CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA

CC FLÁVIO DE QUEIROZ GUIMARÃES

ANÁLISE COMPARATIVA DA ESTRUTURAÇÃO DO SETOR CIBERNÉTICO NACIONAL EM FUNÇÃO DAS DOUTRINAS CIBERNÉTICAS INTERNACIONAIS

Brasília
2017

CC FLÁVIO DE QUEIROZ GUIMARÃES

ANÁLISE COMPARATIVA DA ESTRUTURAÇÃO DO SETOR CIBERNÉTICO NACIONAL EM FUNÇÃO DAS DOUTRINAS CIBERNÉTICAS INTERNACIONAIS

Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais apresentado ao Centro de Instrução de Guerra Eletrônica como requisito para obtenção do Grau de Pós-Graduação *Lato Sensu*, nível de especialização em Guerra Cibernética.

Orientador: Cap Felipe Rodrigues de Vasconcellos

Coorientador: 2ºTen OTT/BIBLIO THAIS RIBEIRO MORAES MARQUES

Brasília
2017

Ficha Catalográfica Elaborada pela Biblioteca
do Centro de Instrução de Guerra Eletrônica (CIGE)
Bibliotecária Responsável: 2° Ten Thaís Moraes CRB1/1922

G963e

Guimarães, Flávio Queiroz
Análise comparativa da estruturação do setor cibernético nacional em função das doutrinas cibernéticas internacionais. / Fulano de Tal Silva – Brasília: Centro de Instrução de Guerra Eletrônica, 2017.
51f.; il.

Trabalho de conclusão apresentado ao Curso de Guerra Cibernética para Oficiais – Centro de Instrução de Guerra Eletrônica, Brasília, 2017.

Bibliografia: f. 49-51.

1. Setor cibernético, estruturação. 2. Cibernética, doutrina. 3. Doutrina internacional. I Guimarães, Flávio Queiroz. II. Centro de Instrução de Guerra Eletrônica. III. Título.

CDD355

CC FLÁVIO DE QUEIROZ GUIMARÃES

ANÁLISE COMPARATIVA DA ESTRUTURAÇÃO DO SETOR CIBERNÉTICO NACIONAL EM FUNÇÃO DAS DOUTRINAS CIBERNÉTICAS INTERNACIONAIS

Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais apresentado ao Centro de Instrução de Guerra Eletrônica como requisito para obtenção do Grau de Pós-Graduação *Lato Sensu*, nível de especialização em Guerra Cibernética.

Aprovado em: 27 de novembro de 2017.

_____

Cap Felipe Rodrigues de Vasconcellos

Orientador

_____

2º Ten OTT/BIBLIO Thais Ribeiro Moraes Marques

Coorientador

_____

Maj Anderson Lellis Alves Moura

Membro da comissão de avaliação

_____

1º Ten Vinícius Luís Paludeto

Membro da comissão de avaliação

Brasília
2017

Ao meu filho, João Pedro, que este trabalho lhe sirva de inspiração futura.

AGRADECIMENTOS

A Deus por ter me guiado com energia, sabedoria e equilíbrio para que eu pudesse ter logrado êxito em mais uma meta pessoal.

À Marinha do Brasil, que me proporcionou condições para dedicação exclusiva ao curso, em especial ao Capitão de Fragata Salmon e Capitã de Corveta Kátia, que me incentivaram e apoiaram na condução das minhas atribuições na DCTIM, por ocasião da minha ausência, acreditando no meu vindouro sucesso e cumprimento desta importante missão.

Aos senhores membros da banca examinadora, por terem manifestado seus juízos de valor, contribuindo sobremaneira para o aperfeiçoamento deste trabalho.

Ao meu orientador e coorientadora, Capitão Vasconcellos e 2º Ten Thais, pela forma objetiva e profissional com que me conduziram durante o processo de pesquisa.

Aos amigos das demais forças, pelo ambiente de camaradagem, agradeço o convívio e ambiente agradável proporcionados neste período de bancos escolares.

À minha família, amada esposa Andrea e querido filho João Pedro, pela inspiração que vocês me deram, paciência e palavras de carinho e estímulo que sempre me revitalizaram nos momentos difíceis desta singradura. Agradeço pela compreensão de minhas ausências e apoio incondicional.

Descobri como é bom chegar quando se tem paciência. E para se chegar, onde quer que seja, aprendi que não é preciso dominar a força, mas a razão. É preciso, antes de mais nada, querer.

Amyr Klink

RESUMO

Referência: GUIMARÃES, Flávio de Queiroz. **Análise Comparativa da Estruturação do Setor Cibernético Nacional em Função das Doutrinas Cibernéticas Internacionais,** 2017. 50 folhas. Monografia (Curso de Guerra Cibernética para Oficiais) - Centro de Instrução de Guerra Eletrônica, Brasília, 2017.

A preocupação com as consequências dos ataques cibernéticos vem se tornando o foco das atenções mundiais nos últimos anos. O avanço da tecnologia de controle das infraestruturas críticas das nações permite que a guerra cibernética obtenha um efeito cinético, impactando diretamente na proteção da sociedade. De forma a minimizar essas ameaças emergentes, os Estados vem adotando doutrinas de forma a criar uma estratégia cibernética nacional de defesa. Ao analisar o setor cibernético desses países, pode-se perceber que, foram priorizados diferentes segmentos na concepção do setor cibernético como a capacitação técnica, a defesa de infraestruturas críticas, os tratados de cooperação e impacto da guerra cibernética no desenvolvimento econômico. Percebe-se ainda, que há pontos básicos em comum entre os componentes da doutrina de defesa cibernética dos Estados. A partir dessa análise, é possível comparar e observar que, de forma geral, a doutrina e o setor cibernético brasileiro se coadunam com a dos países pesquisados.

Palavras-chave: Estratégia cibernética. Setor cibernético. Guerra cibernética.

ABSTRACT

Concern over the consequences of cyber attacks has become the focus of world attention in recent years. The advancement of technology to control the critical infrastructures of nations allows cyber warfare to have a kinetic effect, directly impacting the protection of society. In order to minimize these emerging threats, States have been adopting doctrines in order to create a national cyber defense strategy. In analyzing the cybernetic sector of these countries, it can be seen that different segments were prioritized in the design of the cyber sector, such as technical training, defense of critical infrastructures, cooperation treaties and the impact of cyber warfare on economic development. It is also noticed that there are basic points in common between the components of the cyber defense doctrine of the States. Based on this analysis, it is possible to compare and observe that, in general, the doctrine and the Brazilian cyber sector are in line with that of the countries surveyed.

Keywords: Cyber strategy. Cyber sector. Cyber warfare.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ANSSI	Agência Nacional de Segurança de Sistemas de Informação
CCN	Centro Criptológico Nacional
ComDCiber	Comando de Defesa Cibernética
CDCiber	Centro de Defesa Cibernética
CNS	Conselho Nacional de Segurança
CNSC	Conselho Nacional de Segurança Cibernética
CSDSN	Centro de Situação do Departamento de Segurança Nacional
DoD	Department of Defense
DSIC	Departamento de Segurança da Informação e Comunicações
END	Estratégia Nacional de Defesa
EUA	Estados Unidos da América
FA	Forças Armadas
GCHQ	Government Communication Headquarters
GOSCC	Global Operations and Security Control Centre
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IGC	Índice Global de Cibersegurança
JCC	Joint Concept on Cyberspace
JIOWC	Joint Information Operations Warfare Center
LBDN	Livro Branco de Defesa Nacional
MD	Ministério da Defesa
NCSC	National Cyber Security Center
NuCDCiber	Núcleo do Centro de Defesa Cibernética
NOSC	Network Operations Security Centers
PDN	Política de Defesa Nacional
RENASIC	Rede Nacional de Segurança da Informação e Criptografia

SMDC	Sistema Militar de Defesa Cibernética
SISMC2	Sistema Militar de Comando e Controle
TIC	Tecnologia da Informação e Comunicação
UIT	União Internacional de Telecomunicações
USCYBERCOM	United States Cyber Command
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command

SUMÁRIO

1 INTRODUÇÃO

As rápidas mudanças devido ao desenvolvimento da tecnologia causou impactos substanciais no processo de guerra. A Tecnologia da Informação e Comunicação (TIC) é um dos principais agentes de mudança ao utilizar o espaço cibernético como um domínio para exploração da força oponente. Algumas das diferenças entre os setores cibernéticos dos países, parecem ser problemas de maturidade na compreensão do domínio do espaço cibernético. A tradução de estratégias de guerra de outros domínios para uma arte operacional cibernética é um processo que está em fase de iniciação em muitos países. Já outras nações, estão mais avançadas, com seus setores cibernéticos e doutrinas mais consolidadas.

1.1 PROBLEMA

É essencial para o desenvolvimento do setor cibernético de um Estado moderno estabelecer uma compreensão abrangente do que é necessário para se defender de uma guerra cibernética. A identificação das dependências que uma Força Armada tem em relação à TIC está associado à definição dos ativos necessários à defesa cibernética, que por conseguinte, está correlacionado à definição de uma doutrina de defesa cibernética. Nesse contexto, é possível definir o quão desigual estará a doutrina e o setor cibernético brasileiro quando comparado com os países com doutrinas e setores cibernéticos considerados maduros?

1.2 JUSTIFICATIVA

Ao longo das últimas décadas, os avanços tecnológicos transformaram a comunicação e a capacidade de adquirir, disseminar e utilizar as informações. Por outro lado, estes avanços ampliaram a superfície de ataque do espaço cibernético. Como consequência, as Forças Armadas modernas avançaram nas suas capacidades de defesa e ataque cibernético através do estabelecimento de doutrinas. A convergência das operações cibernéticas militares em prol de objetivos

econômicos, mostra que as infraestruturas críticas são objetivos militares viáveis em tempos de guerra. Assim, a Internet e a TIC vem se tornando um domínio viável de conflito militar. A implementação de um ataque cibernético poderia ser rapidamente preparada por um grupo relativamente pequeno e poderia ser lançado sem qualquer comunicação prévia, de qualquer lugar e contra qualquer possível ativo de TIC. Dependendo da vulnerabilidade explorada, pode-se em questão de minutos indisponibilizar uma infraestrutura crítica nacional (PARRISH, 2011). Isso significa que cada Estado moderno deve estar preparado para ser alvo de um ataque cibernético e estar pronto para lançar uma contra-ofensiva efetiva. Para tal, faz-se necessário o estabelecimento de uma doutrina de defesa cibernética e um ganho de maturidade no setor cibernético.

