INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2021/2022

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

ORGANIZAÇÃO PARA A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Alexandre Luckemeyer Machado Carrion

CORONEL DE CAVALARIA (BRA)

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

ORGANIZAÇÃO PARA A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL

COR CAV (BRA) Alexandre Luckemeyer Machado Carrion

Trabalho de Investigação Individual do CPOG 2021/2022

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

ORGANIZAÇÃO PARA A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL

COR CAV (BRA) Alexandre Luckemeyer Machado Carrion

Trabalho de Investigação Individual do CPOG

Orientadora: Coronel Enginf Ana Cristina Domingos de Oliveira Rodrigues Telha

Apoiante: Major Tiago Miguel Marques Vilela da Costa

Pedrouços 2022

Declaração de compromisso antiplágio

Eu, Coronel de Cavalaria do Exército Brasileiro Alexandre Luckemeyer Machado Carrion, declaro por minha honra que o documento intitulado "Organização para a Segurança e Defesa Cibernética no Brasil" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do CPOG 2021/2022 no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 12 de julho de 2022.

Alexandre Luckemeyer Machado Carrion

Agradecimentos

A Deus por ter me dado saúde e força, neste momento delicado e difícil que enfrentamos devido à situação pandêmica.

A minha família pelo amor, incentivo e apoio incondicional.

A minha orientadora Coronel Enginf Ana Cristina Domingos de Oliveira Rodrigues Telha e ao Major Tiago Miguel Marques Vilela da Costa, Oficial Apoiante do IUM, cujo apoio foi essencial para estabelecer as linhas orientadoras do trabalho e corrigir rumos desta investigação.

Deixo um especial agradecimento a todos os auditores do Curso de Promoção a Oficial General 2021/2022, pelo excelente espírito de camaradagem reinante e pelos laços de amizade que certamente subsistirão.

Por último, agradeço aos docentes e integrantes do IUM, por toda a ajuda e disponibilidade demonstradas a este Oficial Superior do Exército Brasileiro.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Índice de Tabelas

Resumo

Este trabalho analisou a Organização para a Segurança e Defesa Cibernética no Brasil com o objetivo de propor contributos para a sua melhoria. O estudo se faz relevante face às crescentes ameaças surgidas à segurança nacional no ciberespaço.

A metodologia empregada teve abordagem dedutiva, com uma investigação qualitativa em estudos de casos onde os modelos dos Estados Unidos da América e da Organização do Tratado do Atlântico Norte foram analisados.

O trabalho teve abordagem temporal transversal e recolha de dados em pesquisas bibliográficas, análise de documentos emitidos em fontes oficiais e abertas e entrevistas com especialistas no assunto.

Os principais contributos encontrados se referem à necessidade do trabalho conjunto entre os países, o setor civil e os Governos, que deve ser buscado visando à sinergia dos esforços na busca de um ambiente cibernético mais seguro.

Além disso, uma estruturada legislação, com documentos claros e precisos, o intercâmbio de informações, exercícios cibernéticos e trabalhos conjuntos entre os países e as instituições nacionais são necessários.

Por fim, verificou-se que a formalização da Política Nacional de Segurança Cibernética no Brasil deve ser emanada pelos altos escalões do setor político para guiar os esforços na busca de um ciberespaço nacional mais seguro.

Palavras-chave: Segurança, Defesa, Cibernética, Segurança e Defesa Cibernética, Guerra Cibernética

Abstract

This research analyzed the Organization for Cyber Security and Defense in Brazil with the objective of proposing contributions to its improvement. The study is relevant in view of the growing threats to national security in cyberspace.

The methodology used had a deductive approach, with a qualitative investigation in case studies where the models of the United States of America and the North Atlantic Treaty Organization were analyzed.

The work had a transversal temporal approach and data collection in bibliographic research, analysis of documents issued in official and open sources and interviews with experts on the subject.

The main contributions found refer to the need for joint work between countries and between the civil sector and Governments, which must be sought, aiming at synergy of efforts in the search for a safer cybernetic environment.

In addition, a structured legislation, with clear and precise documents, the exchange of information between nations, cyber exercises and joint work between countries and national institutions.

Finally, it was found that the formalization of the National Cyber Security Policy in Brazil must be issued by the highest levels of the political sector to guide efforts in the search for a safe national cyber environment.

Keywords: Security, Defense, Cybernetics, Cyber Security and Defense, Cyber War

Lista de abreviaturas, siglas e acrónimos

APFB	–	Administração Pública Federal Brasileira
CDCiber	–	Centro de Defesa Cibernética
ComDCiber	–	Comando de Defesa Cibernética
CPOG	–	Curso de Promoção a Oficial-General
CTIR.Gov	–	Centro de Tratamento e Resposta a Incidentes de Redes
DSI	–	Departamento de Segurança da Informação
EME	–	Estado-Maior do Exército
EMCFA	–	Estado-Maior Conjunto das Forças Armadas
END	–	Estratégia Nacional de Defesa
EU	–	União Europeia
EUA	–	Estados Unidos da América
FA	–	Forças Armadas
GSI	–	Gabinete de Segurança Institucional da Presidência da República
IUM	–	Instituto Universitário Militar
ITU	–	*International Telecommunication Union*
LVSC	–	Livro Verde de Segurança Cibernética
MD	–	Ministério da Defesa
NATO	–	Organização do Tratado do Atlântico Norte
OE	–	Objetivo Específico
OG	–	Objetivo Geral
ONU	–	Organização das Nações Unidas
PDN	–	Política de Defesa Nacional
PNSC	–	Política Nacional de Segurança Cibernética
PSC	–	Política de Segurança Cibernética

QC	–	Questão Central
QD	–	Questão Derivada
SISMC2	–	Sistema Militar de Comando e Controle
S&DC	–	Segurança e Defesa Cibernética
S&DCB	–	Segurança e Defesa Cibernética no Brasil
STIC2	–	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TIC	–	Tecnologia da Informação e Comunicações
USCYBERCOM	–	*U.S. Cyber Command*

1. Introdução

A humanidade está passando por um processo de evolução do conhecimento nunca antes experimentado na história. Segundo a Organização das Nações Unidas (ONU), mais de quatro mil milhões de pessoas utilizam a rede mundial (ONU, 2019). Esses utilizadores da internet e da tecnologia da informação interagem entre si, trocando informações, enviando mensagens e emails, utilizando serviços do governo, comprando pela internet, interagindo, vivendo e trabalhando no mundo virtual criado pela cibernética.

As ameaças e os riscos para a segurança e defesa nacional provenientes do ciberespaço são pouco conhecidos e complexos, decorrente da natureza classificada e da multiplicidade de fatores agentes e ameaças no ciberespaço.

Com o emprego cada vez maior da tecnologia da informação na Administração Pública Federal Brasileira (APFB) e com a crescente evolução das ameaças, o assunto tem-se tornado um assunto de primordial importância para o país.

O Brasil, quando da emissão da Política de Defesa Nacional (PDN), em 2005, já havia expressado sua intenção de atuar no ciberespaço de forma a "minimizar os danos de possíveis ataques cibernéticos, assegurando que é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento" (PDN, 2005, p.8).

O Governo demonstrou que pretende atuar fortemente no ambiente cibernético quando, através da Estratégia Nacional de Defesa (END), foram priorizados os setores espacial, nuclear e o cibernético como os três setores decisivos para a defesa nacional (END, 2008, p.6).

Este trabalho tem por assunto a organização para a Segurança e Defesa Cibernética no Brasil (S&DCB) com enfoque nos documentos já emanados pelo Governo Federal e que regulamentam o assunto, nas responsabilidades definidas para os agentes da APFB e na sua efetividade face às ameaças cibernéticas.

Este trabalho está enquadrado na seção do Estudo das Crises e dos Conflitos Armados das Ciências Militares (Decreto-Lei n.º 249/2015, de 28 de outubro), pois realiza a análise da organização da S&DCB, uma das responsabilidades das Forças Armadas, em conjunto com as demais instituições do Estado.

A investigação foi delimitada (Santos & Lima, 2019) temporalmente no período que abrange o lançamento da PDN até os dias atuais, limitando-se ao espaço cibernético brasileiro, contemplando a análise da organização da S&DCB.

O Objetivo Geral (OG) deste trabalho é de propor contributos para a organização da S&DCB, tendo por Objetivos Específicos (OE) OE1 - analisar dois modelos estrangeiros para a Segurança e Defesa Cibernética (S&DC) – Estados Unidos da América (EUA) e Organização do Tratado do Atlântico Norte (NATO), OE2 - analisar as medidas político/estratégicas e documentos governamentais expedidos para a S&DCB e OE3 - analisar a organização da S&DCB e as funções das Instituições Governamentais envolvidas nessa Segurança.

O problema de investigação delimitado foi a necessidade de melhorar a S&DCB, sendo que para isso foi formulada como Questão Central (QC): Como contribuir para a Organização da S&DCB? Além dela, foram criadas três Questões Derivadas (QD), sendo a primeira: Quais modelos dos EUA e da NATO que regulam a Segurança e Defesa Cibernética? Já a QD 2 irá investigar Quais os documentos e medidas político/estratégicas que regulam a S&DCB? A QD3 analisará: Como está organizada a S&DCB e quais as funções das principais Instituições responsáveis.

Este trabalho de investigação está organizado em sete capítulos, correspondendo o primeiro à introdução. O segundo capítulo apresenta uma revisão da literatura e a contextualização da investigação, bem como a definição de vários conceitos relativos ao tema e ao modelo de análise.

O terceiro capítulo apresenta a metodologia adotada, referindo as fases do percurso metodológico, as técnicas de recolha, tratamento e análise dos dados utilizados. O quarto capítulo analisa os modelos de organização para a S&DC nos EUA e na NATO e responde a QD1. O quinto capítulo analisa as medidas político/estratégicas e documentos governamentais expedidos para a S&DCB e responde a QD2. O sexto capítulo analisa a organização para a S&DCB e as funções das Instituições Governamentais envolvidas nessa segurança sendo assim respondida a QD3.

O capítulo sétimo apresenta a conclusão, realizando um breve enquadramento do tema, um sumário do procedimento metodológico. Ainda são apresentados, como resposta à QC, os principais resultados obtidos e contributos para a organização da S&DCB, as limitações e estudos futuros sobre a temática em questão.

2. Enquadramento teórico e conceptual

Neste capítulo será apresentado o estado da arte, alguns conceitos importantes acerca do tema da cibernética e o modelo de análise empregado no presente trabalho de investigação.

2.1. Estado da arte e revisão da literatura

De acordo com o Livro Verde de Segurança Cibernética (LVSC), com o emprego cada vez maior da tecnologia da informação na APFB e a crescente evolução das ameaças, o assunto da segurança cibernética tem-se tornado um assunto de primordial importância para o Brasil e todos os países do mundo (LVSC, 2010).

Vários países do mundo já lançaram ou revisaram suas estratégias nacionais, como, por exemplo, "EUA, Reino Unido, Japão, Espanha, Austrália, dentre outros, incluindo as questões de proteção das infraestruturas críticas da Nação." (LVSC, 2010, p.28).

A NATO (2016) lançou sua Política de Segurança Cibernética (PSC) com o objetivo de proteger a Aliança e os países membros de ataques. Esse ato político e estratégico denota a contextualização da importância dada ao tema, visando a garantia da segurança do espaço cibernético.

2.1.1 Cibernética

O termo cibernética possui origens remotas e algumas mais atuais. A origem remota seria na Grécia antiga, onde o filósofo Platão servia-se da palavra cibernética, em grego *Κυβερνήτης* (pronunciada *kubernêtes)*, que significa piloto, para designar a arte de pilotagem, bem como, num sentido figurado, a arte de dirigir os homens (Wiener, 1970).

O matemático Norbert Wiener publicou sua obra *Cybernetics: or the Control and Communication in the Animal and the Machine*, na qual apresenta as hipóteses e os fundamentos da cibernética, fruto de anos de investigações e troca de experiências com intelectuais de diversas áreas científicas, dentre as quais se podem citar as ciências sociais (Wiener, 1970).

Wiener já considerava que o tema era algo tão familiar a ponto de achar que o seu livro, intitulado Cibernética, já estaria ultrapassado em 1970, quando da sua edição.

No contexto deste trabalho, a cibernética pode ser remetida à comunicação e controle, atualmente relacionada ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação no espaço virtual (MD31-M-07, 2014).

No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de

Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais (MD31-M-07, 2014).

2.1.2. Espaço Cibernético ou Ciberespaço

Carvalho (2011, p.31) afirma que o mar era um grande desconhecido para os navegadores portugueses e espanhóis à época das grandes navegações e que agora o espaço cibernético é o grande desafio para o mundo contemporâneo, onde não existem referências nem modelos para a sua conquista.

Richard Clarke (2010, p. 10), autor norte-americano, considera o ciberespaço como o "quinto domínio da guerra, após a terra, o mar, o ar e o espaço sideral." Essa evolução tem tudo a ver com a evolução do uso do ciberespaço no mundo. Para Clarke (2010, p.10), o *cyberspace* seria, então, o quinto domínio a ser conquistado e utilizado pelo ser humano nas suas ações.

