impactos políticos, econômicos e sociais. Diante da sua complexidade, muitos entraves se fazem presentes e necessitam de uma atuação planejada e eficaz. Assim, esta pesquisa buscou retratar, de maneira geral, os obstáculos enfrentados pelo SMDC frente à necessidade da sua reorganização com o intuito de minar as adversidades decorrentes do espaço cibernético e seu avanço.

Isso posto, em consequência das ameaças que esse espaço acarreta, as IC se tornaram o centro das atenções acerca dos cuidados necessários, tendo em vista o vazio que há no ordenamento jurídico brasileiro quanto a definição das IC que necessitam de uma atuação mais ativa do Estado. Consequentemente, as instalações de governo e da Defesa ficam descobertas e propícias a ataques.

Em comparação com os países citados nesta pesquisa, no Brasil, há a necessidade de uma reestruturação completa a fim de que os riscos recorrentes do mundo cibernético sejam sanados. Como exposto, além do vácuo constitucional, também há uma escassez de políticas e planos, tanto no âmbito político quando no âmbito estratégico, tais como a ENSIC, que viabilizem a segurança cibernética dos cidadãos, das instituições privadas e das IC.

Outrossim, como evidenciado, verifica-se a ausência de um órgão de controle que alcance toda a esfera cibernética, a fim de desenvolver técnicas e mecanismos de proteção aos ataques que surgem exponencialmente e demandam uma atuação urgente e célere. Diante disso, a proposta da presente pesquisa consiste em ampliar, para alcance nacional, a competência dos órgãos de Defesa e da APF para lidar com os domínios políticos e estratégicos, referentes à segurança cibernética. Além disso, torna-se imprescindível o aumento do orçamento destinado ao SMDC e ao ComDCiber que possibilite a formulação de projetos e pesquisas referentes ao tema com o propósito de que este torne-se conhecido e não mais um campo minado a ser guerreado pelas nações.

Por fim, muitos são os obstáculos a serem vencidos pelo SMDC em esforço conjunto com a nação brasileira, suas instituições públicas, e privadas e seus cidadãos. Tal esforço visa superar as incertezas do espaço cibernético e fazer do Brasil um modelo internacional de infraestrutura, de estratégias, e de planos operacionais e táticos, no que concerne aos avanços tecnológicos e suas vulnerabilidades.

REFERÊNCIAS

ALEMANHA. *Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.* ***Sektoren und Branchen Kritischer Infrastrukturen.*** 2020. Disponível em: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html. Acesso em: 22 ago. 2020.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa. Brasília, DF: Presidência da República. 2008a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em: 21 abr. 2020.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República. 2018b. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 21 abr. 2020.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação [...]. Brasília, DF: Presidência da República. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 21 abr. 2020.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.htm. Acesso em: 21 abr. 2020.

BRASIL. Comando do Exército. **Portaria nº 666, de 4 de agosto de 2010.** Cria o Centro de Defesa Cibernética do Exército e dá outras providências, 2010. Disponível em: http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=824&act=bre. Acesso em: 22 jul.2020.

BRASIL. Estado-Maior do Exército. **Portaria nº 11, de 14 de janeiro de 2019**. Aprova a Diretriz de Iniciação do Projeto Centro de Coordenação de Operações Móvel, Brasília, 2019b. Disponível em: http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=724&act=sep. Acesso em: 22 jul.2020.

BRASIL. Gabinete de Segurança Institucional. **Portaria nº 2/GSI, de 8 de fevereiro de 2008**. Institui Grupos Técnicos de Segurança de Infra-estruturas Críticas (GTSIC) e dá outras providências. Brasília, 2008b. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=11/02/2008&totalArquivos=88. Acesso em: 22 jul.2020

BRASIL. Gabinete de Segurança Institucional. **Portaria nº 93/GSI, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Brasília, 2019a. Disponível em:

https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 22 jul.2020.

BRASIL. **Lei n.º 7.783, de 28 de junho de 1989.** Dispõe sobre o exercício do direito de greve, define as atividades essenciais, regula o atendimento das necessidades inadiáveis da comunidade, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8142.htm. Acesso em: 02 jul.2020.

BRASIL. **Lei n.º 13.844, de 18 de junho de 2019.** Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, 2019c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm. Acesso em: 02 jul.2020.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa.** Brasília, 2017b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf. Acesso em: 30 mai. 2020.

BRASIL, Comandante de Operações Terrestres. Portaria nº 42 - COTER, de 8 de junho de 2017. **Aprova o Manual de Campanha EB70-MC-10.232 Guerra Cibernética**, 1ª Edição, 2017a.