1.3 DELIMITAÇÃO DO TEMA

Analisou-se a doutrina e estrutura do setor cibernético brasileiro e a de seis países considerados consolidados na área de segurança cibernética, de acordo com o Índice Global de Segurança Cibernética de 2017, publicado pela União Internacional de Telecomunicações (UIT), órgão especializado das Nações Unidas para os assuntos de TIC. A UIT vem publicando desde 2014, o documento denominado Índice Global de Cibersegurança (IGC), que mede o compromisso dos 193 Estados-Membros da UIT com a segurança cibernética, apoiando a identificação de áreas de melhoria, sob o aspecto legal, técnico, organizacional e de capacitação e cooperação internacional (INTERNATIONAL TELECOMMUNICATION UNION, 2017). Foram estudadas as doutrinas dos seguintes países, de acordo com a classificação do ICG:

a) Estados Unidos (2º);
b) Estonia (5º);
c) França (8º);
d) Reino Unido (12º);
e) Holanda (15º);
f) Espanha (19º).

De acordo com o IGC 2017, o Brasil se encontra em 38º.

1.4 OBJETIVOS

A seguir, têm-se os objetivos, geral e específicos, a que o presente trabalho se propôs atingir, visando apresentar a solução do problema em questão.

1.4.1 Objetivo Geral

O objetivo deste trabalho é comparar a estruturação e doutrina do setor cibernético brasileiro com as estruturas e doutrinas já consolidadas de outras nações com setor cibernético maduro.

1.4.2 Objetivos Específicos

A fim de fundamentar o alcance do objetivo geral, definiu-se os seguintes objetivos específicos, de forma a organizar uma sequência lógica de raciocínio:

a) Identificar a doutrina e organização atual do setor cibernético de países com maior maturidade de desenvolvimento; e
b) Identificar a doutrina e organização atual do setor cibernético brasileiro; e
c) Verificar a aderência da doutrina e setor cibernético brasileiro às demais doutrinas e setores estudados.

1.5 MÉTODO DE PESQUISA

Utilizado fundamentos técnicos, com base em pesquisa bibliográfica e documental, compreendendo as seguintes técnicas:

a) estudo documental, baseado nas doutrinas de guerra cibernética de países com elevados níveis de maturidade no setor cibernético;
b) método comparativo, com o objetivo de identificar semelhanças e compreender divergências entre as doutrinas de guerra cibernética; e
c) coleta de material de estudo a partir da Internet, por meio de documentos oficiais e artigos acadêmicos.

1.6 ESTRUTURA DO TRABALHO

Os documentos referem-se à doutrina e política nacional de segurança cibernética e documentos legais, incluindo as estratégias nacionais de segurança e defesa cibernética e atos legais relevantes.

1.7 REFERENCIAL TEÓRICO

A revisão literária proporcionou identificar dois níveis estratégicos de definição da estruturação de segurança cibernética adotada pelos países:

a) Uma Estratégia Nacional de Segurança e Defesa, com o propósito de documentar no mais alto nível de planejamento, o estabelecimento de objetivos e diretrizes de segurança e defesa para todos os setores considerados estratégicos, incluindo-se o setor cibernético estatal; e

b) Uma Estratégia Nacional de Segurança Cibernética, com propósito de definir especificamente a estruturação do setor cibernético estatal.

A revisão literária está organizada em documentos de países europeus, documentos norte-americanos e documentos brasileiros, de acordo com os Quadros 1, 2 e 3, respectivamente.

Quadro 1 - Publicações de Estratégia Nacional de Segurança e Defesa e publicações de Estratégia Nacional de Segurança Cibernética de países europeus

País	Estratégia Nacional de Segurança e Defesa	Estratégia Nacional de Segurança Cibernética
Estônia	• National Security Concept of Estonia (2010) • National Defence Strategy (2010)	• Cyber Security Strategy (2008) • Cyber Security Strategy (2014)
França	• White Paper: Defence and National Security (2008)	• Information Systems Defence and Security - France's Strategy (2011)
Espanha	• National Security Strategy: Sharing a Common Project (2012)	• National Cyber Security, a Commitment for Everybody (2012) • National Cyber Security Strategy (2013)
Reino Unido	• A Strong Britain in an Age of Uncertainty: The National Security Strategy (2010)	• The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World (2011) • National Cyber Security Strategy (2016)
Holanda	• National counterterrorism strategy (2011) • International Security Strategy (2013)	• Defence Cyber Strategy (2012) • National Cyber Security Strategy 2 (2013)

FONTE: Próprio autor (2017).

Quadro 2 - Publicações de Estratégia Nacional de Segurança e Defesa e publicações de Estratégia Nacional de Segurança Cibernética norte-americanas

País	Estratégia Nacional de Segurança e Defesa	Estratégia Nacional de Segurança Cibernética
Estado Unidos	• National Security Strategy (2015)	• The National Strategy to Secure Cyberspace (2003) • Cyberspace Policy Review (2009) • International Strategy for Cyberspace (2011) • Department of Defense Strategy for Operating in Cyberspace (2011) • Strategy for Improving Critical Infrastructure Cybersecurity (2014) • President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity (2013) • The Department of Defence Cyber Strategy (2015)

FONTE: Próprio autor (2017).

Quadro 3 - Publicações de Estratégia Nacional de Segurança e Defesa e publicações de Estratégia Nacional de Segurança Cibernética brasileiras

País	Estratégia Nacional de Segurança e Defesa	Estratégia Nacional de Segurança Cibernética
Brasil	• Política de Defesa Nacional PDN (2005) • Estratégia Nacional de Defesa END (2008) • Livro Branco de Defesa Nacional LBDN (2012) • Minuta da Política Nacional de Defesa PND (2017) • Minuta do Livro Branco de Defesa Nacional LBDN (2017) • Minuta da Estratégia Nacional de Defesa END (2017)	• Livro Verde: Segurança Cibernética no Brasil (2010) • Política Cibernética de Defesa (2012) • Doutrina Militar de Defesa Cibernética (2014)

FONTE: Próprio autor (2017).

2 DOUTRINA E ESTRUTURA DO SETOR CIBERNÉTICO DE PAÍSES EUROPEUS

Para comparação do estudo com países europeus, foram escolhidos aqueles com maior maturidade no setor: Estônia, França, Reino Unido, Holanda e Espanha.

2.1 ESTÔNIA

Em 2008, a Estônia foi um dos primeiros países do mundo a adotar uma Estratégia Nacional de Segurança Cibernética. A estratégia foi elaborada pelo Ministério da Defesa delineando como principais áreas: a aplicação de um sistema de medidas de segurança; desenvolvimento de experiência e conhecimento na segurança da informação; desenvolvimento de uma regulamentação e estrutura legal para suportar uma segura operacionalidade dos sistemas de informação e promover cooperação internacional com o objetivo de fortalecer a segurança cibernética global (EUROPEAN DEFENCE AGENCY, 2010).

Em setembro de 2014, publicou-se a Estratégia de Segurança Cibernética liderada pelo Ministério da Assuntos Econômicos e Comunicação, com segmentos dos setores público, privado e da academia, com os objetivos de garantir a proteção dos sistemas de informação dos serviços vitais, através da definição de métodos para a operação ininterrupta e a resiliência dos serviços e a protecção das infraestruturas críticas de informação contra ameaças cibernéticas (ESTÔNIA, 2014).

A coordenação geral da política de segurança cibernética é de responsabilidade do Ministério de Assuntos Econômicos e Comunicações. O Conselho de Segurança Cibernética do Comitê de Segurança do Governo, como um órgão interinstitucional, vem apoiando, desde 2009, a cooperação estratégica interinstitucional supervisionando a implementação dos objetivos estratégicos da segurança cibernética no país.

No âmbito das Forças armadas, o Ministério da Defesa (MD) é a autoridade coordenadora da defesa cibernética nacional. Em 2014, foi instituído o Departamento de Política de Segurança Cibernética do Ministério da Defesa, composto por especialistas em tecnologia e política de segurança, coordenando o desenvolvimento de sistemas de informação e tecnologia da informação no âmbito do MD.

As Forças de Defesa da Estônia possuem um Batalhão de Sinais,

responsável por assegurar a disponibilidade e a funcionalidade das comunicações estratégicas das Forças de Defesa, comunicação estratégica e tecnologia da informação, sob a coordenação do Centro de Comunicação Estratégica. O Centro é o responsável pela administração, manutenção e controle das medidas relacionadas à tecnologia da informação e às redes e projetos de pesquisa e desenvolvimento de guerra eletrônica, orientados para a defesa e planejamento da segurança cibernética.

Além do MD, a defesa cibernética nacional é apoiada pela Unidade de Defesa Cibernética, organização da Liga de Defesa da Estónia, que inclui profissionais de segurança cibernética de entidades públicas e privadas. A Liga de Defesa da Estónia é uma organização que atua na área do governo, no âmbito do Ministério da Defesa integrando o sistema nacional de defesa.

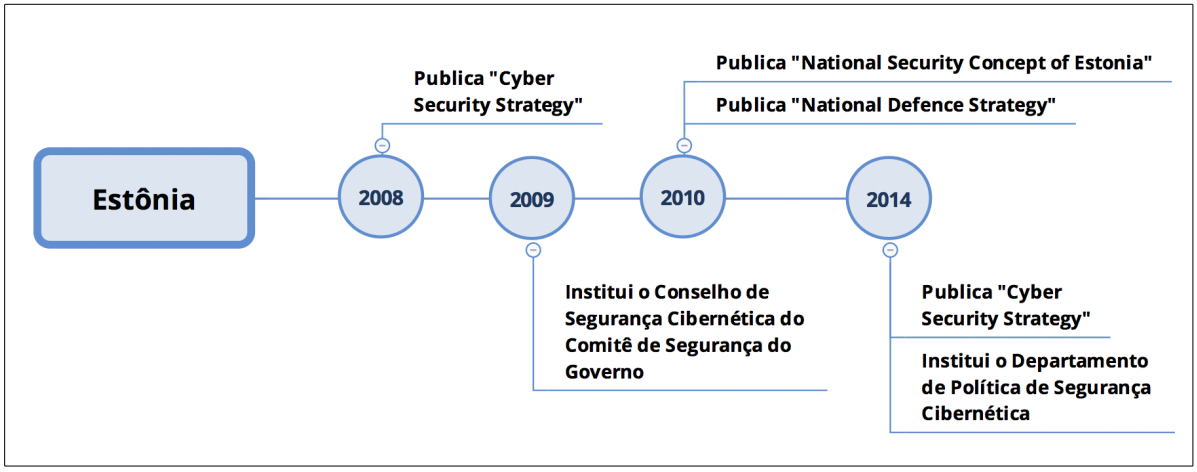
No Quadro 4, tem-se a estrutura principal do setor cibernético da Estônia. A Figura 1, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da Estônia.