O ciberespaço foi reconhecido pela NATO e por várias nações do mundo como um novo domínio operacional, tão crítico para a defesa nacional quanto os domínios da terra, do mar, do ar e do espaço, conforme pode-se verificar na Figura 1 apresentada em seguida (NATO, 2016, pp.70-71).

No Brasil, a definição de espaço cibernético foi adotada no manual do Ministério da Defesa (MD), que trata da Doutrina das Operações, como sendo o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (MD31-M-07, 2011, p.43).

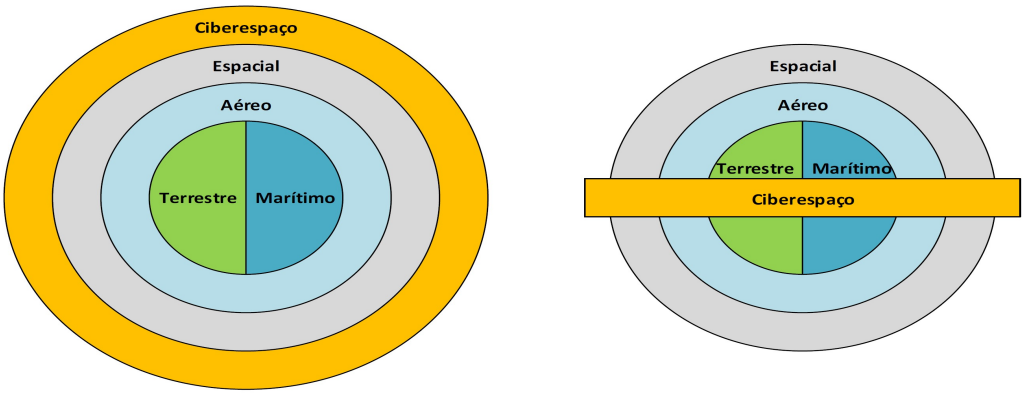

Figura 1 – Representações usuais dos cinco espaços/domínios
Fonte: Honorato (2016).

2.1.3. Ameaça Cibernética

"Causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse" (MD31-M-07, 2014, p.18).

2.1.4. Infraestruturas Críticas

O conceito de infraestruturas críticas está expresso na Doutrina Militar de Defesa Cibernética (MD31-M-07, 2014, p.18) como sendo as instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, económico, político, internacional ou à segurança do Estado e da sociedade.

2.1.5. Defesa Cibernética

É o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (MD31-M-07, 2014, p.19).

2.1.6. Segurança Cibernética

De acordo com a *International Telecommunication Union* (ITU), a segurança cibernética é a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e propriedades de usuários(as) (ITU, 2008).

A União Europeia (EU) define o conceito como o conjunto de salvaguardas e ações que se podem empregar para proteger o domínio cibernético, tanto no âmbito civil quanto militar, frente às ameaças vinculadas com suas redes interdependentes e sua infraestrutura de informação, ou que possam afetar estas (*European Comission*, 2013).

No Brasil, Segurança Cibernética é definida como a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, os seus ativos de informação e as suas infraestruturas críticas (MD31-M-07, 2014, p.19).

2.1.7. Guerra Cibernética

O manual MD30-M-01 (2011) já considerava que os ataques cibernéticos fariam parte da ameaça assimétrica, ou seja, aquela ameaça decorrente da possibilidade de serem empregues meios ou métodos não ortodoxos, que incluem terrorismo, ataques cibernéticos, armas convencionais avançadas e armas de destruição em massa para anular ou neutralizar

os pontos fortes de um adversário, explorando suas fraquezas, a fim de obter um resultado desproporcional.

A Guerra Cibernética corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar (MD31-M-07, 2014, p.19).

Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC (MD31-M-07, 2014, p.19).

2.1.8. Teoria Realista das Relações Internacionais

A Teoria Realista das Relações Internacionais de Hans Morgenthau possibilita um maior entendimento dos fatores sociais que afetam as nações e podem alterar a ordem vigente entre as nações, sendo que as crises e os conflitos armados internacionais são as de maior importância (Morgenthau, 1948, cit. por Candian, 2021).

Dessa forma, depreende-se que o ambiente cibernético revela ameaças devido à sua grande vulnerabilidade e as transformações significativas em curso o transformam em um novo e promissor campo de batalha, a quinta dimensão deste campo, ou domínio onde os conflitos ocorrerão.

Para Candian (2021), a obra de Morgenthau possui grande relevância no esforço de chefes de Estado e estudiosos do tema no sentido de compreender, de forma mais precisa, o papel de cada ator e os possíveis desdobramentos de crises do sistema internacional. A situação que está a ocorrer na Segurança e na Defesa Cibernética a nível mundial pode ser um exemplo delas, havendo necessidade de maior aprofundamento deste conceito.

2.1.9. Infraestrutura Crítica da Informação

Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (MD31-M-07, 2014, p.19).

2.1.10. Poder Cibernético

Capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder (MD31-M-07, 2014, p.19).

2.1.11. Resiliência Cibernética

Capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa (MD31-M-07, 2014, p.19).

2.1.12. Domínios Operacionais

Segundo o MD31-M-07 (2014, p.18), o espaço cibernético é um dos cinco domínios operacionais e permeia todos os demais. São eles: o terrestre, o marítimo, o aéreo e o espacial, que são interdependentes e estão representados na Figura 2.

Segundo Carneiro (2017), as atividades no Espaço Cibernético podem criar liberdade de ação para atividades em outros domínios, assim como atividades em outros domínios também criam efeitos dentro e através do Espaço Cibernético.

O objetivo central da integração dos domínios é a habilidade de se alavancar capacidades de vários domínios para que sejam criados efeitos únicos e, frequentemente, decisivos (Carneiro, 2017).

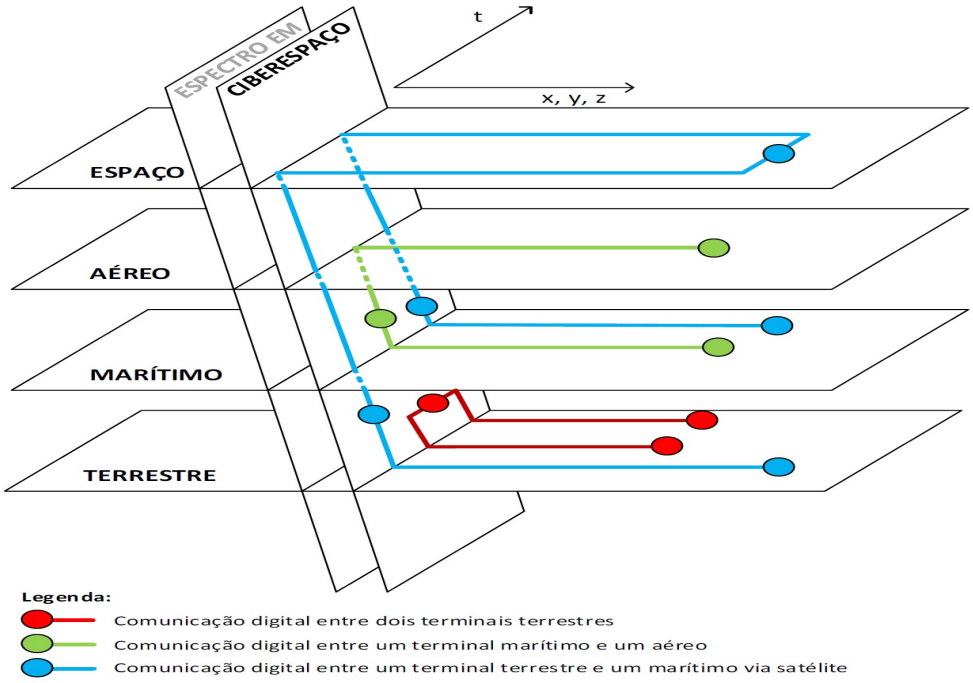

Figura 2 – Representação do ciberespaço em relação aos demais espaços
Fonte: Honorato (2016).

2.2. Modelo de Análise

O modelo de análise encontra-se disponível no Apêndice A (Apd – A).

3. Metodologia

Esta investigação foi realizada de acordo com a metodologia vigente no Instituto Universitário Militar (IUM) (Santos & Lima, 2019), com base snas Normas de Execução Permanente (NEP) aprovadas, INV 001 (IUM, 2020a) e INV 003 (IUM, 2020b) e foi seguida a norma da *American Psychological Association* (Fachada, Ranhola, Marreiros & Santos, 2019).

A metodologia empregada pode ser visualizada melhor na Figura 3, apresentada em seguida.

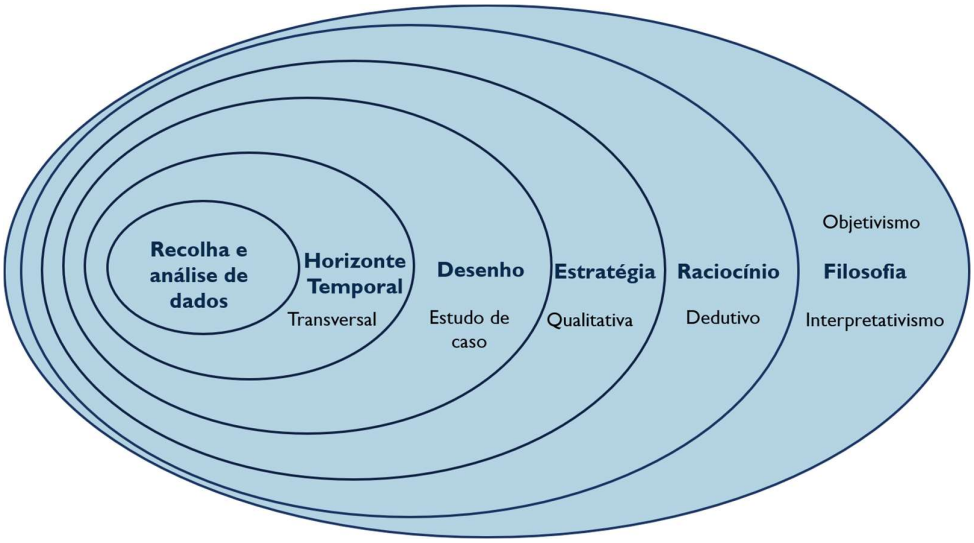

Figura 3 - "Cebola" da investigação
Fonte: Adaptado a partir de Saunders et al. (2009, cit. por Santos & Lima, 2019).

No processo de raciocínio adota-se uma abordagem dedutiva, atendendo à observação de modelos gerais [de teorias] para aplicação num aspeto particular da realidade (Santos & Lima, 2019, p. 19). Por outras palavras, o investigador "[…] parte da lei geral para o particular, ou seja, raciocinar dedutivamente, partindo da teoria em busca de uma verdade" (Santos & Lima, 2019, p. 19).

A investigação foi realizada de forma qualitativa, tendo em consideração que este trabalho procura compreender uma realidade complexa de modo abrangente, onde temos vários sistemas diferentes e em mutação, onde a análise e os principais dados foram obtidos através de documentação constante de fontes abertas e entrevistas semiestruturadas (Santos & Lima, 2019, pp. 27-29).

Foi realizado estudo de caso, sendo realizada a confrontação exaustiva da teoria com os múltiplos modelos existentes (Santos & Lima, 2019, p. 36).

Em termos de horizonte temporal foi realizada uma abordagem transversal, atendendo a que se vai proceder à "[…] recolha de dados de mais de um caso, num determinado instante de tempo, de forma a coligir dados quantitativos ou qualitativos, com uma ou mais variáveis, que após a sua análise permitem detetar padrões de associação, estabelecendo a variação" (Bryman, 2012, cit. por Santos & Lima, 2019, p. 33).

No que toca à recolha de dados, foram realizadas intensas pesquisas bibliográficas, análise de documentos emitidos em fontes oficiais e abertas e entrevistas por vídeo chamada e por *e-mail* com especialistas no assunto que ocupam funções relevantes na organização da S&DCB.

Foram entrevistados o senhor Marcelo Paiva Fontenele, Diretor do Departamento de Segurança da Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI). Senhor Victor Hugo da Silva Rosa, Coordenador-Geral da Coordenação-Geral de Gestão de Segurança da Informação do DSI. Senhor Ulisses Peixoto Pinto Neto, Assessor Técnico do Centro de Tratamento e Resposta a Incidentes de Redes (CTIR.Gov) do GSI. Senhor Marcelo António Righi, Coronel do Exército, Coordenador e Líder de *Theat Hunting* na Empresa ISH Tecnologia. O guião da entrevista se encontra no Apêndice B (Apd – B) deste trabalho.

A conclusão procurou entregar uma estrutura flexível e própria, pois, para Creswell (2010, p.26), aqueles que se envolvem na investigação qualitativa apoiam uma maneira de encarar a pesquisa que honra um estilo indutivo, um foco no significado individual e na importância da interpretação da complexidade de uma situação.