BRASIL. Ministério da Defesa. **MD30-M-01:** Doutrina de Operações Conjuntas. 1ª Edição. Brasília, 2011.

BRASIL. Ministério da Defesa. **MD31-M-07:** Doutrina Militar de Defesa Cibernética. 1ª Edição. Brasília, 2014a.

BRASIL. Ministério da Defesa. **MD35-G-01:** Glossário das Forças Armadas. 5. ed. Brasília, 2015.

BRASIL. Ministério da Defesa. **Nota Escolar nº 004/CIDOC, de 23 de maio de 2018.** O uso da capacidade cibernética e de guerra eletrônica em operações conjuntas, 1ª Edição, 2018c.

BRASIL. Ministério da Defesa. **Portaria nº 2.777/MD, de 27 de outubro de 2014**. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Brasília, 2014b. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=7&data=28/10/2014. Acesso em: 22 jul.2020.

BRASIL. Senado Federal. Comissão de Relações Exteriores e de Defesa Nacional. **Relatório de Avaliação de Política Pública a Política Nacional sobre Defesa Cibernética**, de 9 de dezembro de 2019. Brasília, 2019d.

COSTA, Alan Denilson Lima. **O Sistema Militar de Defesa Cibernética e seus reflexos para a Defesa Nacional.** EB Revistas. 1º quadrimestre, 2016. Disponível em: http://www.ebrevistas.eb.mil.br/index.php/ADN/article/download/3444/2808. Acesso em: 20 jun. 2020.

EUA. *Department of Homeland Security.* ***Guidance on the Essential Critical Infrastructure Workforce***, 2020. Disponível em: https://www.cisa.gov/critical-infrastructure-sectors. Acesso em: 22 ago. 2020.

EUA. *Federal Bureau of Investigation.* ***Wanted by the FBI – Park Jin Hyok***, 2018b. Disponível em: https://www.fbi.gov/wanted/cyber/park-jin-hyok/download.pdf. Acesso em: 22 ago. 2020.

EUA. Lei nº 113-274, de 18 de dezembro de 2014. ***Cybersecurity Enhancement Act of*** **2014**. Disponível em: https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf. Acesso em: 22 ago. 2020.

EUA. *White House.* ***National Cyber Strategy of United States of America.*** Washington, 2018a. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 22 ago. 2020.

GALINEC, Darko; MOŽNIK, Darko; GUBERINA, Boris. ***Cybersecurity and cyber defence: national level strategic approach.*** Automatika v. 58, n. 3, p. 273-286, 2017. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/00051144.2017.1407022?needAccess=true. Acesso em: 23 jul.2020.

INTERNATIONAL STANDARD. **ISO/IEC 27000:2018**: *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Suiça: ISO/IEC, 2018.

JAPÃO. Lei nº 104, de 12 de novembro de 2014. ***The Basic Act on Cybersecurity****,* 2014. Disponível em: http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01. Acesso em: 22 ago. 2020.

OEA. Comitê Interamericano Contra o Terrorismo (CICTE). **Declaração do Panamá sobre a Proteção da Infraestrutura Crítica no Hemisfério frente ao Terrorismo**. Panamá, 2007.

OTAN, *Summit in Warsaw*. ***NATO heads of state and government recognised cyberspace as a domain of operations****.* Varsóvia, 2016. Disponível em: https://www.cimic-coe.org/resources/coe-catalogue-2017-small.pdf. Acesso em: 20 jun. 2020.

LIMA E SILVA, Walbery Nogueira de. ***Cyberspace: Protection of Critical Infrastructure.*** *Concordiam Journal of European Security and Defense Issues.* Volume 9, Issue 1, 2018.

LTABANSKY, Lior. ***Basic concepts in cyber warefare.*** *Military and strategic Affairs.* Vol. 3, nº 1, 2011. Disponível em: http://book.itep.ru/depository/cyberwar/1308129610.pdf. Aceso em: 20 jun. 2020.

SILVA, Júlio Cezar Barreto Leite da. **Guerra Cibernética: A Guerra no Quinto Domínio, Conceituação e Princípios.** Revista da Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193 – 211, jan./jun, 2014. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/download/194/156. Acesso em: 20 jun. 2020.

UE. União Europeia. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões sobre a Estratégia da UE para a União da Segurança**, 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605&from=EN. Acesso em: 22 jun. 2020.

UIT. União Internacional de Telecomunicações. ***Global Cybersecurity Index.*** *Studies & research, ITU Publications*, 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. Acesso em: 12 jul. 2020.