Quadro 4 - Estrutura principal do setor cibernético da Estônia

Principais Órgãos	Principais Responsabilidades
Ministério de Assuntos Econômicos e Comunicações	Coordenação geral da política de segurança cibernética.
Conselho de Segurança Cibernética do Comitê de Segurança do Governo	Cooperação estratégica interinstitucional supervisionando a implementação dos objetivos estratégicos da segurança cibernética no país.
Ministério da Defesa	Coordenação da defesa cibernética nacional.
Departamento de Política de Segurança Cibernética do Ministério da Defesa	Coordenação do desenvolvimento de sistemas de informação e tecnologia da informação no âmbito do Ministério da Defesa.
Unidade de Defesa Cibernética da Liga da Defesa da Estónia	Apoio à defesa cibernética nacional, incluindo profissionais de segurança cibernética de entidades públicas e privadas.

FONTE: Próprio autor (2017).

Figura 1 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da Estônia



FONTE: Próprio autor (2017).

2.2 FRANÇA

Em 2008, o Ministério da Defesa francês emitiu o Livro Branco sobre Defesa e Segurança Nacional, no qual enfatizou a ameaça de ataques cibernéticos de grande escala, contra as infraestruturas críticas, como a mais importante preocupação de segurança nacional. O documento desenvolveu a estratégia de defesa cibernética em duas vertentes: através da introdução de um conceito de defesa cibernética organizado em profundidade, coordenado pela Agência Nacional de Segurança de Sistemas de Informação (ANSSI), sob a autoridade direta do primeiro-ministro e sob a competência da Secretaria-Geral de Defesa e Segurança Nacional e o estabelecimento de uma capacidade de guerra cibernética (FRANÇA, 2008). A missão da Agência é detectar e implementar reações precoces a ataques cibernéticos; apoiar o desenvolvimento de produtos e serviços confiáveis para instituições estatais e atores econômicos; aconselhar e apoiar instituições estatais e operadores de infraestrutura vital, bem como aumentar a conscientização e comunicar ativamente sobre ameaças cibernéticas (VITEL; BLIDDAL, 2015).

Em 2011, a Secretária-Geral da Defesa e Segurança Nacional publicou a Estratégia Francesa de Defesa e Segurança dos Sistemas de Informação, destacando a garantia da soberania da informação da França e liberdade de decisão, a melhoria da segurança cibernética das infraestruturas críticas e manutenção da privacidade no espaço cibernético (FRANÇA, 2011). A França

organizou sua segurança e defesa cibernética de forma centralizada, de acordo com suas tradições históricas do estado, bastante diferentes das abordagens realizadas por outros Estados com estruturas descentralizadas, como por exemplo, os Estados Unidos.

O Ministério da Defesa francês desenvolve e opera sistemas complexos de informação e comunicação, em particular os relacionados às suas armas mais sofisticadas, como o arsenal nuclear do país. O MD, portanto, possui suas próprias estruturas de segurança e defesa que trabalham em estreita colaboração com a ANSSI e outros ministros encarregados das tarefas de segurança cibernética. Em 2011, o Ministério da Defesa francês instituiu o conceito de Defesa Cibernética Conjunta, definindo a estrutura, os princípios e as capacidades necessárias para operações militares no espaço cibernético na qual o MD estabeleceu sua organização para a defesa cibernética. (VITEL; BLIDDAL, 2015).

A Doutrina Conjunta criou o cargo de Oficial Encarregado Geral da Defesa Cibernética sob o Chefe de Defesa francês, ficando no topo da cadeia de comando operacional para a segurança cibernética e a defesa nas forças armadas francesas. O Encarregado da Defesa Cibernética cumpre o papel operacional no Centro de Planejamento e Operações, sendo responsável pelo planejamento, coordenação e conduta de defesa cibernética no que diz respeito aos sistemas de informação no âmbito do MD.

Já o Ministro do Interior, atua à medida que as tarefas de segurança e defesa cibernéticas não estejam tão claras quanto ao papel a ser desempenhado pela ANSSI e o Ministério da Defesa. Os esforços de segurança cibernética do Ministério do Interior também foram fortalecidos por duas iniciativas em 2014 e 2015, onde o governo promulgou uma lei de combate ao terrorismo, intensificando a proibição do uso da Internet para a desestabilização nacional, ao introduzir a noção de "ameaça através do espaço cibernético". A lei também implementou disposições de segurança cibernética, como "patrulhas cibernéticas" contra o crime organizado; a introdução do roubo de dados digitais como infração criminal; penas mais severas para ataques organizados em sistemas automatizados de processamento de dados estatais e a facilitação de pesquisas de dados computadorizados e decodificação de dados criptografados (VITEL; BLIDDAL, 2015). Em 2016, o governo francês anunciou a criação do seu Comando Cibernético, de forma a incrementar a capacidade cibernética ofensiva e defensiva (REEVE, 2016).

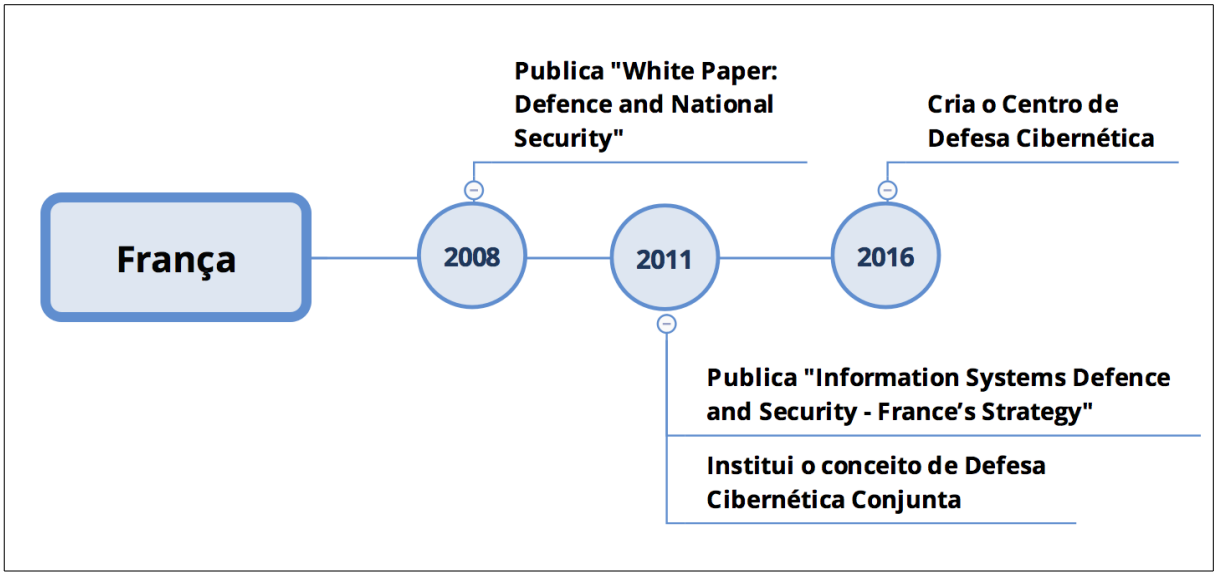
No Quadro 5, tem-se a estrutura principal do setor cibernético da França. A Figura 2, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da França.

Quadro 5 – Estrutura principal do setor cibernético da França

Principais Órgãos	Principais Responsabilidades
Agência Nacional de Segurança de Sistemas de Informação	Detectar e implementar reações a ataques cibernéticos; apoiar o desenvolvimento de produtos e serviços confiáveis para instituições estatais e atores econômicos.
Ministério da Defesa	Coordenação da defesa cibernética nacional.
Centro de Planejamento e Operações	Planejar, coordenar e conduzir a defesa cibernética no que diz respeito aos sistemas de informação no âmbito do MD.
Ministério do Interior	Atuar nas tarefas de segurança e defesa cibernética que não estejam bem definidas para a execução do MD e ANSSI.

FONTE: Próprio autor (2017).

Figura 2 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da França



FONTE: Próprio autor (2017).

2.3 REINO UNIDO

Em 2010, o Reino Unido publicou a sua Estratégia de Segurança Cibernética, destacando a responsabilidade individual dos usuários do espaço cibernético, tanto aqueles de empresas privadas, quanto aqueles usuários domésticos e profissionais. A estratégia anunciou que as agências de inteligência, em conjunto com o Ministério da Defesa, teriam um papel importante na redução das vulnerabilidades e ameaças do espaço cibernético. A sede de comunicação do governo, Government Communication Headquarters (GCHQ), é a agência de inteligência britânica responsável por proporcionar a inteligência de sinais, de forma a disponibilizar informações ao governo e às forças armadas do Reino Unido, sob a responsabilidade do Secretário de Estado para Relações Exteriores, que possui um papel central na sincronização de todos os esforços na área cibernética (UK GOVERNMENT, 2011).

Em 2011, o governo do Reino Unido emitiu uma revisão da doutrina de Defesa, denominada “Securing Britain in an Age of Uncertainty: e Strategic Defence and Security Review”, cujo principal objetivo foi anunciar um financiamento de 650 milhões de libras esterlinas para um novo Programa Nacional de Segurança Cibernética, de forma a investir nos departamentos e agências que possuem um papel fundamental na segurança cibernética. O documento também apresentou uma nova organização, o UK Defense Cyber Operations Group, que passou a realizar a integração da segurança cibernética no âmbito do Ministério da Defesa (UK PRIME MINISTER’S OFFICE, 2010).

Neste período, as Forças Armadas britânicas foram expandidas com duas novas unidades cibernéticas. A primeira é a Unidade Cibernética Conjunta como parte do novo Global Operations and Security Control Centre (GOSCC) do Reino Unido, hospedado no GCHQ. O GOSCC possui o objetivo de desenvolver novas táticas, técnicas e planos para entregar os efeitos militares através de operações no espaço cibernético, atuando como um centro de defesa cibernética das forças armadas. Uma segunda Unidade Cibernética Conjunta incorporada no GOSCC, desenvolve e usa uma série de técnicas, incluindo medidas proativas contra as ameaças à segurança da informação do Reino Unido. Embora não tenha sido declarado e documentado abertamente, no âmbito cibernético das Forças Armadas britânicas, as forças estão habilitadas para realizar operações de defesa cibernética,

operações cibernéticas ofensivas e operações de exploração cibernética (DUCHEINE; OSINGA; SOETERS, 2012).

Em 2016, o governo britânico publicou a Estratégia de Segurança Cibernética 2016-2021 (NÚCLEO DA ESCOLA NACIONAL DE DEFESA CIBERNÉTICA, 2017), estabelecendo um conjunto de metas, ações e métricas mapeadas a partir do fortalecimento das próprias defesas de TI, trabalho integrado com a indústria para garantir que as redes, os dados e os sistemas do Reino Unido sejam protegidos contra a evolução das ameaças cibernéticas, estabelecimento de medidas ofensivas que possam ser adotadas quando necessárias e investimento continuado nas agências de segurança para investigar crimes cibernéticos.