4. Modelos de Organização para a Segurança e Defesa Cibernética

A necessidade de alcançar a condição de segurança do espaço nacional cibernético e de defender este novo domínio da guerra é um fato que não pode ser relegado a segundo plano pelos Estados no século XXI.

Cerca de cento e sessenta países do mundo estão examinando ativamente e conscientemente suas capacidades de S&DC. EUA, Rússia e China lideram a corrida, seguidos pela Índia, Irão, Coreia do Norte, Japão e Israel (SAE, 2011, p.79). Serão analisados, em seguida, os modelos dos EUA e da NATO de S&DC.

4.1. Estados Unidos da América

Os primeiros esforços norte-americanos para lidar com os riscos de segurança da informação em sistemas computacionais ocorreram no final dos anos sessenta, quando o Departamento de Defesa (DoD) iniciava a interligação de seus computadores e pretendia proteger e controlar o acesso a dados e informações sigilosas (Branco Júnior, 2005, p.49).

Schwartau (1996, pp. 43 e 79) afirmou que os EUA estavam fadados a enfrentar um *Pearl Harbor* eletrónico caso não começassem a desenvolver políticas e implementar procedimentos defensivos. Para tanto, alertava que a sinergia seria vital para a sobrevivência na guerra da informação.

4.1.1. Dimensões Política e Estratégica

A *Presidential Decision Directive* 63 (PDD-63, 1998), assinada em maio de 1998, pelo então Presidente dos EUA, Bill Clinton, estabeleceu uma estrutura sob a liderança da Casa Branca para coordenar as atividades dos departamentos e agências, em parceria com atores do setor privado. Tal iniciativa tinha por objetivo eliminar vulnerabilidades contra ataques físicos e cibernéticos nas infraestruturas críticas dos EUA.

Essa diretriz, considerada a primeira dos EUA a tratar do assunto da segurança cibernética, foi reformulada e, no ano de 2003, foi lançada a *National Strategy to Secure Cyberspace* (NSSC, 2003), que definia que o ciberespaço é o sistema nervoso, o sistema de controle do país.

A NSSC (2003) apresentava cinco prioridades nacionais na área cibernética. A primeira prioriza a melhoria da resposta aos incidentes cibernéticos e reduzir o dano potencial de tais eventos. As segunda, terceira e quarta prioridades visam reduzir as ameaças e as vulnerabilidades a ataques cibernéticos. A quinta prioridade é destinada a minimizar os ataques cibernéticos que poderiam afetar os ativos de segurança nacional e melhorar a gestão internacional de resposta a esses ataques.

Com a finalidade de dar sinergia ao processo de cibersegurança, foram criadas agências e organizações governamentais. As missões e tarefas foram estabelecidas de forma que o processo fosse gerenciado e contextualizado através de medidas ativas e passivas na área cibernética (NSSC, 2003).

Branco Júnior (2005, pp. 27-28), em seu trabalho elencou algumas das organizações governamentais dos EUA que tratam da temática cibernética naquele país:

• *National Security Agency* (NSA) ou Agência de Segurança Nacional, que tem por missão, dentre outras, operar o sistema de monitoramento global Echelon e proteger as comunicações relativas à segurança nacional, enquanto explora as de outros países;

• *National Computer Security Center* (NCSC), que conduz a segurança dos sistemas de informação dentro da NSA;

• *National Institute of Standards and Technology* (NIST), órgão do Departamento do Comércio responsável pelo desenvolvimento de políticas e programas relacionados com a proteção de informações sensíveis não sigilosas;

• *Defense Information Systems Agency* (DISA), que trata de segurança de TI no Departamento de Defesa;

• *Computer Emergency Response Team Coordination Center* (CERT-CC) que coordena várias outras equipes de resposta a emergência nos EUA;

• *Federal Computer Incident Response Center* (FEDCIRC), que tem por missão prover uma ampla capacidade de resposta a incidentes no âmbito governamental;

• *Office of Science and Technology Policy* (OSTP), que coordena pesquisa e desenvolvimento em apoio à proteção de infraestruturas críticas;

• *Office of Management Budget* (OMB) que desenvolve, supervisiona e implementa políticas governamentais, princípios, padrões e regras para programas do governo federal para a segurança computacional;

• *Central Intelligence Agency* (CIA);

• *Department of Justice*;

• *Federal Bureau of Investigation* (FBI);

• *Defense Intelligence Office for Information Operations*, criado em virtude da necessidade de conhecer o potencial que eventuais adversários poderiam ter em realizar "ataques digitais" e, também, com o objetivo de apoiar as atividades relacionadas a *information operations*;

• *Joint Task Force – Computer Network Operations* (JTF-CNO), responsável por ações defensivas e ofensivas de guerra cibernética;

• *Information Assurance Technology Analysys Center* (IATAC) que mantém um repositório de informações sobre técnicas e ferramentas de segurança e para a condução de conferências e treinamentos; e

• *Information Assurance Division, C4 Directory* (J6K) é responsável pelas ações que visam assegurar a supremacia da informação.

Vários modelos de segurança cibernética são seguidos dos EUA, como *frameworks* (NIST por exemplo) e que são colocados como melhores práticas para a instituição e que orientam as ações, tanto operacionais como de *compliance* (M. A. Righi, entrevista por email, 05 de fevereiro de 2022).

Em maio de 2011, os EUA deram um grande passo na busca da regulação política na área cibernética. A Estratégia Internacional para o Ciberespaço (EIC) estabeleceu a visão dos EUA para o futuro da Internet, e estabelece uma agenda de parcerias com outras nações e povos para alcançar a segurança cibernética (NSSC, 2011).

Os EUA consideram seu papel extremamente importante e relevante para a segurança do ciberespaço afirmando que os norte-americanos possuem a oportunidade de construir o sucesso do seu país no ciberespaço e garantir o futuro dele para a comunidade global (NSSC, 2011).

Nesse contexto, depreende-se que, se os EUA estão interessados na segurança global no ciberespaço, é de vital interesse que este espaço seja controlado e a sua segurança mantida pela ação estatal tanto no âmbito interno quanto no âmbito internacional (NSSC, 2011). Dessa forma, é essencial a delimitação das fronteiras no espaço cibernético com sua demarcação bem realizada e sua defesa definida.

O documento revela que o futuro de um ciberespaço aberto, seguro, confiável e interoperável, depende de nações que reconhecem e salvaguardam que devem dar suporte e confrontar aqueles que tentam desestabilizar ou enfraquecer o ciberespaço e o mundo conectado (NSSC, 2011, p.3).

Além disso, os Estados devem proteger as infraestruturas de informação e os sistemas nacionais de danos ou contra uso indevido. O direito de autodefesa é citado como sendo uma resposta para os atos agressivos no ciberespaço (NSSC, 2011, p.10).

Para concretizar a segurança do espaço cibernético e ajudar a promulgar normas de direito sobre o tema, os EUA irão combinar diplomacia, segurança e desenvolvimento para

aumentar a prosperidade, a segurança e a abertura de forma que todos possam se beneficiar da tecnologia da rede. Estas três abordagens são fundamentais para os esforços a nível internacional (NSSC, 2011).

Para os EUA, um ataque nas redes de uma nação pode ter impactos danosos que vão muito além das fronteiras cibernéticas. O país tem o direito de responder a atos hostis no ciberespaço como seria para qualquer outra ameaça real e factível (NSSC, 2011).

Segundo a NSSC (2011, p.10), todos os Estados possuem o direito inerente de legítima defesa, certos atos hostis realizados através do ciberespaço podem obrigar a ações coerentes e de acordo com os compromissos assumidos com os Estados aliados.

Os EUA se reservam ao direito de utilizar os meios diplomático, informativo, militar e econômico – que forem necessários e justos, de acordo com o direito internacional, a fim de autodefesa e de seus aliados e seus interesses (NSSC, 2011, p.14).

O país empregaria todos os meios antes da força militar, sempre que possível; sempre levando em conta os custos e riscos da ação contra os custos da inação, em busca da legitimidade, buscando apoio na comunidade das nações, sempre que possível (NSSC, 2011, p.14).

Hosang (2011) considera que a NSSC pode ser utilizada como base para a construção de uma Política Nacional Cibernética no Brasil, levando em conta o avançado nível tecnológico e a experiência dos EUA em atividades relacionadas ao tema.

4.1.2. Dimensões de S&DC

Além dos órgãos que tratam de forma direta ou indireta do assunto, o *Department of Homeland Security* dos EUA criou um exercício para simular um ambiente de guerra cibernética, o *Cyber Storm*. Esse exercício de defesa cibernética é conduzido a cada dois anos pelo governo norte-americano desde o ano de 2006. O primeiro exercício foi chamado de *Cyber Storm* I (CISA, 2022).

O exercício *Cyber Storm* II ocorreu em 2008 e foi importante pelo fato de envolver a participação de cinco países (Austrália, Canadá, Nova Zelândia, Reino Unido e EUA), nove estados dos EUA e mais de quarenta empresas do setor privado. Foi o marco do início da cooperação internacional em busca da segurança cibernética (CISA, 2022).

Já foram realizados sete exercícios, sendo que *Cyber Storm* VIII está programado para ocorrer em meados de 2022 (CISA, 2022).

O CTIR Gov, equipe do DSI, coopera com instituições homólogas de outros países, entre elas a *Cybersecurity & Infrastructure Security Agency* (CISA), dos EUA (V. H. S. Rosa, entrevista por email, 02 de fevereiro de 2022).

Mais um importante passo foi tomado pelo governo dos EUA quando, em junho de 2009, o Presidente Barak Obama anunciou a criação do *U.S. Cyber Command* (USCYBERCOM), um novo comando subordinado à NSA, com sede no *Fort Meade,* localizado em Maryland , com estrutura apresentada na Figura 4 (USCYBERCOM, 2022).

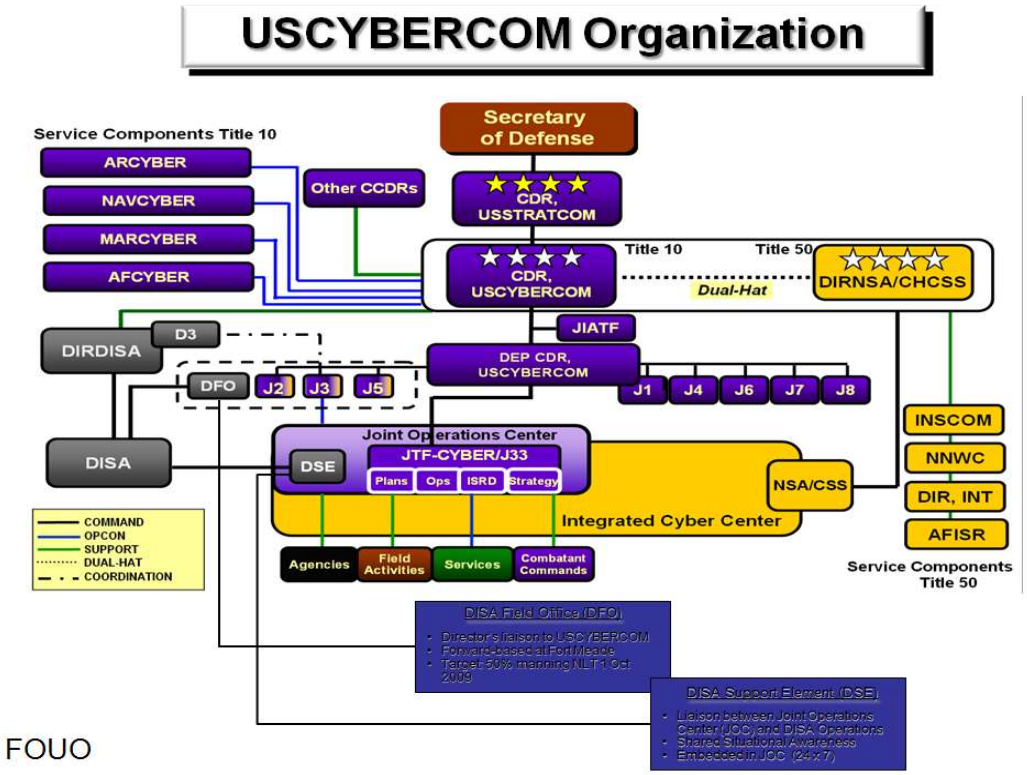

Figura 4 – USCYBERCOM - Organograma
Fonte: USCYBERCOM (2022).

A missão do USCYBERCOM é de coordenar, integrar, sincronizar e conduzir atividades para as operações de defesa de redes de informação e, quando autorizado, realizar operações militares de amplo espectro no ciberespaço, a fim de permitir ações em todos os cinco domínios (ar, mar, terra, espaço e ciberespaço) e garantir aos EUA e seus aliados a liberdade de ação no ciberespaço, negando o seu uso aos adversários (USCYBERCOM, 2022).

4.2. Organização do Tratado do Atlântico Norte

Denning (2001, p.274) considera que as operações militares em Kosovo, no ano de 1999, foram a primeira experiência da NATO com a ameaça cibernética. Durante esse conflito, ativistas e beligerantes de ambos os lados usaram a web para divulgar suas aspirações e sua causa.

O autor apresenta que, houve também uma série de invasões nas redes privadas e governamentais, a maioria com a finalidade de propaganda e de protesto. Em alguns casos, hacktivistas (forma pela qual são conhecidos os ativistas cibernéticos) enviaram vírus e tentaram derrubar sistemas e corromper informações.

Além das partes envolvidas no conflito, hackers chineses, após o bombardeio acidental dos EUA na Embaixada Chinesa em Belgrado, participaram dos ataques cibernéticos contra as forças da NATO (Denning, 2001, p.274).

Em 2010, a NATO já considerava que os ataques cibernéticos estavam se tornando mais frequentes, mais organizados e mais caros nos danos que eles causam nas administrações governamentais, empresas, economias, transportes, redes de abastecimento e infraestruturas críticas, pois podem atingir um limiar que ameaça a prosperidade, a segurança e a estabilidade nacionais e da própria NATO (2010).

Em 2021, a NATO comunicou que os ataques cibernéticos poderiam ser tratados da mesma forma que uma ação militar contra qualquer um de seus membros e que poderia considerar uma resposta militar contra países que apoiaassem grupos nos ataques no ciberespaço (CISO, 2021).

Segundo CISO (2021), pode ser invocado o artigo 5º do tratado da NATO, caso a caso, após um ataque cibernético. Nesse caso, um ataque armado a qualquer membro aliado será considerado um ataque a todos os membros da NATO, que deverão tomar ações para proteger o país atacado (CISO, 2021).

4.2.1. Dimensões Política e Estratégica na NATO

O conceito estratégico para defesa e segurança dos membros da NATO, adotado pelos chefes de Estado e de Governo na Conferência de Lisboa, realizada em 2010, refletiu a preocupação do bloco militar sobre o tema cibernético e direcionou as ações a serem tomadas em caso de ataques cibernéticos contra os países membros e seus aliados (NATO, 2010).

Em 8 de junho de 2011, os Ministros de Defesa da NATO aprovaram a Política de Defesa Cibernética (PDC), definindo uma visão clara para os esforços em defesa cibernética, além de um plano de ação associado à implementação desta defesa (NATO, 2011).

Essa política oferece uma abordagem coordenada para a defesa cibernética, com foco na prevenção de ataques cibernéticos e construção da resiliência dos sistemas integrados por rede e sujeitos a ataques cibernéticos no âmbito da NATO, de forma que todas as estruturas terão proteção centralizada (NATO, 2011).

A política define mecanismos políticos e operacionais de resposta a ataques cibernéticos e integra a resposta a ciberataques contra seus membros. A política também estabelece a forma como a NATO vai ajudar os seus aliados em seus próprios esforços de defesa cibernética, com o objetivo de otimizar a partilha de informações, a consciência situacional, a colaboração e a interoperabilidade cibernética segura, baseada em padrões definidos pelos membros da Aliança (NATO, 2011).

O documento estabelece prioridades na defesa cibernética, além do desenho da sua governança, conforme Figura 5. Ele reconhece que a crescente sofisticação dos ataques cibernéticos, a necessidade de proteção das redes de informação da Aliança e os sistemas de infraestruturas críticas dependem de ações sinérgicas e proativas para sua segurança (NATO, 2011).

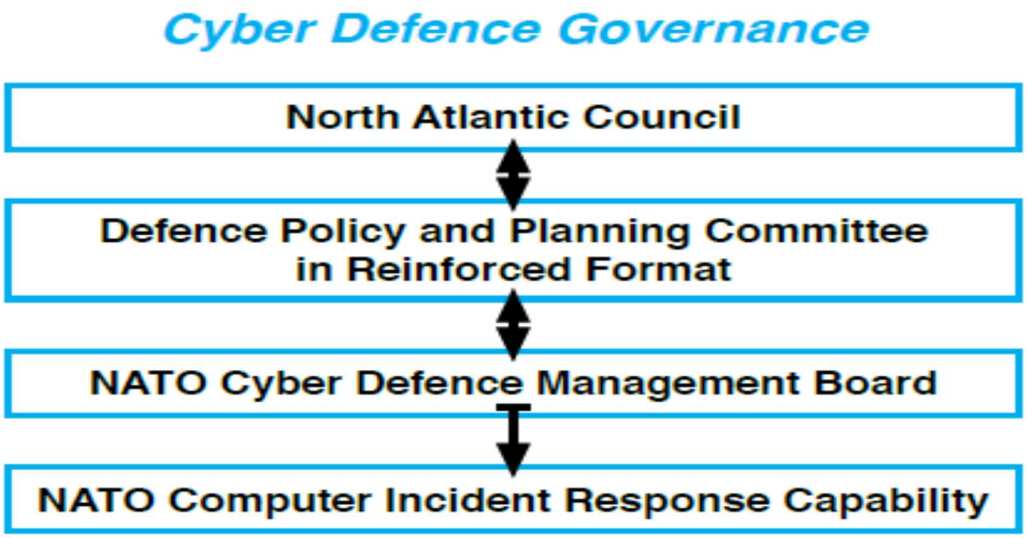

Figura 5 – Governança de Defesa Cibernética da NATO
Fonte: NATO (2011, p.1).

Os esforços baseiam-se nos princípios gerais da prevenção, da resiliência e da não duplicação de esforços, ou sinergia dos processos. A PDC prevê que qualquer resposta de defesa coletiva está subordinada a decisões do conselho da Aliança como um todo. (NATO, 2011, p.2)

Conforme afirma V. H. S. Rosa, (op. cit.), quanto à NATO afirma, o DSI entende que é organização da área de Defesa Cibernética, portanto, as interlocuções com aquela Organização são de competência do Ministério da Defesa e das Forças Singulares. Contudo, o DSI acompanha publicações da NATO e eventualmente participa em eventos seus, que sejam encaminhados pelo Ministério da Defesa e possam trazer subsídios à área de segurança cibernética.

O nível político define os princípios que guiarão a defesa cibernética da NATO com os países parceiros, organizações internacionais, o setor privado e a área acadêmica.

4.2.2. Dimensões de Segurança e Defesa Cibernética na NATO

O ataque cibernético contra a Estônia, em 2007, foi o mais conhecido incidente cibernético relacionado com a NATO. Depois que um memorial de guerra soviético foi retirado de Tallinn, capital do país, ocorreram vários protestos de ativistas de etnia russa nas ruas da cidade. Os protestos espalharam-se pela rede e originaram vários ataques de negação de serviço contra sites do governo, jornais e bancos da Estónia (V. H. S. Rosa, op. cit.).

Estes ataques levaram à criação do Centro de Excelência de Defesa Cibernética Cooperativa da NATO (CCDCOE) para gerenciar defesa cibernética de todos os membros da Aliança. A CCDCOE tem como países fundadores a Estónia, a Alemanha, a Itália, a Letônia, a Lituânia, a Eslováquia e a Espanha, que se uniram para estabelecer o centro em 2008 (CCDCOE, 2022).

Situado na capital da Estônia, em Tallinn, o CCDCOE tem a missão de promover a cooperação, criar as capacidades e estimular o compartilhamento de informações entre os países da NATO sobre segurança cibernética. São realizados exercícios de defesa cibernética, oficinas de direito e de política cibernética, cursos, palestras técnicas, com o objetivo de preparar os países da NATO para a deteção e combate a ataques cibernéticos no âmbito da Aliança (CCDCOE, 2022).

O CCDCOE é financiado e composto pelos seguintes países: Alemanha, Áustria, Bélgica, Canadá, Croácia, República Checa, Dinamarca, Estónia, Finlândia, França, Grécia, Hungria, Islândia, Itália, Japão, Letónia, Lituânia, Luxemburgo, Montenegro, Holanda, Noruega, Polónia, Portugal, Roménia, Eslováquia, Eslovénia, Coreia do Sul, Espanha, Suécia, Suíça, Turquia, Reino Unido e EUA (NATO, 2010).

Já em 2010, a NATO (2010) pretendia desenvolver ainda mais a capacidade de prevenir, detetar, defender e recuperar os seus sistemas de ataques cibernéticos, empregando o processo de planejamento para reforçar e coordenar as capacidades de defesa cibernética,

trazendo todos os membros sob a proteção cibernética centralizada, e uma melhor integração da NATO no alerta e na resposta com os países membros.

Segundo TECNODEFESA (2021), em 2021, foi realizado o exercício *Locked Shields*, que durou um ano e envolveu dois países virtuais que estavam combatendo ameaças das *deepfakes*, instabilidade nos sistemas financeiros e de controle, além das novas ameaças surgidas com a pandemia da covid-19, como os crescimentos da automação e do trabalho remoto.

Ao longo de todo o exercício, 5 mil sistemas virtuais foram alvejados por mais de 4 mil ataques cibernéticos. Além de defenderem os sistemas, os participantes tiveram de lidar com simulações de problemas legais e mediáticos (TECNODEFESA, 2021).

O exercício foi organizado pelo Centro de Excelência em Defesa Cibernética Cooperativo (CCDCOE), órgão ligado à NATO, e foi realizado de forma remota, reunindo mais de 2 mil especialistas de 32 países, segundo o informado no sitio TECNODEFESA (2021).

4.3. Síntese conclusiva e resposta à Questão Derivada 1

Respondendo à QD1, a qual procurou analisar quais modelos dos EUA e da NATO que regulam a S&DC, foi analisada a PDC adotada pela NATO em 2011 e sua comparação com a estratégia adotada pelos EUA leva a crer que as duas seguiram os mesmos princípios básicos, com a edição de Políticas e Estratégias de S&DC pelos mais altos níveis Institucionais e políticos, e que esses princípios priorizam as parcerias e as alianças entre Estados e Instituições.

Além disso foi criada uma estrutura de cooperação entre entidades Estatais e Instituições privadas para que a S&DC seja efetiva e sinérgica. Exemplo disso são os exercícios conjuntos realizados entre os países, como o *Cyber Storm* realizado nos EUA, a cooperação entre os países da NATO, tendo como exemplo o *Locked Shields* e o intercâmbio, troca de informações e conhecimentos realizados na área cibernética.

O trabalho conjunto entre os Estados Nacionais, seus governos e o setor civil é buscado sempre, visando à sinergia dos esforços na busca de um ambiente cibernético mais seguro. Uma estruturada legislação, principalmente com uma PDC (EUA) ou uma Estratégia bem estruturada como a da NATO, com documentos claros e precisos e uma regra clara e sinérgica, o intercâmbio de informações entre as nações, exercícios e trabalhos conjuntos entre os países são os elementos que se destacam dos modelos analisados.

Do que foi apresentado, verificou-se em ambos os casos analisados, que uma PDC deve ser emanada pelos altos escalões do setor político para guiar os esforços na busca da S&DC, sendo base para a busca de um ciberespaço mais seguro, além da manutenção dos intercâmbios, exercícios e trabalhos com outras nações amigas.

5. Principais Medidas Político Estratégicas e Documentos Governamentais da Segurança e Defesa Cibernética no Brasil

HUREL (2021) apresenta duas linhas do tempo com os principais desenvolvimentos institucionais e políticos para a S&DCB, conforme as Figuras 6 e 7 a seguir.

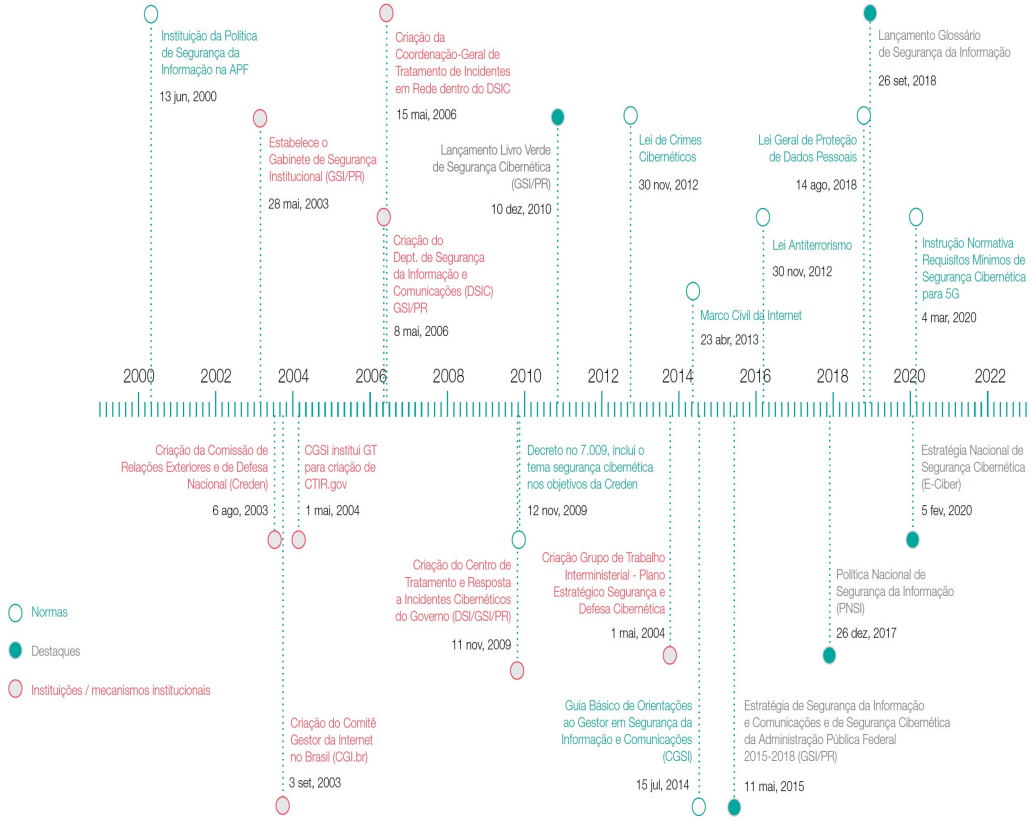

Figura 6 - Linha do Tempo: Segurança Cibernética no Brasil (Administração Pública Federal)
Fonte: Hurel, 2021.