Além disso, a estratégia cria o National Cyber Security Center (NCSC), um novo centro nacional de segurança cibernética, sendo o órgão central do governo que reúne as funções de segurança cibernética do governo, incluindo o Centro de Tratamento de Incidentes de Rede do Reino Unido. O NCSC visa construir parcerias de segurança cibernética entre o governo, a indústria e o público. O compromisso do NCSC de direcionar o engajamento da indústria busca fornecer muitos elementos da estratégia. Assim, o NCSC gerencia incidentes cibernéticos nacionais, fornece conhecimentos e oferece suporte personalizado e assessoria ao governo e à indústria.

A estratégia atual visa prevenir e reduzir o impacto dos ataques cibernéticos no Reino Unido, refletida em um programa denominado "Active Cyber Defense" que visa fornecer proteções automatizadas aos cidadãos que acessam os serviços governamentais on-line e afirma que, sempre que possível, que tecnologias similares devem ser oferecidas ao setor privado e ao cidadão.

A estratégia apoia o compartilhamento de informações, de forma que as organizações governamentais do Reino Unido tenham fácil acesso às informações sobre ameaças cibernéticas e melhorem o compartilhamento entre governo e indústria. O objetivo é garantir que os cidadãos, empresas, organizações e instituições do setor público e privado tenham acesso à informação certa para se defender. Compartilhar inteligência de ameaças sobre ataques cibernéticos avançados, motivações de cibercriminosos e táticas de atores mal-intencionados é essencial para defender redes e evitar ataques bem-sucedidos.

Aumentando os objetivos de resiliência cibernética, a estratégia enfatiza que, tanto na indústria quanto no governo, a segurança cibernética precisa ser vista como

uma preocupação de nível do conselho, não apenas uma questão de TI. A estratégia assinala que a responsabilidade pela segurança cibernética no setor privado cabe aos conselheiros, proprietários e operadores, enquanto a segurança das organizações do setor público do Reino Unido reside nos Ministros, Secretários Permanentes e Conselhos de Administração (KRIZ, 2016).

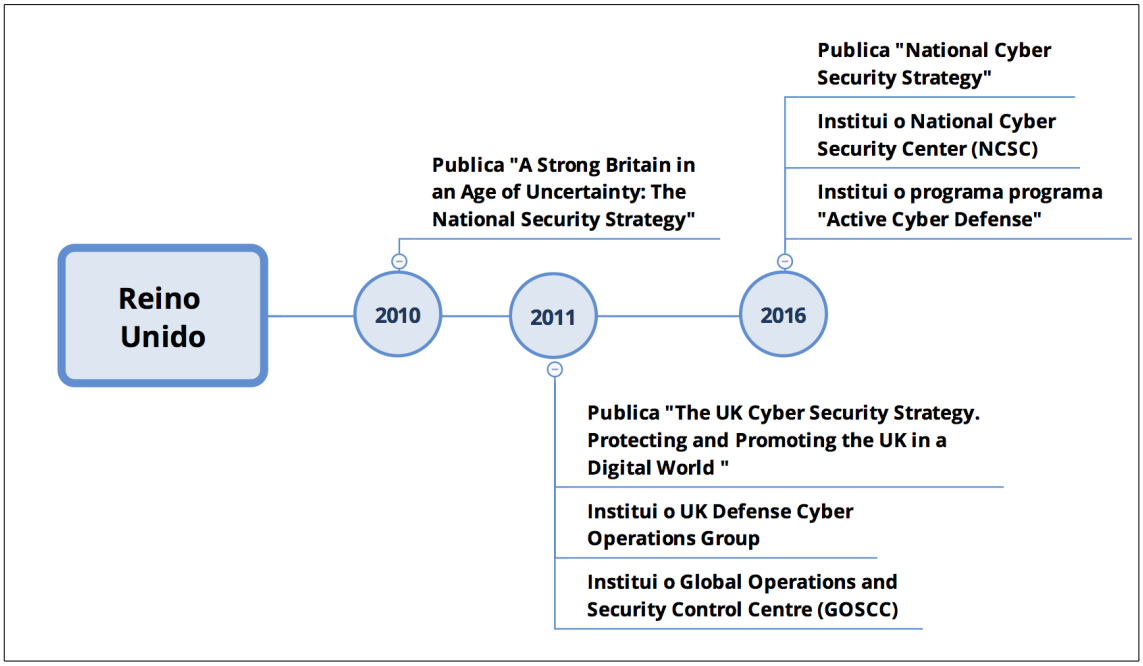
No Quadro 6, tem-se a estrutura principal do setor cibernético do Reino Unido. A Figura 3, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético do Reino Unido.

Quadro 6 – Estrutura principal do setor cibernético do Reino Unido

Principais Órgãos	Principais Responsabilidades
UK Defense Cyber Operations Group	Integrar os assuntos relacionados à segurança cibernética no âmbito do Ministério da Defesa.
Global Operations and Security Control Centre	Desenvolver novas táticas, técnicas e planos para entregar os efeitos militares através de operações no espaço cibernético.
National Cyber Security Center	Manter a segurança cibernética do governo e gerenciamento de incidentes cibernéticos nacionais.

FONTE: Próprio autor (2017).

Figura 3 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético do Reino Unido



FONTE: Próprio autor (2017).

2.4 HOLANDA

O governo holandês emitiu sua Estratégia Nacional de Segurança Cibernética em 2011, estabelecendo que a segurança cibernética é uma responsabilidade individual de cada instituição. No entanto, a cooperação entre entidades públicas e privadas foi estimulada. No governo, o Ministro da Segurança e Justiça possui um papel de coordenador da Segurança Cibernética. Estabeleceu-se um Centro Nacional de Segurança Cibernética (CNSC), cuja missão é coordenar o intercâmbio de informações sobre ameaças cibernéticas e soluções de segurança entre os parceiros privados e públicos. O CNSC também hospeda a Equipe Nacional de Resposta a Emergências de Incidentes de Computadores (DUCHEINE; OSINGA; SOETERS, 2012).

A Holanda adotou explicitamente uma abordagem proativa para o fortalecimento das suas capacidades cibernéticas em suas Forças Armadas, estabelecendo seis áreas focais para desenvolvimento e fortalecimento das capacidades cibernéticas do Ministério da Defesa holandês e das Forças Armadas da Holanda: capacidade de defesa, capacidade ofensiva, inteligência, adaptabilidade e inovação e cooperação.

O Comando Conjunto de Gerenciamento de Informação, operacional desde 2013, é responsável por garantir a resiliência das redes e sistemas da organização de defesa. Faz parte do Comando Conjunto uma Equipe de Resposta de Emergência de Defesa de Computadores, responsável pela segurança das principais redes de defesa. Sua tarefa é supervisionar e garantir a confiabilidade e o funcionamento sem impedimentos, dos sistemas de informação em apoio às operações militares.

Na visão das Forças Armadas da Holanda, uma vez que possam existir vulnerabilidades, tanto nos sistemas da força holandesa, quanto da força oponente, elas precisam ser exploradas, de forma a aumentar sua postura de inteligência e executar operações ofensivas. As atividades atuais das Forças Armadas da Holanda incluem o estabelecimento de um Comando de Defesa Cibernética e um Centro de Expertise de Defesa Cibernética (DUCHEINE; OSINGA; SOETERS, 2012).

O Comando de Defesa Cibernética holandês, pertencente ao Exército Real holandês, atua como autoridade de coordenação para todas as atividades cibernéticas das diversas unidades envolvidas. Porém, semelhante aos acordos

nacionais privados, o proprietário e os operadores de redes, plataformas de armas e sistemas de sensores constituinte do Ministério da Defesa holandês serão responsáveis pela segurança de seus ativos. O Comando de Defesa Cibernética concentra-se em três áreas da segurança cibernética: capacidades defensivas, capacidades de inteligência e capacidades ofensivas. As Forças Armadas holandesas vêem as capacidades cibernéticas ofensivas de forma a influenciar ou antecipar as ações de uma força oponente, explorando exclusivamente alvos militares (HOLANDA, 2017).

Em 2013, o governo holandês estabeleceu a segunda Estratégia Nacional de Segurança Cibernética, comprometendo-se com cinco objetivos estratégicos: a) A Holanda é resiliente aos ataques cibernéticos e protege seus interesses vitais no domínio digital; combater o crime cibernético; investir em produtos e serviços de TIC seguros que protejam a privacidade; possuir conhecimentos e habilidades de segurança cibernética suficiente e investir na inovação em TIC.

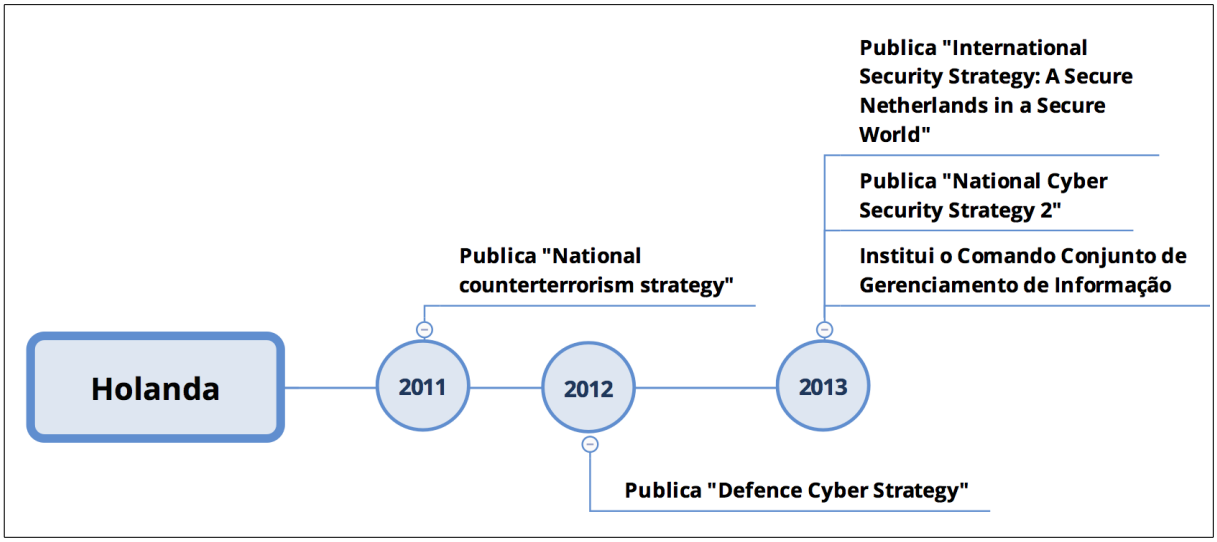
No Quadro 7, tem-se a estrutura principal do setor cibernético da Holanda. A Figura 4, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da Holanda.

Quadro 7 – Estrutura principal do setor cibernético da Holanda

Principais Órgãos	Principais Responsabilidades
Ministério da Segurança e Justiça	Coordenação da Segurança Cibernética
Centro Nacional de Segurança Cibernética (CNSC)	Coordenação do intercâmbio de informações sobre ameaças cibernéticas e tratamento de incidente de redes de computadores no âmbito do governo.
Comando Conjunto de Gerenciamento de Informação	Garantir a resiliência das redes e sistemas da organização de defesa e tratamento de incidente de redes de computadores no âmbito da defesa.
Comando de Defesa Cibernética	Coordenação para todas as atividades cibernéticas no âmbito das Forças Armadas.
Centro de Expertise de Defesa Cibernética	Desenvolver e difundir o conhecimento na área cibernética.

FONTE: Próprio autor (2017).

Figura 4 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da Holanda



FONTE: Próprio autor (2017).

2.5 ESPANHA

Em 2012, a Espanha relacionou os ataques cibernéticos, pela primeira vez, como um dos principais riscos para a segurança nacional na sua Estratégia Nacional de Segurança (ESPANHA, 2012). Dentre as medidas apontadas no documento, destacam-se: incrementar as capacidades de prevenção, detecção, investigação e resposta a ameaças cibernéticas suportadas por um quadro legal eficiente e funcional; promover a formação profissional em segurança cibernética e impulsionar a indústria espanhola através de um programa para pesquisa, desenvolvimento e inovação; desenvolver uma forte cultura de segurança cibernética, sensibilizando os cidadãos, os profissionais e empresas da importância da segurança das TIC e do uso responsável de novos serviços no conhecimento da sociedade e melhorar a cooperação internacional na área.

Em 2013, o governo publicou sua Estratégia Nacional de Segurança Cibernética, com o objetivo geral de garantir o uso dos sistemas de TIC, reforçando as capacidades de prevenção, defesa, detecção e resposta aos ataques cibernéticos, de forma a se criar uma confiabilidade dos recursos (ESPANHA, 2013). Com base nos princípios orientadores da publicação, incluindo uma liderança a nível ministerial, de responsabilidade compartilhada, a Estratégia Nacional de Segurança Cibernética buscou assegurar que os sistemas de TIC utilizados pelas

administrações públicas e infraestruturas críticas, possuam o nível adequado de segurança cibernética e resiliência.

Em 2013 criou-se um novo Sistema de Segurança Nacional no qual o Primeiro-Ministro é responsável pela gestão, liderança e promoção da política de segurança nacional. O núcleo deste sistema é o Conselho Nacional de Segurança (CNS), que é um órgão colegiado composto pelo vice-primeiro-ministro, os secretários estaduais relevantes, o diretor do gabinete do primeiro-ministro e outros membros do governo.

Por iniciativa do CSN, foram criadas comissões especializadas para apoiar o Conselho em áreas específicas da Estratégia Nacional de Segurança. Essas comissões são ativadas em situações específicas que exigem a coordenação de várias agências da Administração Pública. No âmbito da defesa cibernética, duas comissões especializadas específicas auxiliam o CSN: o Conselho Especializado em Segurança Cibernética e o Comitê de Situação Especializada.

Além disso, criou-se Conselho Nacional de Segurança Cibernética (CNSC), sendo um órgão colegiado que apoia o CSN na assessoria ao primeiro-ministro em questões de segurança cibernética, tanto a nível nacional como internacional, através de análises, estudos e iniciativas. O Comitê de Situação Especializada tem a tarefa de auxiliar o CSN em situações de crise, em questões de segurança cibernética que não foram canalizadas através de mecanismos de resposta convencionais devido à sua extensão ou natureza.

O principal órgão oficial encarregado da segurança da informação espanhola é o Centro Criptológico Nacional (CCN), subordinado ao serviço de inteligência espanhol, o Centro Nacional de Inteligência (CNI), que atualmente faz parte do Ministério da Presidência. As responsabilidades da CCN incluem a segurança de sistemas pertencentes ao Governo que processam, armazenam ou transmitem informações em formato eletrônico, bem como a segurança de sistemas com informações classificadas. O CCN desempenha funções a nível técnico, que incluem o desenvolvimento e divulgação de regras, instruções, diretrizes e recomendações para garantir a segurança dos sistemas de TIC da Administração Pública e a coordenação da promoção, desenvolvimento, aquisição, comissionamento e operação de tecnologias de segurança. Ele também avalia e certifica as capacidades dos produtos de criptografia e dos sistemas de TIC para gerenciar informações de forma segura através de um organismo de certificação. Também

coordena respostas conjuntas a incidentes de segurança a nível nacional e internacional.

No âmbito das Forças Armadas, foi criado em 2013, o comando cibernético espanhol, denominado Comando Conjunto de Defesa Cibernética, que é o e o órgão encarregado das questões da área no Ministério da Defesa. Como parte da Chefia Conjunta da Defesa espanhola, esta instituição comanda e coordena as atividades das Forças do Exército espanhol neste campo, incluindo o desenvolvimento, gerenciamento e controle de políticas de segurança da informação. Sua missão é planejar e realizar ações militares de defesa cibernética nas redes de telecomunicações e sistemas de informação das Forças Armadas ou outras redes que lhe possam ser confiadas. O Comando Conjunto de Defesa Cibernética contribui, em um nível tático, para a resposta aos riscos ou ameaças do espaço cibernético que possam afetar a defesa nacional.

Em 2014, foi criado pelo Ministério da Defesa, nos escritórios do Comando Conjunto de Defesa Cibernética, um Centro de Resposta a Incidentes de Segurança Cibernética do Ministério da Defesa. Este centro opera a nível técnico para facilitar o trabalho de defesa, exploração e resposta, utilizando laboratórios forenses e outras instalações.

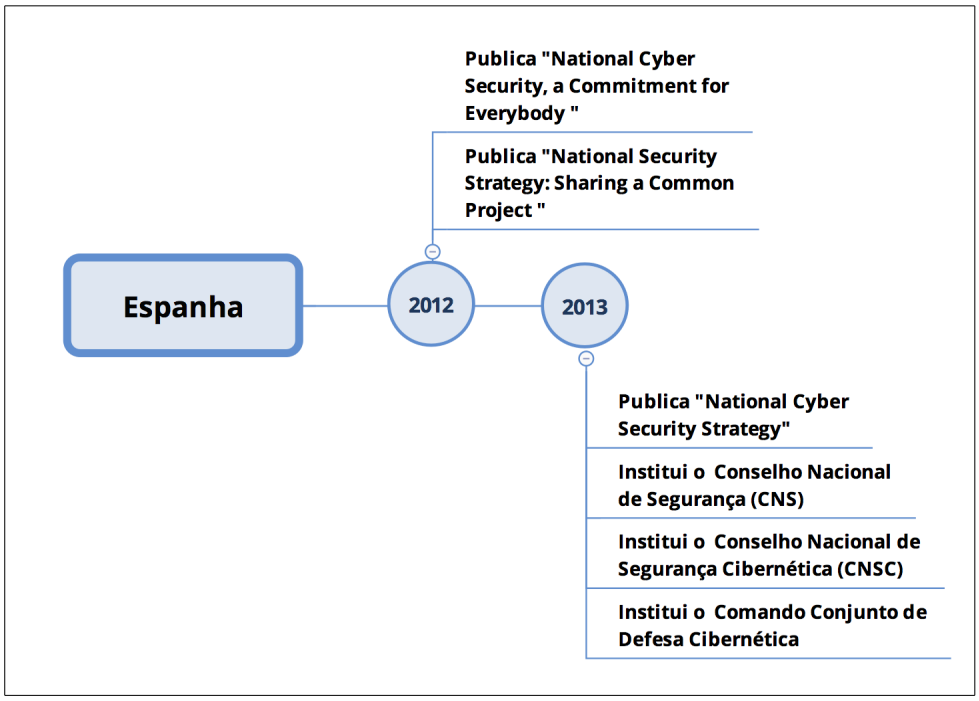
No Quadro 8, tem-se a estrutura principal do setor cibernético da Espanha. A Figura 5, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da Espanha.

Quadro 8 – Estrutura principal do setor cibernético da Espanha

Principais Órgãos	Principais Responsabilidades
Conselho Nacional de Segurança Cibernética	Apoiar o Conselho Nacional de Segurança na assessoria ao primeiro-ministro em questões de segurança cibernética.
Centro Criptológico Nacional	Assegurar os sistemas pertencentes ao governo e coordenação do tratamento e resposta a incidentes de rede no âmbito da APF.
Comando Conjunto de Defesa Cibernética	Planejar e realizar ações militares de defesa cibernética nas redes de telecomunicações e sistemas de informação das Forças Armadas.
Centro de Resposta a Incidentes de Segurança Cibernética do MD	Tratamento e resposta a incidentes de rede no âmbito do Ministério da Defesa.

FONTE: Próprio autor (2017).

Figura 5 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético da Espanha



FONTE: Próprio autor (2017).

3 DOUTRINA E ESTRUTURA DO SETOR CIBERNÉTICO DOS ESTADOS UNIDOS

Em 2011 foi elaborada a Estratégia Internacional do Espaço Cibernético com o objetivo de abranger o espaço cibernético dos EUA, centrado em torno de sete principais prioridades políticas internacionais, que visam promover um espaço cibernético interoperável, seguro e confiável.

No plano interno dos EUA, o “Department of Homeland Security”, criado em 2002, reúne 22 entidades federais com o propósito comum de melhorar a segurança interna dos EUA, onde o Secretário de Segurança Interna tem importantes responsabilidades em relação à segurança do ciberespaço dos EUA, como o desenvolvimento de um plano nacional abrangente para garantir recursos-chave e infraestrutura crítica, providenciar gerenciamento de crises em resposta a um ataque e oferecer assistência técnica ao setor privado e outras instituições governamentais (TIKK, 2011). Em 2011, o Departamento divulgou o “Plano para um Futuro Cíclico Seguro”, destacando-se a necessidade de proteção cibernética das atuais infraestruturas críticas dos EUA.

No plano militar, o governo norte-americano publicou em 2011 a Estratégia de Defesa para Operação no Espaço Cibernético, onde a principal iniciativa estratégica foi tratar o espaço cibernético como um domínio operacional para organizar, treinar e equipar o Department of Defense (DoD) dos Estados Unidos para que possa aproveitar ao máximo o potencial daquele domínio. Outras iniciativas incluem a proteção das redes e sistemas DoD dos EUA, a cooperação com outros departamentos governamentais dos EUA e o setor privado e a cooperação internacional com parceiros internacionais dos EUA para fortalecer a segurança cibernética coletiva. Além disso, foi inclusa a noção de "equivalência", ou seja, se um ataque cibernético produzir a morte, dano, destruição ou perturbação de alto nível, nas mesmas proporções que um ataque militar tradicional causaria, os EUA poderiam utilizar como recurso o "uso de força " contra o atacante.

O núcleo de todas as atividades cibernéticas militares é o United States Cyber Command (USCYBERCOM), que é o comando cibernético sub-unificado das forças armadas subordinado ao United States Strategic Command (USSTRATCOM). O comando cibernético é composto de vários componentes das Forças Armadas americanas, sendo guarnecido de forma conjunta. O comando projeta, coordena, integra, sincroniza e conduz atividades para direcionar as operações em todo o

espectro do espaço cibernético de forma a permitir ações em todos os domínios. Sua missão é garantir a liberdade de ação dos EUA no espaço cibernético e negar o mesmo aos seus adversários (US STRATEGIC COMMAND, 2012). Depois de se tornar operacional, o comando cibernético americano inspirou muitas outras nações para criar seus comandos cibernéticos, como o Reino Unido e a Holanda.

O Joint Information Operations Warfare Center (JIOWC) também foi criado em 2005, para planejar, integrar e sincronizar operações de informação em suporte direto de Comandantes da Força Conjunta e servir como o líder do USSTRATCOM para melhorar as operações de informação em todo o Departamento de Defesa. Além disso, o diretor da Agência Nacional de Segurança, National Security Agency (NSA) também atua como o diretor da USCYBERCOM, tornando-os organizações de dupla proteção (US GOVERMENT ACOUNTABILITY OFFICE, 2017b).

Cada ramo militar designou um componente de suporte para a segurança cibernética que opera sob o USCYBERCOM: US Army Cyber Command, Comando Cibernético do Exército dos EUA; US Fleet Cyber Command / US 10th Fleet, da Marinha dos EUA; 24th Air Force/AFCYBER, da Força aérea americana; e US Marine Corps Forces Cyberspace (MARFORCYBER), dos Fuzileiros Navais americanos (LEWIS; TIMLIM, 2011).

Dentre as outras organizações DoD que possuem funções de segurança cibernética estão: Network Operations Security Centers (NOSC), os centros de segurança de operações de rede, que fornecem relatórios de operações de rede e consciência situacional para as Forças Armadas, bem como para outros comandos; National Guard, a Guarda Nacional americana; e DoD Criminal Investigative Services, os Serviços de Investigação Criminal.

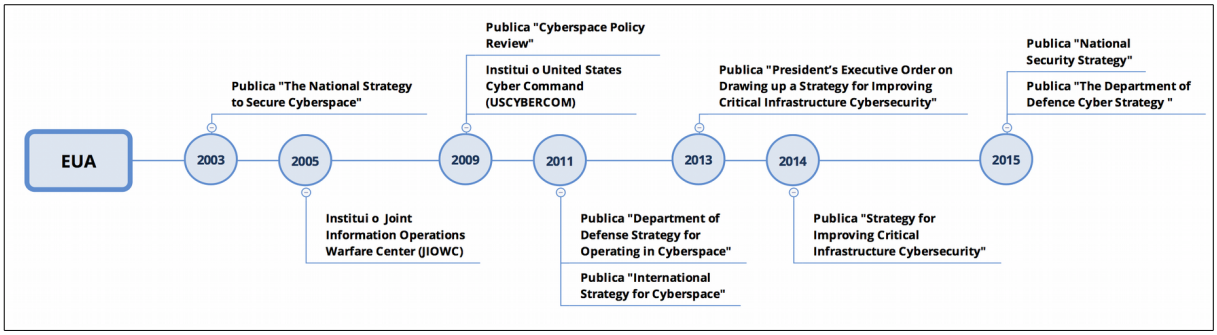
O DoD desenvolveu o conceito de Joint Concept on Cyberspace (JCC). O conceito identifica os aspectos estratégicos e as capacidades militares disponíveis para alcançar a superioridade do espaço cibernético. Esta superioridade é descrita como um grau de dominação que uma força mantém sobre o oponente que permite a liberdade de ação no espaço cibernético em um determinado momento e lugar, negando o mesmo a esse oponente. O JCC distinguiu três maneiras diferentes de ganhar a superioridade do espaço cibernético: através de operações de redes de informações globais, visando proteger a informação; através de operações cibernéticas defensivas, visando proteger as redes estáticas e implantáveis do DoD e através de operações cibernéticas ofensivas. Esta última categoria inclui

atividades para acessar o hardware e o software de um oponente por meios remotos e diretos; ataques a processadores e controladores de equipamentos e sistemas de um oponente; atacar as informações do oponente de forma a dissuadi-lo ou enganá-lo; mitigar e indisponibilizar as ações de um oponente; e fornecer aos decisores da ofensiva cibernética uma inteligência precisa sobre o espaço cibernético (US DEPARTMENT OF DEFENSE, 2017).

O DoD adotou uma abordagem descentralizada para a organização de sua estrutura de segurança cibernética. Existem várias organizações, divisões e agências que abordam as necessidades de segurança cibernética do DoD, tanto nos níveis de formulação de políticas como nos níveis operacionais. O Comando das Forças Conjuntas dos EUA, US Joint Forces Command (JFCOM) e vários escritórios dentro do Escritório do Secretário de Defesa, Office of the Secretary of Defense, têm papéis no desenvolvimento de políticas e orientação da estratégia de segurança cibernética (US GOVERMENT ACOUNTABILITY OFFICE, 2017a).

No Quadro 9, tem-se a estrutura principal do setor cibernético dos EUA. A Figura 6, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético dos EUA.

Figura 6 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético dos EUA



FONTE: Próprio autor (2017).

Quadro 9 – Estrutura principal do setor cibernético dos Estados Unidos

Principais Órgãos	Principais Responsabilidades
Department of Homeland Security	Desenvolver um plano nacional abrangente para garantir recursos-chave e infraestrutura crítica, providenciar gerenciamento de crises em resposta a um ataque e oferecer assistência técnica ao setor privado e outras instituições governamentais.
US Cyber Command	Planejar, coordenar, integrar, sincronizar e conduzir atividades para direcionar as operações e a defesa de determinadas redes de informação do Departamento de Defesa americano.
US Joint Forces Command	Desenvolver políticas e orientação da estratégia de segurança cibernética.
Joint Information Operations Warfare Center	Planejar, integrar e sincronizar operações de informação em suporte direto de Comandantes da Força Conjunta.
US Army Cyber Command	Compor o suporte para a segurança cibernética que opera sob o USCYBERCOM no âmbito do Exército dos EUA.
US Fleet Cyber Command	Compor o suporte para a segurança cibernética que opera sob o USCYBERCOM no âmbito da Marinha dos EUA.
24th Air Force	Compor o suporte para a segurança cibernética que opera sob o USCYBERCOM no âmbito da Força Aérea dos EUA.
U.S. Marine Corps Forces Cyberspace	Compor o suporte para a segurança cibernética que opera sob o USCYBERCOM no âmbito da Força de Fuzileiros Navais dos EUA.
Network Operations Security Centers	Fornecer relatórios de operações de rede e consciência situacional para as Forças Armadas.

FONTE: Próprio autor (2017).

4 DOUTRINA E ESTRUTURA DO SETOR CIBERNÉTICO BRASILEIRO

A Política de Defesa Nacional (PDN), estabelecida em 2005, já promovia a necessidade de se estabelecer uma Doutrina Cibernética brasileira, uma vez que abordava que os avanços da tecnologia da informação e dos meios de comunicação, introduziram vulnerabilidades que poderiam ser exploradas, possibilitando a inviabilidade do uso dos sistemas de defesa brasileiros (BRASIL, 2005).

A Estratégia Nacional de Defesa (END), publicada em 2008, foi dada uma ênfase na necessidade de se estabelecer uma segurança cibernética das infraestruturas críticas, em especial, nos setores de energia, transporte, abastecimento de água e telecomunicações. A END estabeleceu que o Comando do Exército ficaria responsável pela coordenação e integração das ações de defesa cibernética no âmbito das Forças Armadas, contribuindo para a formulação da política e doutrina de defesa no setor. (BRASIL, 2008).

Em 2010 foi ativado o Núcleo do Centro de Defesa Cibernética (NuCDCiber), responsável por coordenar as atividades do setor cibernético, no âmbito do Ministério da Defesa (MD). No corrente ano, foi elaborado o Livro Verde sobre Segurança Cibernética no Brasil estabelecendo as diretrizes para a futura elaboração do Livro Branco da Política Nacional de Segurança Cibernética, propondo fomentar a articulação de acordos internacionais, com o objetivo de incrementar a segurança cibernética no país, a capacidade de defesa e dissuasão e elaborar uma Política Nacional de Segurança das Infraestruturas Críticas (MANDARINO JUNIOR; CANONGIA, 2010).

Em 2012, foi criado o CDCiber, a partir da concepção do seu núcleo em 2010, o qual ficou responsável pela coordenação e integração das atividades
de defesa cibernética, no âmbito do Ministério da Defesa (MD). Naquele ano, foi disponibilizado o Livro Branco de Defesa Nacional (LBDN), documento público, em forma de livro, que expõe a visão do governo sobre o tema da defesa, a ser apresentado à comunidade nacional e internacional. (BRASIL, 2012a). Dentre as propostas, destaca-se o Projeto de Sistema de Proteção Cibernética, a partir de uma estrutura de planejamento e execução da segurança cibernética, uma estrutura de pesquisa científica na área, uma estrutura de capacitação e preparo e emprego

operacional às necessidades do setor Cibernético.

Também em 2012, foi publicada a Política Cibernética de Defesa (BRASIL, 2012b) com o objetivo de orientar as atividades de defesa cibernética, no nível estratégico e de guerra cibernética, nos níveis operacional e tático, no âmbito das Forças Armadas. As diretrizes definidas pelo documento serviram de referência para a defesa cibernética nos grandes eventos que foram sediados no país: a Copa das Confederações de 2013, a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016. Com a definição dessa política, o MD buscou assegurar o uso efetivo do espaço cibernético pelas Forças Armadas de forma a impedir ou dificultar sua utilização contra os interesses do país. O documento também previu a criação do Sistema Militar de Defesa Cibernética (SMDC), prevendo contar com a participação de civis e militares da Marinha, do Exército e da Aeronáutica.

Em 2014, o MD cria o Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (EnaDCiber) na Estrutura Regimental do Comando do Exército, contando na forma da legislação, com o exercício de militares das três Forças Armadas, cabendo ao Estado-Maior Conjunto das Forças Armadas (EMCFA) as atividades de coordenação nos casos de operações conjuntas (BRASIL, 2014b).

Ainda em 2014, foi estabelecida a Doutrina Militar de Defesa Cibernética, de forma a proporcionar uma unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético. Além das definições dos conceitos relacionados a área cibernética, foi definido o Sistema Militar de Defesa Cibernética (SMDC), como a estrutura essencial de proteção cibernética conjunta do Sistema Militar de Comando e Controle (SISMC2). O SMDC é o responsável por coordenar e integrar a proteção das infraestruturas críticas de Informação de interesse da Defesa Nacional, definidas pelo MD (BRASIL, 2014a).

Em 2016, as minutas da revisão da Política Nacional de Defesa (PND), da Estratégia Nacional de Defesa (END) e do Livro Branco de Defesa Nacional (LBDN) foram encaminhadas para apreciação do Congresso Nacional. As minutas das publicações foram disponibilizadas para consulta pública em 2017. O objetivo é permitir o acesso da comunidade acadêmica, civil e militar, e da sociedade como um todo às principais ideias e aos novos conceitos apresentados na proposta atual dos documentos. A edição definitiva depende da apreciação pelo Congresso Nacional e

sua posterior aprovação por Decreto Presidencial. (BRASIL, 2017a).

No âmbito da Administração Pública Federal, o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) , criado em 2006, é responsável por planejar, orientar, coordenar e desenvolver as políticas e ações de segurança da informação. O DSIC também define os requisitos metodológicos para a implementação de ações de segurança da informação e comunicações, incluídas as de segurança cibernética e de segurança das infraestruturas críticas da informação do Estado, pelos órgãos e entidades da Administração Pública Federal (BRASIL, 2017b). Em 2008, criou-se a Rede Nacional de Segurança da Informação e Criptografia (RENASIC) no GSI para cuidar dos aspectos de fomento de Ciência e Tecnologia na área de segurança cibernética.

Para tratamento de incidentes de redes, o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov) auxilia o desenvolvimento da cooperação entre os grupos de respostas de incidentes existentes no Brasil e no exterior, o fomento das iniciativas de gerenciamento de incidentes e a distribuição de informações, alertas e recomendações para os administradores de segurança em redes de computadores da Administração Pública Federal para os domínios gov.br, jus.br, leg.br, mil.br, mp.br e def.br (CTIR GOV, 2017). Os serviços prestados pelo CTIR Gov podem ter caráter reativo ou proativo. Em ambos os casos, o Centro tem condições de determinar tendências e padrões das ameaças no ciberespaço que afetam não só a APF, mas, trabalhando em conjunto com os demais Centros de Tratamento das Forças Armadas e instituições que compõem as infraestruturas críticas de Estado. O CTIR Gov funciona, portanto, como o ponto central da rede colaborativa de grupos de tratamentos de incidentes de segurança computacionais por todo o país.

4.1 O SISTEMA MILITAR DE DEFESA CIBERNÉTICA (SMDC)

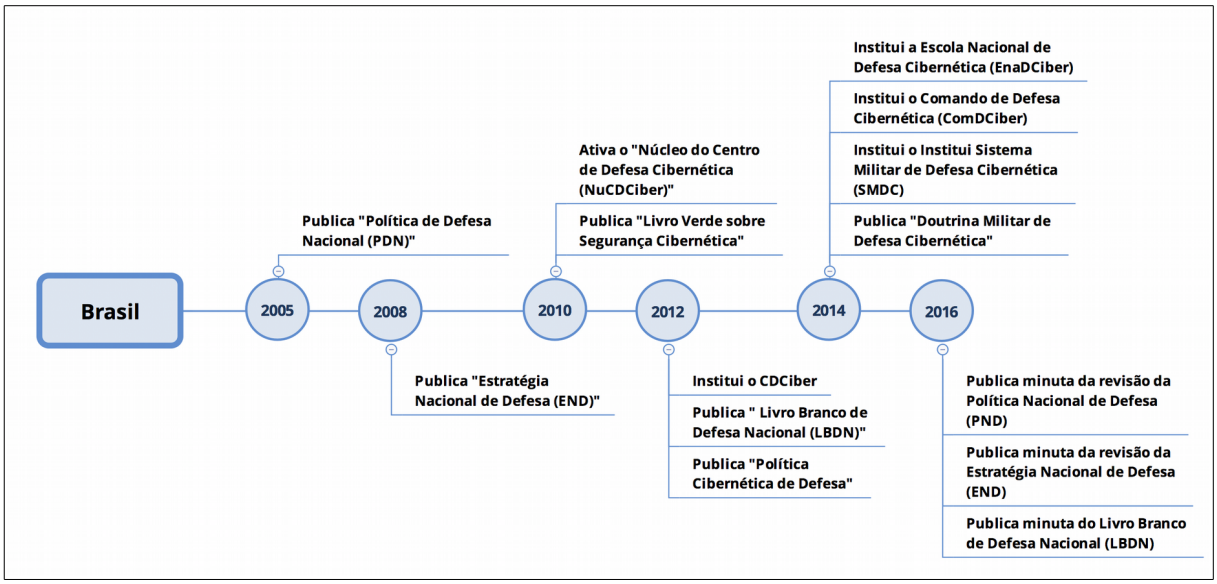
O Estado-Maior Conjunto das Forças Armadas (EMCFA) é o órgão responsável por assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC, com a finalidade de garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de se-

gurança necessários. O ComDCiber é o órgão central do SMDC, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas brasileiras e impedir ou dificultar sua utilização contra interesses da defesa nacional. Sua missão é planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do SMDC (EXÉRCITO BRASILEIRO, 2017). Subordinado ao ComDCiber há o Centro de Defesa Cibernética (CDCiber), que passa ao controle operacional do MD nas Operações Conjuntas. O CDCiber atua sob orientação e supervisão do MD, no nível estratégico, realizando as ações de coordenação e integração do Setor Cibernético nas Forças Armadas, mantendo um canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética. Além disso, o CDCiber mantém canal sistêmico/técnico com os órgãos centrais de inteligência das Forças Armadas, no âmbito do Sistema de Inteligência de Defesa (SINDE), no tocante ao Setor Cibernético, para a difusão e obtenção dos dados obtidos por intermédio da Fonte Cibernética.

Com o surgimento da necessidade de coordenação entre as agências vinculadas a estrutura de defesa cibernética, seja no nível estratégico, operacional e tático, configurou-se, caso necessário, o emprego de um Destacamento Conjunto de Defesa Cibernética ou um Destacamento Conjunto de Guerra Cibernética, além de elementos de Guerra Cibernética integrantes das Forças Componentes. O Destacamento Conjunto de Defesa Cibernética quando ativado, poderá ser estruturado com um comandante e subcomandante, elementos especializados em guerra cibernética das FA, de ligação inter-agências, civis especialistas, para operação assistida e assessoria.

No Quadro 10, tem-se a estrutura principal do setor cibernético brasileiro. A Figura 7, ilustra-se a linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético brasileiro.

Figura 7 – Linha do tempo dos principais eventos relacionados à evolução da doutrina e estrutura do setor cibernético brasileiro



FONTE: Próprio autor (2017).

Quadro 10 – Estrutura principal do setor cibernético brasileiro

Principais Órgãos	Principais Responsabilidades
Comando de Defesa Cibernética	Órgão central do SMDC, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas brasileiras e impedir ou dificultar sua utilização contra interesses da defesa nacional.
Centro de Defesa Cibernética	Coordenar as atividades do setor cibernético, no âmbito do Ministério da Defesa .
CTIR Gov	Tratar incidente de redes de computadores de órgãos da Administração Pública Federal.
Estado-Maior Conjunto das Forças Armadas	Assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC.
DSIC	Implementar de ações de segurança cibernética nos órgãos e entidades da Administração Pública Federal.

FONTE: Próprio autor (2017).

5 ANÁLISE COMPARATIVA

Realizou-se uma análise comparativa da doutrina e estruturação do setor cibernético do Brasil em função da doutrina e estrutura países pesquisados, dividindo-se em pontos em comum e pontos distintos.

5.1 PONTOS EM COMUM ENTRE A DOUTRINA E ESTRUTURAÇÃO DO SETOR CIBERNÉTICO DOS PAÍSES PESQUISADOS E A BRASILEIRA

Do estudo realizado, observa-se que as doutrinas do setor cibernético são predominantemente ostensivas e estão em constante atualização ao longo do tempo, uma vez que, o seu processo de formulação se dá a partir da evolução tecnológica e ganho de maturidade no setor cibernético de cada país. Um artifício executado pelo Brasil e pela França, na publicação das doutrinas, é a disposição do conteúdo no formato de Livro Branco, documento público em forma de livro, que expõe a visão do governo sobre o tema da defesa, a ser apresentado à comunidade nacional e internacional, para posterior análise e formalização.

Uma vez que a segurança cibernética é afetada pela evolução tecnológica, os países mantiveram a preocupação com a manutenção da capacitação de emprego do pessoal na segurança cibernética e pesquisa na área, através de acordos com instituições de ensino nacionais e acordos de internacionais.

O estabelecimento de uma cooperação internacional é um ponto comum, havendo um incentivo para a troca de experiências entre as forças de defesa, contribuindo para o desenvolvimento de técnicas defensivas e ofensivas entre os países cooperados.

Outro ponto em comum é a preocupação de manter a segurança cibernética das infraestruturas críticas estatais, uma vez que a operacionalidade dos serviços vitais estatais estão cada vez mais dependentes da tecnologia proveniente do espaço cibernético. A exploração de uma vulnerabilidade de uma infraestrutura crítica pode criar uma instabilidade econômica e social, como a indisponibilidade de serviços públicos público e transações no mercado financeiro.

Percebe-se que de forma geral, há na estrutura do setor cibernético de cada país, um órgão central responsável pela segurança cibernética e tratamento de incidentes no nível interno governamental, voltado para a proteção dos órgãos da

administração pública e um órgão central responsável pela segurança cibernética, no âmbito da defesa, envolvendo as Forças Armadas.

Quadro 11 – Resumo dos pontos em comum entre a doutrina e estruturação do setor cibernético dos países pesquisados e a brasileira

Ponto Observado	Descrição
Influência da evolução tecnológica na doutrina e estruturação do setor cibernético	A constante atualização da doutrina e setor cibernético o longo do tempo, deve-se a partir da evolução tecnológica e ganho de maturidade no setor cibernético de cada país.
Incentivo ao intercâmbio de informações e tratados de cooperação no setor cibernético	Preocupação em manter a capacitação de emprego do pessoal na guerra cibernética e pesquisa na área.
Preocupação com a segurança cibernética de infraestruturas críticas	A exploração de uma vulnerabilidade de uma infraestrutura crítica pode criar uma instabilidade econômica e social.
Existência de um órgão central no âmbito da administração pública e um órgão no âmbito da defesa	No nível interno governamental, há um órgão central voltado para a proteção dos órgãos da administração pública e um órgão central responsável pela segurança cibernética, no âmbito da defesa, envolvendo as Forças Armadas.

FONTE: Próprio autor (2017).

5.2 PONTOS DISTINTOS ENTRE A DOUTRINA E ESTRUTURAÇÃO DO SETOR CIBERNÉTICO DOS PAÍSES PESQUISADOS E A BRASILEIRA

O primeiro ponto a ser observado é a diferença da ordem de grandeza da disponibilidade dos recursos financeiros, materiais e humanos empregados no setor cibernético dos países considerados potência militar, como os EUA e países emergentes como o Brasil. Isso reflete diretamente na estrutura do setor norte-americano, que diferente da brasileira, é extremamente descentralizada, com vários órgãos atuantes na área operacional etática.

Outra influência na formação da doutrina e estruturação do setor cibernético é o aumento da ameaça de utilização da cibernética por grupos terroristas e criminosos. Uma vez que, no Brasil, esse tipo de ação é considerada inexpressiva, não há uma influência desta ameaça na formação da doutrina e estruturação do setor cibernético brasileiro.

Como consequência da iminência de um ataque cibernético a uma grande potência, os EUA expressam explicitamente em sua doutrina que podem responder a um ataque cibernético de um oponente, com ações cinéticas. Diferentemente da doutrina brasileira, a doutrina norte-americana e a doutrina holandesa adotam explicitamente uma abordagem proativa nas suas operações ofensivas. O Brasil optou por manter uma abordagem através da defesa cibernética ofensiva por dissuasão.

Quadro 12 – Resumo dos pontos distintos entre a doutrina e estruturação do setor cibernético dos países pesquisados e a brasileira

Ponto Observado	Descrição
Disponibilidade de recursos financeiros, materiais e humanos no setor	A disponibilidade de recursos financeiros, materiais e humanos no setor cibernético influencia na descentralização da estruturação do setor cibernético.
Aumento da ameaça do uso da cibernética por grupos terroristas	Inclusão de ações contra grupos terroristas devido ao aumento da ameaça do uso da cibernética por grupos terroristas.
Doutrinas com abordagem explicitamente proativa nas operações ofensivas	Como consequência da iminência de um ataque cibernético a uma grande potência, os EUA expressam explicitamente em sua doutrina que podem responder a um ataque cibernético de um oponente, com ações cinéticas.

FONTE: Próprio autor (2017).

6 CONCLUSÃO

Nos últimos anos, o Brasil vem projetando-se no cenário internacional, com a realização dos grandes eventos, como a Jornada Mundial da Juventude (2013), Copa das Confederações (2013), Copa do Mundo (2014) e Olimpíadas do Rio (2016). Assim, a crescente ameaça de ataques cibernéticos e a realização dos grandes eventos no Brasil foram fatores preponderantes, que motivaram o governo brasileiro a impulsionar a estruturação da defesa do setor cibernético nacional e o estabelecimento de uma doutrina para respaldar as ações em caso de atuação das operações cibernéticas defensivas e ofensivas. Além disso, buscou-se a formalização da unificação do pensamento sobre o assunto no âmbito do Ministério da Defesa.

No entanto, foi identificado que quando se compara a doutrina e estrutura do setor cibernético brasileiro, com as demais de países mais maduros, pode-se perceber que, de forma geral, a concepção das doutrinas são similares. Há uma constante atualização por parte dos países ao longo do tempo, devido a evolução tecnológica e ganho de maturidade no setor cibernético. Além disso, uma vez que o conhecimento está em evolução, há uma preocupação de todos em manter a capacitação de emprego do pessoal na guerra cibernética e pesquisa na área. Outra preocupação comum é manter a segurança cibernética das infraestruturas críticas, uma vez que sua exploração pode-se criar instabilidade. Já na estruturação do setor, há a similaridade da criação de um órgão central responsável pela defesa dos setores internos e um órgão responsável pela defesa no âmbito das Forças Armadas.

Porém, há pontos distintos criados pela influência de questões específicas de cada país. Um fator decisivo é a disponibilidade de recursos financeiros, materiais e humanos no setor cibernético, possibilitando a descentralização do setor. Outro fator é a inclusão de norma e lei contra ações de grupos terroristas. Já por parte da doutrina, diferentemente da norte-americana e holandesa, o Brasil não expressa explicitamente que pode responder a um ataque cibernético de um oponente, com ações cinéticas.

Logo, conclui-se que a doutrina e estruturação do setor cibernético brasileiro se coadunam com aquelas pesquisadas, considerando os países com maior nível de maturidade no setor. Avalia-se que os pontos distintos analisados, são consequência

do histórico recente de cada país e do posicionamento mundial como potência armada. Sendo assim, espera-se que o Brasil se mantenha com sua capacidade defensiva e ofensiva, ganhando maturidade a medida que o setor cibernético se torne consolidado.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Decreto nº 5.484, de 30 de junho de 2005. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 1 jul. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm>. Acesso em: 24 out. 2017.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 19 dez. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm>. Acesso em: 24 out. 2017.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética** [MD31-M-07], 2014.Disponível em: <http://defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina /md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 17 ago. 2017.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional,** 2012. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 17 ago. 2017.

BRASIL. Ministério da Defesa. **Minutas do Livro Branco, da PND e da END estão disponíveis para leitura** .Disponível em: <http://www.defesa.gov.br/noticias/29093-minutas-do-livro-branco-da-pnd-e-da-end-estao-disponiveis-para-leitura>. Acesso em: 23 out. 2017.

BRASIL. Ministério da Defesa. **Política Cibernética de Defesa** [MD31-P-02], 2012.

BRASIL. Presidência da República. Gabinete de Seguraça Institucional. Disponível em: <http://dsic.planalto.gov.br/assuntos/missao-dInstitucionalo-dsic>. Acesso em 19 out. 2017.

BRASIL. Portaria Normativa nº 2.777/MD**,** de 27 de outubro de 2014. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 28 out. 2014. Disponível em: <www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=1314&act=bre>. Acesso em: 24 out. 2017.

CTIR GOV. **Sobre o CTIR Gov**. Disponível em: <http://www.ctir.gov.br/index.html> Acesso em 19 out. 2017.

DUCHEINE, P.; OSINGA F.; SOETERS, J. Cyber Security and Policy Responses**.** **Cyber Warfare**: Critical Perspectives. Netherlands Annual Review of Military Studies, 2012.

ESPANHA. Presidencia del Gobierno, **The National Security Strategy:** Sharing a Common Project. Departamento de Seguridad Nacional, 2012 - 58 pages. Disponível em: <http://www.dsn.gob.es/es/file/330/download?token=1SwPdUQU>. Acesso em: 20 out. 2017.

ESPANHA. Presidencia del Gobierno, **Estrategia de Ciberseguridad Nacional**, 2013. Disponível em: <https://www.ccn-cert.cni.es/publico/dmpublido cuments/EstrategiaNacionalCiberseguridad.pdf>. Acesso em: 24 out. 2017.

ESTÔNIA. Ministry of Economic affairs and communication. **Cyber Security Stategy**, 2014. Disponível em: <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>. Acesso em: 24 out. 2017.

EUROPEAN DEFENCE AGENCY. **National Security Concept of Estonia**, 2010 Disponível em: <https://www.eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf>. Acesso em: 24 out. 2017.

EXÉRCITO BRASILEIRO. **Comando Conjunto na Defesa Cibernética**. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/id/8110427>. Acesso em: 20 out. 2017.

FRANÇA. Ministère de la Défense. Dèfense et Sécurité Nationale. **Le Livre Blanc**, 2008. Disponível em: <http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf>. Acesso em: 27 out. 2017.

FRANÇA. Ministère de la Défense. **Stratégie de la France**: Défence et sécurité des systèmes d'information, 2011. Disponível em: <https://pt.scribd.com/document/48880185/ 2011-02-15-Defense-Et-Securite-Des-Systemes-d-Information-Strategie-de-La-France>. Acesso em: 27 out. 2017.

HOLANDA. Ministry of Defence. **Defence Cyber Command**. Disponível em: <https://www.defensie.nl/english/topics/cyber-security/cyber-command>. Acesso em: 17 ago. 2017.

INTERNATIONAL TELECOMMUNICATION UNION. **Global Cybersecurity Index 2017.** Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf>. Acesso em: 27 out. 2017.

KRIZ, D. **Prosperity in the UK and Worldwide.** Disponível em: <https://research-center.paloalton etworks.com/2016/12/gov-uks-national-cyber-security-strategy-contributing-increasing-cybersecurity-prosperity-uk-worldwide/>. Acesso em: 24 out. 2017.

LEWIS, J; TIMLIM, K. **Cybersecurity and Cyberwarfare**. Preliminary Assessment of National Doctrine and Organization, Washington, DC: Center for Strategic and International Studies, 2011.

MANDARINO JUNIOR, R.; CANONGIA, C. **Livro Verde Segurança: Segurança Cibernética no Brasil**. Brasília - DF: [s.n.], 2010. 63 p.

NÚCLEO DA ESCOLA NACIONAL DE DEFESA CIBERNÉTICA. **Estratégia Nacional de Segurança Cibernética (2016 - 2021).** Disponível em: <http://enadciber.eb.mil.br/images/V_Seminario/palestras/2_AGO_17_3_A_Nova_Estrutura_de_Seguranca_e_Defesa_Cibernetica_no_Reino_Unido.pdf>. Acesso em: 24 out. 2017.

PARRISH, Karen. **Cyber Threat Grows More Destructive**. American Forces Press Service, jul. 2011.

REEVE, Tom. **France unveils cyber command in response to 'new era in warfare'**. Disponível em: <https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671/>. Acesso em: 24 out. 2017.

TIKK, E. **Frameworks for International Cyber Security.** National Cyber Security Policies and Strategies. Tallinn: CCD COE Publications, 2011.

UK GOVERNMENT. **UK Cyber Security Strategy:** Protecting and Promoting the UK in a Digital World, 2011. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>. Acesso em: 19 out. 2017.

UK PRIME MINISTER'S OFFICE, **Strategic Defence and Security Review, 2010.** Disponível em: <https://www.gov.uk/government/news/strategic-defence-and-security-review—3>. Acesso em: 23 out. 2017.

US DEPARTMENT OF DEFENSE. **The DoD Cyber Strategy.** Disponível em: <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> Acesso em: 19 out. 2017.

US GOVERMENT ACOUNTABILITY OFFICE. Defense Department Cyber Efforts. Disponível em: **DOD Faces Challenges In Its Cyber Activities**, Office, July 2011, <http://www.gao.gov/products/GAO-11-75> Acesso em: 23 out. 2017.

US GOVERMENT ACOUNTABILITY OFFICE. Defense Department Cyber Efforts. Disponível em: **More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities.**
<http://www.gao.gov/products/GAO-11-421>. Acesso em: 23 out. 2017.

US STRATEGIC COMMAND. **U.S. Cyber Command (USCYBERCOM).** Disponível em: <http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/> Acesso em: 19 out. 2017.

VITEL, P; BLIDDAL, H. **French Cyber Security and defense**: an overview. Information & Security International Journal, 2015.