Hurel (2021) afirma que, apesar da linha do tempo apresentar mais de vinte anos de trabalhos, na prática, o desenvolvimento de uma série de leis e normas sobre a cibernética foi impulsionada em 20127/13 com a Lei de Crimes Cibernéticos e as informações reveladas por Edward Snowden, que contribuíram sobremaneira para a construção do Marco Civil da Internet.

Como pode-se ver na Figura 6, há mais de dez anos, o Brasil desenvolve capacidades cibernéticas para defesa, tendo como marco inicial o reconhecimento do setor cibernético como um dos pilares estratégicos para a defesa nacional em 2008, com a END (Hurel, 2021).

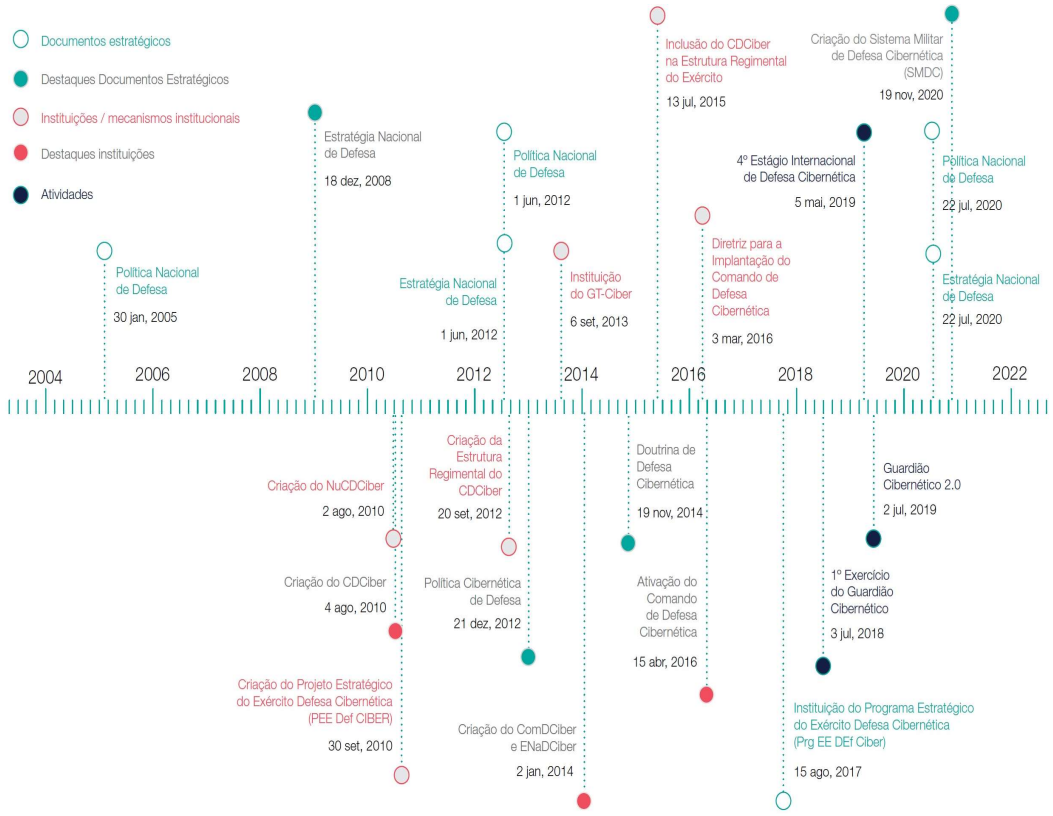

Figura 7 - Linha do Tempo: Defesa Cibernética no Brasil (Administração Pública Federal)
Fonte: Hurel, 2021.

Hurel (2021) informa que ocorreu grande desenvolvimento de ações entre os anos de 2010 e 2016, ocasião em que o Brasil se preparava e sediava importantes eventos de grande visibilidade internacional (Rio Mais 20 em 2010 e as Olimpíadas de 2016).

Nesse período foi desenvolvida uma estratégica brasileira no setor, como exemplo a Política Cibernética de Defesa e a Doutrina de Defesa Cibernética, com instituições dedicadas à operacionalização e implementação de atividades de defesa cibernética, além do Centro de Defesa Cibernética (CDCiber) e o Comando de Defesa Cibernética (ComDCiber) (Hurel, 2021).

5.1. Política de Defesa Nacional de 2005

O Brasil demonstrou, com o lançamento da PDN, clara intenção governamental de atuar na S&DCB, a nível Político e Estratégico, face ao surgimento de vulnerabilidades que podem ser exploradas, com o objetivo de inviabilizar o uso dos meios no ciberespaço (PDN, 2005, p.10).

5.2. Estratégia Nacional de Defesa de 2008

Ficou ainda mais clara a intenção do Governo Federal Brasileiro de atuar expressivamente no ambiente cibernético quando, através da END, (2008, p.6) foram priorizados os setores espacial, nuclear e o cibernético como os três setores decisivos para a defesa nacional.

A independência nacional será alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento (END, 2008, p.9).

A END (2008, p.12) deixou claro que o fortalecimento dos três setores assegurará o atendimento ao conceito de flexibilidade, afirmando que esses setores transcendem a divisão entre desenvolvimento e defesa e entre o civil e o militar, indicando a necessidade do trabalho conjunto de todos os setores da sociedade buscando a Segurança Cibernética.

A Segurança Cibernética, portanto, se caracteriza como uma função estratégica de Estado, e essencial à manutenção e preservação das infraestruturas críticas de um país, tais como energia, transporte, telecomunicações, águas, finanças, informação, dentre outras (LVSC, 2010a, p.19).

A partir do estabelecimento do Setor Cibernético, decorrente da aprovação da END, em 2008, dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR), e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas, conforme Figura 8 (MD31-M-07, 2014, p.17).

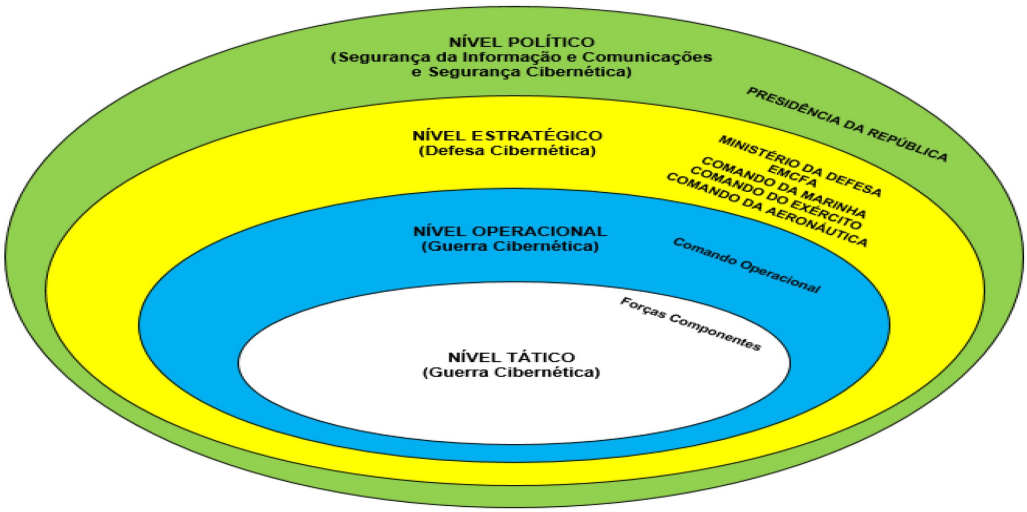

Figura 8 – Níveis de decisão
Fonte:MD31-M-07 (2014)

5.3. Livro Verde de Segurança Cibernética de 2010

O LVSC (2010) trata sobre S&DCB e foi resultado do trabalho realizado pelo Grupo Técnico instituído no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, e teve como objetivo propor diretrizes e estratégias de Segurança Cibernética. A coordenação do grupo foi exercida pelo GSI, por intermédio de seu Departamento de Segurança da Informação (DSI) (LVSC, 2010, p.19).

Segundo o LVSC (2010), as diretrizes consideradas essenciais a serem desenvolvidas para assegurar a existência e a continuidade da Sociedade da Informação da nação brasileira, garantindo e protegendo, no ciberespaço, os ativos de informação e as infraestruturas críticas do país são:

- Caracterizar a segurança cibernética como alta prioridade e de extrema urgência para o país, no curto prazo, implementando uma robusta estratégia nacional de segurança cibernética;

- Valorizar e ampliar as competências nos diversos temas que perpassam a temática da segurança cibernética, e temas correlatos, como o de segurança das infraestruturas críticas da informação, no curto e médio prazo;

- Lançar, no curto prazo, a Política Nacional de Segurança Cibernética (PNSC);

- Criar órgão central para macrocoordenação da PNSC, no curto prazo;

- Estabelecer programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, no curto, médio e longo prazo;

- Desenvolver arcabouço conceitual da segurança cibernética para o Estado brasileiro, no curto prazo;

- Estender a capacidade da defesa do país para proteção da nação no espaço cibernético; e

- Incrementar a capacidade dissuasória da defesa do país para fazer frente a ameaça cibernética.

5.4. Estratégia Nacional de Segurança Cibernética de 2020

Segundo ENISA (2022), as estratégias nacionais de segurança cibernética são documentos com ações para impulsionar a resiliência e a segurança de infraestruturas, serviços e cidadãos. Elas apresentam os principais objetivos, prioridades e princípios a serem alcançados pelo país nos anos seguintes.

De Lucca (2020) cita que o Brasil aprovou, pelo Decreto Presidencial 10.222, de 5 de fevereiro de 2020, sua E-Ciber onde estão previstas as principais ações do governo na área

de segurança cibernética entre os anos 2020-2023, tanto na área nacional, quanto na área internacional, sendo o décimo segundo país a publicar sua estratégia.

De Luca (2020) afirma que com a E-Ciber, de 2020 e uma Política ou Lei Nacional de Segurança Cibernética, o país tem a oportunidade de integrar a expertise das instituições e suas boas práticas na área em um ambiente de cibersegurança dentro de um panorama de conhecimentos e mecanismos de coordenação de outros setores.

5.5. Política Nacional de Segurança Cibernética de 2020

O Livro Verde de Segurança Cibernética já considerava em 2010 que o Brasil precisava desenvolver mecanismos que permitam sistematizar a identificação, a monitoração, a minimização e a mitigação de riscos cibernéticos, impulsionando o desenvolvimento de ações preventivas, pró-ativas, reativas, e de repressão, a todo o tipo de ameaças, **sendo necessária uma Política de Estado**, visando assegurar e defender os interesses do país e da sociedade brasileira (LVSC, 2010, p.15).

No que concerne à Segurança Cibernética, essa Política de Estado, será resultado da edição de lei que institua a PNSC, cuja elaboração da minuta do Projeto de Lei está sendo coordenada pelo GSI e está previsto na Estratégia Brasileira para Transformação Digital (E-Digital, p. 43 – Ações Estratégicas, no título '2. Defesa e Segurança no Ambiente Digital'), com vistas, entre outros objetivos, a criar uma governança de segurança cibernética em âmbito nacional (V. H. S. Rosa, op. cit.).

Nota-se que a adoção de uma PNSC é uma aspiração do setor político e estratégico nacional, deve ser precedida de análises e consensos construídos com a participação de especialistas para a viabilização e otimização do processo como um todo, criando uma agenda de Estado político-estratégica e técnica e está na lista de prioridades das autoridades que tratam do assunto (M. P. Fontenele, entrevista por vídeo conferência pela internet, 05 de fevereiro de 2022).

5.6. Síntese conclusiva e resposta à Questão Derivada 2

Como forma de responder à QD2, que buscava verificar quais documentos e medidas político/estratégicas regulam a S&DCB, verifica-se que o Brasil trilhou um caminho bem sustentado na construção dos seus principais documentos, faltando ainda a edição da PNSC, almejada há mais de 12 anos.

A PDN de 2005 lançou as bases de uma consciência cibernética, ao passo que a END em 2008 discorreu diretamente sobre o tema e o priorizou, junto com os setores espacial e nuclear como setor decisivo para a defesa nacional.

O LVSC emitiu as diretrizes básicas para a construção da PNSC. Verifica-se que as mesmas estão em consonância com os esforços internacionais e bem alinhadas com as emitidas pelos EUA e pela NATO.

A E-Ciber de 2020 foi um grande passo para a regulação da S&DCB e regulou as ações a serem tomadas no quadriênio 2020 – 2023, sendo uma base sólida para o lançamento da PNSC pelo país. A observação de que o Brasil precisa de uma política de Estado para regular o tema da segurança cibernética é importante.

Finalmente, nota-se que a criação e a **adoção de uma PNSC é uma prioridade para as autoridades** que tratam do assunto no país e que essa política deve ser estruturante para todo o sistema organizacional de segurança e defesa cibernética no Brasil.

6. Organização para a Segurança e Defesa Cibernética no Brasil

A END enumera como órgãos responsáveis pela S&DCB a Casa Civil da Presidência da República, os Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e o GSI, conforme Figura 9, a seguir (END, 2008, p. 66).

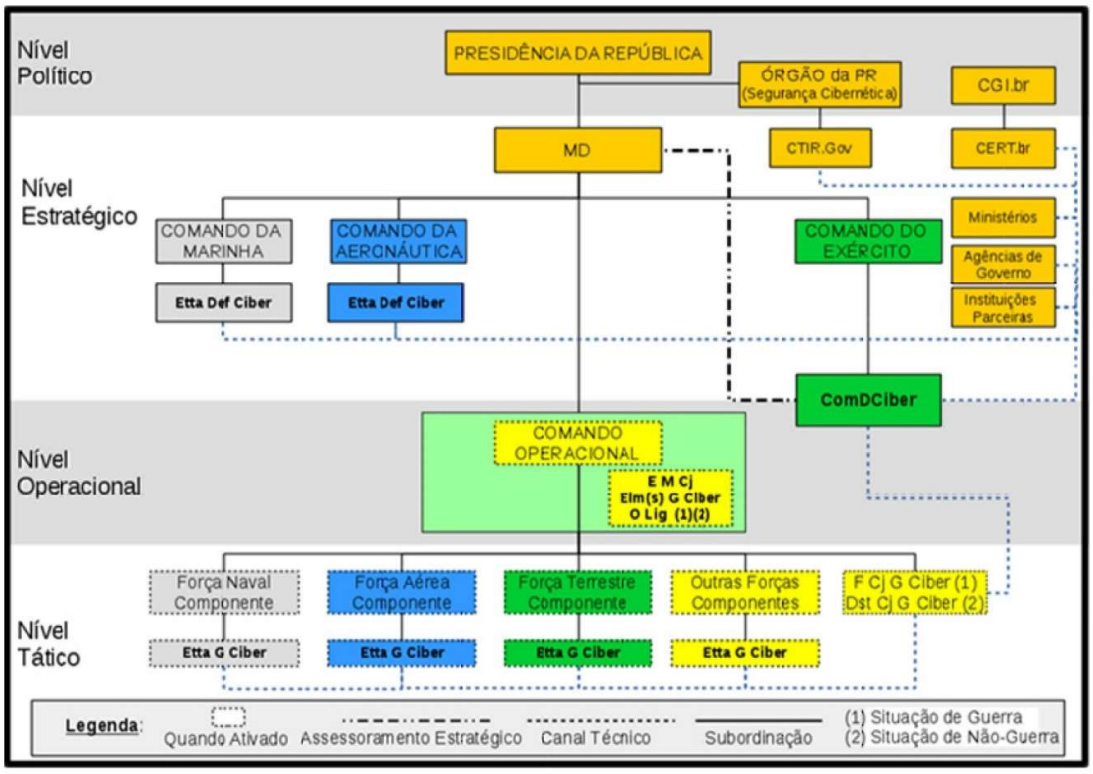

Figura 9 – Sistema Militar de Defesa Cibernética (SMDC)
Fonte: MD31-M-07 (2014)

Os principais órgãos que tratam no nível político da Segurança Cibernética são a Presidência da República, o GSI e o Comité Gestor da Internet (CGI.br) (MD31-M-07, 2014).

Os órgãos que tratam da Defesa Cibernética aparecem no nível estratégico: o Ministério da Defesa, as estruturas de Defesa Cibernética das Forças Armadas, o Estado Maior Conjunto das Forças Armadas (EMCFA) e o Comando de Defesa Cibernética (ComDCiber) (MD31-M-07, 2014).

O ComDCiber atua sob a supervisão do Ministério da Defesa e fomenta a integração técnica com outras instituições, tais como o CERT.br, os órgãos das outras Forças, os ministérios e outras entidades. O EMCFA é o responsável pelas decisões sobre as ações de defesa cibernética em casos não previstos na Doutrina Militar de Defesa Cibernética, dá

suporte ao Ministério da Defesa na gestão do Sistema Militar de Defesa Cibernética e garante a atuação conjunta das Forças Armadas (Marimón, 2019).

No nível tático aparecem os órgãos de Defesa Cibernética e as unidades de guerra cibernética de cada Força. Em 2016, o CDCiber sofreu uma alteração, deixando de estar vinculado ao Departamento de Ciência e Tecnologia do Comando do Exército e passando a ser subordinado ao Comando de Defesa Cibernética (ComDCiber) (Marimón, 2019).

6.1. Conselho De Defesa Nacional

Mandarino (2010) nos apresenta que o Conselho De Defesa Nacional (CDN) é um órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático de direito.

O CDN é órgão de Estado e não de governo, portanto não deve ser influenciado por fatores políticos de momento e tem sua secretaria-executiva exercida pelo ministro-chefe do GSI (Mandarino, 2010, p.109).

6.2. Câmara de Relações Exteriores e Defesa Nacional

A Câmara de Relações Exteriores e Defesa Nacional (CREDEN) possui missão de assessoramento ao Presidente da República nos assuntos relacionados às relações exteriores e à defesa nacional. O Ministro-chefe do GSI é seu presidente e, entre suas atribuições, encontra-se a segurança da informação, atividade essa que se insere no escopo do Setor Cibernético (SAE, 2011, p.205).

6.3. Casa Civil da Presidência da República

Responsável pela execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil) (SAE, 2011, p.20).

Tal atribuição é da competência do Instituto Nacional de Tecnologia da Informação (ITI), uma autarquia federal vinculada à Casa Civil da Presidência da República, que tem o objetivo de manter a ICP-Brasil, da qual é a primeira autoridade na cadeia de certificação, ou seja, é a Autoridade Certificadora Raiz (AC Raiz) (SAE, 2011, p.20).

6.4. Gabinete de Segurança Institucional da Presidência da República

O GSI/PR tem competência para planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da APFB, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas (V. H. S. Rosa, *op. cit.*).

V. H. S. Rosa (*op. cit.*) afirma que a estrutura, missão e principais atividades do GSI, em relação à segurança da informação e segurança cibernética, e do DSI/GSI constam nos incisos IV e V do art. 10 da Lei nº 13.844, de 18 de junho de 2019 e nos incisos IV e V do art. 1, no art. 16-A do Anexo I e no Quadro "a" do Anexo II do Decreto nº 9.668, de 2 de janeiro de 2019.

6.4.1. Departamento de Segurança da Informação e Comunicações

O DSI faz parte do GSI e tem como atribuição operacionalizar as atividades de Segurança da Informação e Comunicações (SIC) na APFB, nos seguintes aspetos (SAE, 2011, p.21):

a. Regulamentar a SIC para toda a APFB;

b. Capacitar os servidores públicos federais, bem como os terceirizados, sobre SIC;

c. Realizar acordos internacionais de troca de informações sigilosas;

d. Representar o País junto à Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético; e

e. Manter o Centro de Tratamento e Resposta a Incidentes de Redes da APFB (CTIR.Gov).

O art. 16-A do Anexo I do Decreto nº 9.668, de 2019, detalha as competências e atividades do DSI, e o Quadro "a" do Anexo II desse Decreto, apresenta a estrutura do DSI (V. H. S. Rosa, *op. cit.*).

6.5. Agência Brasileira de Inteligência

A Abin é o órgão central do Sistema Brasileiro de Inteligência (Sisbin), que tem como objetivo estratégico desenvolver atividades de inteligência voltadas para a defesa do Estado democrático de direito, da sociedade, da eficácia do poder público e da soberania nacional (SAE, 2011, p.21).

Dentre suas atribuições, no que interessa especificamente ao Setor Cibernético, destaca-se a de avaliar as ameaças internas e externas à ordem constitucional, entre elas a cibernética. Conta, em sua estrutura organizacional, com o Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações (Cepesc), que busca promover a pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações (SAE, 2011, p.21).

6.6. Ministério da Justiça

As questões afetas aos crimes cibernéticos estão entre as competências do Ministério da Justiça e Segurança Pública (políticas públicas) e das Polícias Federal e estaduais (investigação) e do Poder Judiciário (processos judiciais) (V. H. S. Rosa, *op. cit.*).

6.7. Secretaria de Assuntos Estratégicos

A Secretaria de Assuntos Estratégicos (SAE) possui a atribuição de realizar estudos e pesquisas destinados a promover o planejamento de longo prazo governamental e contribuir para a implementação da END.

Em razão dessas missões, realiza encontros para discutir, no âmbito da APFB e academia, a orientação do tema S&DC. São realizadas discussões sobre o lançamento de bases para o estabelecimento de um Sistema de S&DCB que venha a envolver também os sistemas de informação ligados às infraestruturas críticas. (SAE, 2011, p.208).

6.8. Ministério da Defesa

O MD, através de Diretriz Ministerial N° 0014 (MD, 2009), direcionou o setor cibernético para o Exército Brasileiro, enquanto o espacial e o nuclear ficaram a cargo da Aeronáutica e da Marinha, respetivamente.

O GSI tem muito cristalino o entendimento de que a competência em Defesa Cibernética é do MD e das Forças Armadas, como se depreende dos incisos do art. 27 da Lei nº 13.844, de 2019 (V. H. S. Rosa, op. cit.).

6.8.1. Estado-Maior Conjunto das Forças Armadas

Compete ao Estado-Maior Conjunto das Forças Armadas (EMCFA) elaborar o planejamento do emprego conjunto das Forças Armadas e assessorar o Ministro de Estado da Defesa na condução dos exercícios conjuntos e quanto à atuação de forças brasileiras em operações de paz, além de outras atribuições que lhe forem estabelecidas pelo Ministro de Estado da Defesa (SAE, 2011, p.209).

O EMCFA possui a função de supervisionar o ComDCiber na Estrutura Regimental do Comando do Exército. Tal Comando, já instituído, conta com o exercício de militares das três Forças Armadas, cabendo ao EMCFA as atividades de coordenação nos casos de operações conjuntas, especificando-se, em atos próprios, os aspetos inerentes ao controle operacional (Guimpbel, 2020).

6.8.2. Exército Brasileiro

Mandarino Júnior (2010) ressalta que o Departamento de Ciência e Tecnologia (DCT), é um órgão de direção setorial do Exército Brasileiro (EB) que engloba determinados vetores

de modernidade. Ao referido Departamento subordina-se o Centro de Desenvolvimento de Sistemas (CDS) e o Centro Integrado de Guerra Eletrônica (CIGE), organizações militares altamente especializadas e possuidoras de pessoal bastante capacitado a trabalhar com tal tema.

Além dos órgãos supracitados, o Instituto Militar de Engenharia (IME) é outro órgão que deve estar vinculado ao sistema em questão por ser um centro de referência nacional no que tange ao ensino e tratar de atividades de natureza técnico-científicas, tendo também, um viés de pesquisa (Mandarino Júnior, 2010, pp. 116 e 117).

Mandarino Júnior (2010) destaca que, além dos órgãos já citados, foi ativado, pela Portaria N° 667, de 4 de agosto de 2010, do Comandante do Exército, o Núcleo do Centro de Defesa Cibernética do Exército (Nu CDCiber), subordinado ao Departamento de Ciência e Tecnologia, responsável pela implantação do Centro de Defesa Cibernética do Exército (CDCiber).

6.8.3. Centro de Defesa Cibernética

Guimpbel (2020) apresenta que o Centro de Defesa Cibernética (CDCiber) foi criado por meio da Portaria Normativa nº 666 de 4 de agosto de 2010 e inaugurado em 2012 por determinação do Comando do Exército e possui a missão de proteger os sistemas de informações e neutralizar a fonte de ataques, tentando inibir possíveis ataques digitais. Ao CDCiber compete (Guimpbel, 2020):

I - assessorar o Comandante do Exército e o Ministro de Estado da Defesa nas atividades do setor, formular doutrina e obter e empregar tecnologias;

II - planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas;

III - executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa.

O CDCiber é o órgão central do SMDC, que passa ao controle operacional do MD nas Operações Conjuntas e conta, permanentemente, com um Estado-Maior Conjunto para realizar o planejamento e o controle das ações planejadas, levando em conta as particularidades de cada Força Armada, de modo a obter uma atuação sinérgica (Guimpbel, 2020).

Como anteriormente já visto, o CDCiber fomenta a integração técnica com outras instituições e outras entidades na área da Defesa Cibernética, contando com o apoio e a direção do EMCFA, que oferece suporte a atuação conjunta das Forças Armadas.

6.8.4. Comando de Defesa Cibernética

O Decreto No 8.913 de 23 de novembro de 2016, marcou a criação do Comando de Defesa Cibernética (ComDCiber), com dependência do Departamento de Ciência e Tecnologia (Guimpbel, 2020).

Guimpbel (2020) afirma que o ComDCiber conta como órgãos subordinados o CDCiber, cuja missão é executar as atividades operacionais e de inteligência no âmbito do Sistema Militar de Defesa Cibernética e a Escola Nacional de Defesa Cibernética (ENaDCiber) que tem por missão fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, nos níveis de sensibilização, conscientização, formação e aperfeiçoamento.

Guimpbel (2020) destaca que, embora sua natureza conjunta, o ComDCiber tem dependência orgânica do Comando do EB, mantendo um canal de assessoramento estratégico com o MD.

A atuação do ComDCiber, no tocante ao SMDC, ocorre sob orientação e supervisão do MD, no nível estratégico, realizando as ações de coordenação e integração do Setor Cibernético nas Forças Armadas e privilegiando, sempre que possível, uma forma de atuação conjunta (Guimpbel, 2020).

6.9. Síntese conclusiva e resposta à Questão Derivada 3

A QD3 buscou analisar como está organizada a Segurança e Defesa Cibernética no Brasil e quais as funções das principais Instituições responsáveis, nas dimensões da organização, da Segurança e da Defesa Cibernética, apresentadas no modelo de análise (Apd A).

Nesse sentido, verificou-se que o Brasil possui uma estrutura de S&DC bem robusta e presente nos níveis político, estratégico e operacional.

A Presidência da República, o GSI e o Comité Gestor da Internet (CGI.br) trabalham no nível político, gerenciando a dimensão da Segurança Cibernética e a legislação referente ao assunto.

O Ministério da Defesa, as estruturas de Defesa Cibernética das Forças Armadas, o EMCFA) e o ComDCiber atuam no nível estratégico e são os principais responsáveis pela dimensão Defesa Cibernética.

O fomento da integração técnica com as outras instituições, realizado pelo CDCiber e o EMCFA atuando como responsável pelas ações de Defesa Cibernética, oferece suporte e torna a atuação de todos os órgãos mais coordenada e sinérgica.

Verifica-se que, no entanto, essa estrutura organizacional foi implementada antes da emissão da Política Nacional de Segurança Cibernética (PNSC), uma aspiração do setor político e estratégico nacional e que está na lista de prioridades das autoridades que tratam do assunto, conforme já foi verificado no Capítulo 5 deste trabalho.

7. Conclusão

O presente trabalho procurou analisar a Organização para a Segurança e Defesa Cibernética no Brasil (S&DCB) com o objetivo de propor contributos para a sua melhoria e enquadra-se na área do Estudo das Crises e dos Conflitos Armados das Ciências Militares. O estudo se faz relevante face às crescentes ameaças surgidas à segurança nacional no ciberespaço

No decorrer do estudo, os conceitos sobre cibernética foram apresentados, principalmente aqueles ligados à S&DC e suas relações com os níveis político e estratégico, respetivamente.

A investigação foi delimitada temporalmente no período que abrange o lançamento da PDN, em 2005, até os dias atuais, limitando-se ao espaço cibernético brasileiro, contemplando a análise da organização da S&DCB.

A Questão Central idealizada foi:

Como contribuir para a Organização da S&DCB?

Foram criadas três Questões Derivadas (QD), sendo a primeira: Quais modelos dos EUA e da NATO que regulam a Segurança e Defesa Cibernética?

Verificou-se, no capítulo 4, que a NATO e os EUA editaram suas Políticas e Estratégias de S&DC pelos mais altos níveis Institucionais e políticos e esses princípios priorizaram as parcerias e as alianças entre Estados e Instituições.

Foi criada uma grande cooperação entre a NATO e os EUA e as Instituições privadas para que a S&DC fossem realmente efetivadas de forma sinérgica e eficaz.

Os EUA e a NATO priorizam o trabalho conjunto do setor civil com as Instituições governamentais, fator que deve ser buscado sempre, visando um ambiente mais seguro, com resposta efetiva contra as ameaças cibernéticas.

Uma estruturada legislação, principalmente com uma PDC (EUA) e uma Estratégia bem consolidada como a da NATO, com documentos claros e precisos, o intercâmbio de informações entre as nações, exercícios e trabalhos conjuntos entre os países, tendo como exemplo disso os exercícios conjuntos realizados, como o *Cyber Storm*, a cooperação entre com os países da NATO , o exercício Locked Shields, do qual o Brasil foi participante no ano de 2021, são os destaques verificados nos modelos analisados.

Foi verificado que tanto dos EUA e a NATO consideram os ataques cibernéticos uma ameaça a soberania dos Estados e que não descartam respostas armadas a ataques sofridos no ciberespaço.

Já a QD 2 analisou os documentos e medidas político/estratégicas que regulam a S&DCB. Nesse sentido, o Brasil seguiu os exemplos bem sucedidos nos EUA e na NATO, na formulação dos seus principais documentos que tratam da S&DC.

Verifica-se que a PDN, de 2005, foi a base de uma consciência cibernética, ao passo que a END, de 2008, priorizou a cibernética como setor decisivo para a defesa nacional.

Destaca-se, no contexto da legislação, que a iniciativa do Livro Verde de Segurança Cibernética, em 2010, foi em consonância com os esforços internacionais e bem alinhada com as diretivas emitidas pelos EUA e pela NATO orientando para a formalização de uma Política Nacional de Segurança Cibernética (PNSC) que deverá, na medida do possível, ser precedida de análises e consensos construídos com a participação de especialistas para a viabilização e otimização do processo como um todo, criando uma agenda de Estado político-estratégica e técnica.

A E-Ciber, lançada em 2020, apresentou base sólida para a Segurança e Defesa Cibernética no quadriênio 2020 – 2023, oferecendo subsídios para a construção de uma PNSC pelo Brasil. Verificou-se que, da análise que o Brasil precisa de uma política de Estado, a PNSC, para melhor definir e regular as dimensões organizacional, de segurança e de defesa cibernética nacionais.

A QD3 analisou como está organizada a S&DCB e quais as funções das principais Instituições responsáveis. Verificou-se que o Brasil possui uma estrutura de S&DC bem robusta com a Presidência da República, o GSI e o Comité Gestor da Internet (CGI.br) atuando no nível político, gerenciando a Segurança Cibernética e a legislação referente ao assunto.

Já no nível estratégico aparecem o MD, as estruturas de Defesa Cibernética das Forças Armadas, o EMCFA e o ComDCiber, principais responsáveis pela Defesa Cibernética. Na base, no nível tático, aparecem os órgãos de Defesa Cibernética e as unidades de guerra cibernética de cada Força.

O nível político é o principal responsável por gerenciar as ações, emitindo diretrizes para que os níveis estratégicos e inferiores possam colocar em prática as ações de defesa e guerra cibernética, tudo visando alcançar a sensação de segurança cibernética. A Segurança da Informação e do setor cibernético no Brasil deve ser coordenada pelo GSI através do DSI.

Como resposta direta à QC formulada para este trabalho de investigação, verificou-se que o Brasil necessita de uma PDC que deve ser emanada pelos altos escalões do setor político para guiar os esforços na busca da S&DCB, sendo base para a busca de um

ciberespaço mais seguro, além da manutenção e fomento de cooperações, dos intercâmbios, de exercícios, citando-se como exemplo o *Cyber Storm* e o *Locked Shields*, além dos trabalhos com outras nações amigas e Instituições civis na área da Segurança e Defesa Cibernética.

Em termos de contributos para o conhecimento verifica-se que a estrutura de S&DC foi implementada no Brasil antes da emissão da Política Nacional de Segurança Cibernética. Infere-se que **existe a premência da edição dessa Política**, de forma coerente com os objetivos no setor, integrada às aspirações da sociedade e do povo brasileiro.

Com uma Política Nacional de Segurança Cibernética que siga os princípios fundamentais da APFB e que seja planejada e implementada dentro de regras bem definidas, o Brasil poderá buscar uma segurança na área cibernética mais efetiva, defendendo, de forma sinérgica e integrada, os interesses nacionais e promovendo a segurança nacional nessa importante área.

As principais limitações encontradas nesta investigação foram relacionadas à dificuldade de contato com os entrevistados no Brasil, primeiramente face à diferença do fuso horário e da agenda cheia das autoridades entrevistadas. Outra limitação foi a falta de informações mais aprofundadas acerca do tema da cibernética nas fontes abertas consultadas dos EUA e da NATO.

A principal recomendação de ordem prática é a de que **a PNSC poderia ser finalizada e aprovada pelo Congresso Nacional e, após todo o processo legislativo, levada para ser sancionada pelo Presidente da República** como forma de dar maior sustentabilidade a toda a estrutura e legislação já existente no país acerca da Segurança e Defesa Cibernética.

Estudos futuros podem ser realizados aprofundando a temática principalmente na busca de melhores práticas, de maior cooperação internacional entre os países e de mitigação dos riscos no ciberespaço, tudo na busca de um ambiente cibernético mais seguro, confiável e estável.

Referências bibliográficas

Branco Júnior, P.R. (2005). Agência de inteligência e guerra cibernética: uma proposta para a Defesa Nacional. 84 f. Monografia. (Especialização em Inteligência Estratégica) – Faculdade Albert Einstein (FALBE), Brasília, 2005.

Candian, K. R. (2021). A Resposta do Conselho de Segurança das Nações Unidas à Crise Síria: Obstáculos à Paz. Trabalho de Investigação Individul (TII). Lisboa: Instituto Universitário Militar.

Carneiro, J. M. E. (2017). As relações entre Defesa e Soberania no Espaço Cibernético. Artigo apresentado no 6º Encontro ABRI. Retirado de https://www.encontro2017.abri.org.br/resources/anais/8/1498479573_ARQUIVO_artigo_ABRI_Joao_Carneiro.pdf.

Carvalho, P.S.M. (2011). O Setor Cibernético nas Forças Armadas brasileiras. Artigo publicado in Desafios Estratégicos para Segurança e Defesa Cibernética, 1. ed. Brasília. 216p.

CCDCOE. (2022). *NATO Cooperative Ciber Defense Centre of Excellence*. Retirado de https://ccdcoe.org/about-us/.

CISA. (2022). *Cibersecurity & Infraestructure Security Agency*. Retirado de https://www.cisa.gov/cybersecurity.

CISO, 2021. NATO adverte que considerará resposta militar a ciberataques. CISO Advisor. Retirado de https://www.cisoadvisor.com.br/otan-adverte-que-considerara-resposta-militar-a-ciberataques/.

Clarke, R. A. (2010). *Cyber War. The Next Threat to National Security and What to Do About It. HarperCollins ebooks.* Retirado de http://www.cloudfile.ml/~cloudmeg/?books5&k=0061962244&b=books&d=21-02-21&l=TM_pop_books_150k&fsig=babc95c&dm=bmNnLm9yZw==.

Creswell, J. W. (2010). Projeto de Pesquisa: métodos qualitativo, quantitativo e misto. Tradução Magda Lopes; consultoria, supervisão e revisão técnica desta 3a edição Dirceu da Silva. Porto Alegre: Artmed.

De Luca, C. (2020). "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". UOL. Retirado de https://porta23. blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

Denning, D. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla J, Ronfeldt D (eds) Networks and Netwars: The Future of Terror, Crime, and Militancy*. 239-288.

Decreto-Lei N.º 249/2015, de 28 de outubro. (2015). Aprova a orgânica do ensino superior militar e o Estatuto do Instituto Universitário Militar. Diário da República, 1ª série – N.º 211 – 28 de outubro de 2015, pp. 9298–9311. Ministério da Defesa Nacional.

EME. Estado-Maior do Exército. (2001). Manual de Estratégia. C 124-1. Brasília, DF.

END. Estratégia Nacional de Defesa. (2008). Presidência da República. Casa Civil. Decreto nº 6.703, de 18 de dezembro de 2008. Brasília, DF.

ENISA. (2022). *National Cybersecurity Strategies.* s.d. Retirado de https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

European Comission. EC. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruxelas, 7 fevereiro 2013. Retirado de http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

Fachada, C. P. A., Ranhola, N. M. B., & Santos, L. A. B. (2019). Regras e Normas de Autor no IUM. (2ª ed., revista atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.

Guimpel, L. P. (2020). A Estrutura da Defesa Cibernética na República Argentina e na República Federativa do Brasil, entre os anos 2014 e 2019: um estudo comparado. CAED. ESG. Rio de Janeiro. Retirado de https://repositorio.esg.br/bitstream/123456789/1176/1/CAEPE.60%20TCC%20VF.pdf.

Hosang, A. (2011). Política nacional de segurança cibernética: uma necessidade para o Brasil. Trabalho de Conclusão de Curso. Escola Superior de Guerra (ESG), Rio de Janeiro.

Hurel, L.M. (2021). Cibersegurança no Brasil: uma análise da estratégia nacional. INSTITUTO IGARAPÉ. Retirado de https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf.

Honorato, M.C., Santos, L. F. C. D. S., Mateus, R. M. J. R. (2016). O Ciberespaço como 5.º Domínio Operacional. Trabalho de Investigação de Grupo (TIG). Lisboa: Instituto Universitário Militar. Retirado de https://comum.rcaap.pt/handle/10400.26/21956.

IUM. (2020a.). NEP/INV-001(A1) – Procedimentos relativos à elaboração de Trabalhos de Investigação realizados no âmbito de cursos que não atribuem grau académico. NEP IUM.

IUM. (2020b.). NEP/INV-003(A3) - Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no IUM. NEP IUM.

ITU. (2008). *Series X: Data Networks, Open System Communications and Security - Telecommunication Security - Overview of cybersecurity*. Genebra. Retirado de http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=en>.

LVSC. Livro Verde de Segurança Cibernética. (2010). GSIPR. DSIC. Brasília, DF. Retirado de https://www.bibliotecadeseguranca.com.br/wp-content/ uploads/2015/10/Livro_ Verde_SEG_CIBER.pdf.

Mandarino Júnior, R. (2010). Recife: Cubzac, 182 p. 2010.

Marimón, A. C. (2019). Guerra Cibernética [página online]. Retirado de https://velho general.com.br/2019/03/07/guerra-cibernetica-visao-geral/.

MD. Ministério da Defesa. (2009). Diretriz Ministerial Nr 014. de 09 Nov 2009. Brasília, DF.

MD30-M-01 (2011). Ministério da Defesa. Doutrina de Operações Conjuntas. 1o Volume - MD30-M-01 – 1. ed. Brasília, DF.

MD31-M-07 (2014). Ministério da Defesa. Doutrina Militar de Defesa Cibernética. MD31-M-07, 1. ed. Brasília, DF.

MD35-G-01 – 4. (2007). Ministério da Defesa. Glossário das Forças Armadas. MD35-G-01

– 4. ed. Brasília, DF, 2007.

Morgenthau, H. J. T., Kenneth, W. (1948). *Politics among nations. The struggle for power and peace.* Retirado de http://saldanha.pbworks.com/f/Morgenthau.Politics+Among+Nations.pdf.

NATO. (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon. 2010.* Retirado de http://www.nato.int/cps/en/natolive/official_texts_68580.htm#cyber.

NATO. (2011). *The NATO Policy on Cyber Defence.* Retirado de http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

NATO. (2016). *Warsaw Summit Communiqué (at NATO Portal).* Retirado de http://www.nato.int/cps/en/natohq/official_texts_ 133169.htm#cyber.

NSSC. (2003). *National Strategy to Secure Cyberspace. February*, 2003. (Washington DC: The White House). Retirado de http://www.uscert.gov/reading_room/cyberspace_strategy.pdf.

NSSC. (2011). *International Strategy for Cyberspace. May, 2011. (Washington DC: The White House)*. Retirado de http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Obama, B. (2009). *Remarks By The President On Securing Our Nation's Cyber Infrastructure. (Washington DC: The White House).* Retirado de http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

ONU. (2019). Estudo da ONU. Retirado de https://news.un.org/pt/story/2019/11/1693711.

PDD-63. (19998). *Presidential decision directive 63. Critical infrastructure protection. The White House*. Retirado de http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

PDN. Política de Defesa Nacional (2005). Presidência da República. Casa Civil. Decreto nº

5.484, de junho de 2005. Brasília, DF, 2005. Impresso no EGGCF.

SAE. Secretaria de Assuntos Estratégicos da Presidência da República. (2011). Desafios estratégicos para segurança e defesa cibernética. 1. ed. Brasília. 216p. 2011b.

Santos, L. A. B., & Lima, J. M. M. (Coord). (2019). Orientações metodológicas para a elaboração de trabalhos de investigação. (2ª ed., revista atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Schwartau, W. (1996). *Information Warfare. Cyber terrorism: protecting your personal security in the electronic age.* Nova York: Thunder's Mouth Press, 1996. 2. ed. 768 p.

TECNODEFESA. (2021). Brasil participa do maior exercício de defesa cibernética do mundo. Redação de Tecnologia e Defesa. Retirado de https://tecnodefesa.com.br/brasil-participa-do-maior-exercicio-de-defesa-cibernetica-do-mundo/

Wiener, N. (1970). *Cybernetics, or Control and Communication in the Animal and the Machine*. 2nd ed. Trad. G. K. Ghinzberg. Polígono/USP. Retirado de http://www.citi.pt/educacao_final/trab_final_inteligenciaartificial/historiadacibernetica.html.

USCYBERCOM. (2022). *U.S. Ciber Command.* Retirado de https://www.cybercom.mil/About/Mission-and-Vision/.

Apêndice A - Modelo de análise

De acordo com o objeto de estudo, os objetivos, geral e específicos e respetivas questões, central e derivadas, foi estabelecido o modelo de análise que se apresenta no quadro seguinte.

Quadro 1 – Modelo de análise

Objetivo Geral	**Propor contributos para a Organização da Segurança e Defesa Cibernética no Brasil.**			
Objetivos Específicos	**Questão Central**	**Como contribuir para a Organização da Segurança e Defesa Cibernética no Brasil?**		
	Questões Derivadas	**Conceitos**	**Dimensões Indicadores**	**Técnicas de recolha de dados**
OE1 Analisar dois modelos estrangeiros para a Segurança e Defesa Cibernética – EUA e NATO.	QD1 Quais modelos dos EUA e da NATO que regulam a Segurança e Defesa Cibernética?	Defesa Cibernética, Segurança Cibernética.	Política. Estratégica. Segurança. Defesa.	Análise documental, pesquisa bibliográfica e entrevistas semiestruturadas.
OE2 Analisar as medidas político/estratégicas e documentos governamentais expedidos para a Segurança e Defesa Cibernética no Brasil.	QD2 Quais documentos e medidas político/estratégia-cas regulam a Segurança e Defesa Cibernética no Brasil?	Defesa Cibernética, Segurança Cibernética.	Política. Estratégica. Segurança. Defesa. Ações governamentais.	
OE3 Analisar a organização da Segurança e Defesa Cibernética no Brasil e as funções das Instituições Governamentais envolvidas nessa Segurança.	QD3 Como está organizada a Segurança e Defesa Cibernética no Brasil e quais as funções das principais Instituições responsáveis?	Defesa Cibernética, Segurança Cibernética.	Organização. Segurança. Defesa.	Análise documental, pesquisa bibliográfica e entrevistas semiestruturadas.

Apêndice B – Guião da entrevista

1. Objeto da investigação e sua delimitação

1.1 Objeto da investigação

O objeto de investigação está centrado na Organização para a Segurança e Defesa Cibernética no Brasil.

1.2 Delimitação da investigação

A investigação foi delimitada pelo investigador, para garantir a amplitude e a profundidade necessárias à abrangência deste tema, conforme os seguintes parâmetros contidos na Tabela 1.

Tabela 4. Delimitação da investigação

1	Temporal	Abrange o período do lançamento da Política de Defesa Nacional no Brasil, em 2005 até os dias atuais.
2	Espacial	Brasil.
3	Conteúdo	Contempla a análise da Organização da Segurança e Defesa Cibernética no Brasil.

1.3 Objetivos da investigação

Propõe-se conduzir a presente investigação de forma a cumprir o Objetivo Geral (OG) indicado na tabela 2. No mesmo quadro são especificados os Objetivos Específicos (OE) que se pretendem completar para que o OG possa ser atingido.

Tabela 5 − Objetivo geral e objetivos específicos

Objetivo Geral
OG – Propor contributos para a Organização da Segurança e Defesa Cibernética no Brasil.
Objetivos Específicos
OE1 – Analisar dois modelos estrangeiros para a Segurança e Defesa Cibernética – EUA e NATO.

OE2 – Analisar as medidas político/estratégicas e documentos governamentais expedidos para a Segurança e Defesa Cibernética no Brasil.

OE3 – Analisar a organização da Segurança e Defesa Cibernética no Brasil e as funções das Instituições Governamentais envolvidas nessa Segurança.

1.4 Problema da investigação

Tendo em atenção que "a formulação do problema consiste em apresentar de "forma explícita, clara, compreensível e operacional" a dificuldade que identificamos e que pretendemos resolver" (Freixo, 2011, cit. Santos & Lima, 2019, p. 50), apresenta-se o seguinte problema de investigação: necessidade de melhorar a Segurança e Defesa Cibernética no Brasil.

No âmbito do problema da investigação, e em linha com os objetivos anteriormente definidos, este capítulo apresenta a formulação da Questão Central (QC) da investigação e das três Questões Derivadas (QD) (Tabela 3).

Tabela 6 – Questão central e questões derivadas

Questão Central
QC – Como contribuir para a Organização da Segurança e Defesa Cibernética no Brasil?
Questões Derivadas
QD1 – Quais modelos dos EUA e da NATO que regulam a Segurança e Defesa Cibernética?
QD2 – Quais documentos e medidas político/estratégicas regulam a Segurança e Defesa Cibernética no Brasil?
QD3 – Como está organizada a Segurança e Defesa Cibernética no Brasil e quais as funções das principais Instituições responsáveis?

GRELHA ANALÍTICA

Quadro 2 – Grelha analítica

PROBLEMÁTICAS	DIMENSÕES
QC **Como contribuir para a Organização da Segurança e Defesa Cibernética no Brasil?**	Política. Estratégica. Segurança. Defesa. Ações governamentais.
QD 1 Quais modelos dos EUA e da NATO que regulam a Segurança e Defesa Cibernética?	Política. Estratégica. Segurança. Defesa.
QD2 Quais documentos e medidas político/estratégicas regulam a Segurança e Defesa Cibernética no Brasil?	Política. Estratégica. Segurança. Defesa. Ações governamentais.
QD3 Como está organizada a Segurança e Defesa Cibernética no Brasil e quais as funções das principais Instituições responsáveis?	Organização. Segurança. Defesa.

GRELHA DE ENTREVISTA – A SER RESPONDIDA PELO ENTREVISTADO

Quadro 3 – Grelha de Entrevista

TÓPICO	PERGUNTAS	INFORMAÇÃO PRETENDIDA	RESPOSTAS
1	Bom dia. Qual seu nome, função e órgão ou empresa na qual trabalha?	Dados pessoais e profissionais.	
2	Qual seu grau de conhecimento e experiências profissionais no assunto Segurança e Defesa Cibernética?	Conhecimento do assunto, experiência na função, participações em simpósios, trabalhos de investigação, monografias, trabalhos realizados na área, participação na construção de manuais, documentos, leis e decretos sobre o assunto.	
3	O senhor poderia discorrer sobre a estrutura, a missão, organograma e as principais atividades de sua Instituição na área de Segurança e Defesa Cibernética?	Conhecer a Instituição na qual o entrevistado trabalha ou colabora.	
4	Quais modelos dos EUA e da NATO que regulam a Segurança e Defesa Cibernética?	Verificar se o entrevistado conhece a estrutura existente nos EUA e NATO e se ele visualiza alguma similaridade ou oportunidade de obter contributos para a melhoria da Segurança e Defesa Cibernética do Brasil.	

5	Quais documentos e medidas político/estratégicas regulam a Segurança e Defesa Cibernética no Brasil?	Obter contributos do entrevistado sobre o assunto que possam elucidar como foi construída e quais modelos utilizados na regulação da Segurança e Defesa Cibernética do Brasil.	
6	Como está organizada a Segurança e Defesa Cibernética no Brasil e quais as funções das principais Instituições responsáveis?	Obter informações e mais detalhes sobre o assunto e sobre a participação da Instituição do entrevistado na Segurança e Defesa Cibernética do Brasil.	
7	Quais contributos ou melhorias o senhor, de acordo com sua experiência profissional, considera como fundamentais para a melhoria da Segurança e Defesa Cibernética do Brasil?	Obter, de forma resumida, os contributos para a Segurança e Defesa Cibernética do Brasil.	
8	O senhor teria mais alguma contribuição ou comentário adicional sobre o assunto?	Obter informações adicionais ou conclusões sobre a Segurança e Defesa Cibernética do Brasil.	

9 Considerações finais: