MARINHA DO BRASIL
ESCOLA DE GUERRA NAVAL
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS MARÍTIMOS

EDUARDO ANDRÉ ARAUJO DE SOUZA

A QUESTÃO DA SEGURANÇA E DEFESA CIBERNÉTICA: O ESFORÇO POLÍTICO-ADMINISTRATIVO DA MARINHA DO BRASIL

Rio de Janeiro
2017

EDUARDO ANDRÉ ARAUJO DE SOUZA

A QUESTÃO DA SEGURANÇA E DEFESA CIBERNÉTICA: O ESFORÇO POLÍTICO-ADMINISTRATIVO DA MARINHA DO BRASIL

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Estudos Marítimos – PPGEM, da Escola de Guerra Naval, como parte dos requisitos necessários à obtenção do título de Mestre em Estudos Marítimos, área de concentração em Segurança, Defesa e Estratégia Marítima, Linha de Pesquisa em Ciência, Tecnologia, Inovação e Poder Marítimo.

Orientador: Prof. Dr. Nival Nunes de Almeida

Rio de Janeiro

2017

CATALOGAÇÃO NA FONTE

ESCOLA DE GUERRA NAVAL BIBLIOTECA

Souza, Eduardo André Araujo de
S729 A Questão de Segurança e Defesa Cibernética: O Esforço Político-Administrativo da Marinha do Brasil /Eduardo André Araujo de Souza. - Rio de Janeiro, 2017.
136f: il

Orientador: Professor Dr. Nival Nunes de Almeida
Dissertação (Mestrado) – Escola de Guerra Naval,
Programa de Pós-Graduação em Estudos Marítimos (PPGEM), 2017.

1. Segurança. 2. Defesa. 3. Cibernética. 4. Securitização.
I. Almeida, Nival Nunes de. II. Escola de Guerra Naval (BRASIL)
III.Título.

CDD 001.53

_____ _____

Assinatura Data

A QUESTÃO DA SEGURANÇA E DEFESA CIBERNÉTICA: O ESFORÇO POLÍTICO-ADMINISTRATIVO DA MARINHA DO BRASIL

EDUARDO ANDRÉ ARAUJO DE SOUZA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Estudos Marítimos – PPGEM, da Escola de Guerra Naval, como parte dos requisitos necessários à obtenção do título de Mestre em Estudos Marítimos, área de concentração em Segurança, Defesa e Estratégia Marítima, Linha de Pesquisa em Ciência, Tecnologia, Inovação e Poder Marítimo.

Aprovada em 28 de março de 2017.

Banca Examinadora:

_____

Prof. Dr. Nival Nunes de Almeida (EGN)

Doutor pela UFRJ – RJ, Brasil / CPF 711.482.567-68

_____

Prof. Dr. José Augusto Abreu de Moura (EGN)

Doutor pela UFF – RJ, Brasil / CPF 093.284.327-15

_____

Prof. Dr. Márcio Rocha (UFF)

Doutor pela UFF – RJ, Brasil / CPF 869.413.308-30

Rio de Janeiro

2017

DEDICATÓRIA

À lembrança carinhosa da memória de meus avós maternos, Mario de Oliveira Araujo e Maria Araujo, dedico este trabalho, que representa mais um degrau na busca contínua do aperfeiçoamento através da educação muito celebrada e valorizada por esses, que, a despeito de todas as dificuldades impostas em suas sacrificadas vidas, não mediram esforços para que seu neto pudesse usufruir das melhores condições de ensino possível. A eles, o meu eterno agradecimento.

AGRADECIMENTOS

A Deus, pela inspiração e força para continuar a caminhada até a vitória final.

À minha esposa, Joice de Albuquerque, pelos momentos de abnegação, apoio e paciência no transcurso desta etapa.

Ao meu filho, Enzo Gabriel Albuquerque de Souza, que, à revelia de sua vontade, fora privado da companhia de seu pai em detrimento dos esforços de pesquisa.

Ao Professor Doutor Nival Nunes de Almeida, orientador e amigo, que tem me conduzido nesta grande caminhada.

À banca examinadora, por sua valiosa contribuição a este trabalho.

Ao CF (CA) Collazo, pelos valorosos trabalhos de revisões, correções e sugestões a esta dissertação.

Aos colegas do CASNAV-30, pelo companheirismo, disponibilidade e incentivo ao longo da árdua caminhada.

Ao CASNAV, por mais essa oportunidade a mim concedida, os meus sinceros agradecimentos.

Agradeço também à Escola de Guerra Naval, em especial aos professores e a todo o pessoal de apoio, da Secretaria e da Administração.

Enfim, agradeço a todos que, direta ou indiretamente, me ajudaram nesta caminhada.

RESUMO

A segurança e a defesa cibernética tornaram-se cada vez mais presentes não só nas elevadas esferas de estudos estratégicos por parte dos Estados, como também no cotidiano do cidadão comum em sua lida com artefatos tecnológicos num mundo cada vez mais conectado. A percepção de uma gama de ameaças oriundas desse novo domínio justifica a necessidade de investimentos de ordem técnica e normativa como garantidores da disponibilidade, integridade, confidencialidade e autenticidade da informação. O espaço cibernético propriamente dito proporcionou à humanidade uma nova ordem global, contudo caótica e anárquica, tanto quanto a própria arena internacional. Este estudo buscou inicialmente uma fundamentação teórica para o estudo do conceito de segurança amparado pelas Relações Internacionais, identificando sua origem, evolução histórica e a proposta de ampliação da agenda dos estudos de segurança pelos estudiosos da Escola de Copenhagen ao apresentar a Teoria da Securitização. Com base nessa visão construtivista, em que se entende que os atores dessa arena são cada vez mais assimétricos e que o espaço cibernético é um objeto sujeito a uma variedade de ameaças, dirigiu-se o estudo para a forma na qual a Administração Pública Federal e, em particular, a Marinha do Brasil organizaram-se na condução da segurança e defesa do seu espaço cibernético, corroborando uma tratativa securitizadora.

Palavras-chaves: Segurança. Defesa. Cibernética. Securitização.

ABSTRACT

Security and cyber defense became more and more present not only in the high spheres of strategic studies on the part of the States, but also in the daily lives of the ordinary citizen in his dealing with technological artifacts in an increasingly connected world. The perception of a range of threats arising from this new area justifies the need for technical and regulatory investments as guarantors of the availability, integrity, confidentiality and authenticity of the information. Cyberspace itself has given mankind a new global order, yet chaotic and anarchic as much as the international arena itself. This study initially sought a theoretical basis for the study of the concept of security supported by International Relations, identifying its origin, historical evolution and the proposal to expand the security studies agenda by Copenhagen School´s academics in presenting the Theory of Securitization. Based on this constructivist view, where it is understood that the actors in this arena are increasingly asymmetrical and that cyberspace is an object under a variety of threats, the study was directed towards the way in which the Federal Public Administration and in particularly the Brazilian Navy organized themselves in the conduct of security and defense of their cyberspace, corroborating a securitizing issue.

Key words: Security. Defense. Cybernetic. Securitization.

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
AGNU	Assembleia Geral das Nações Unidas
APF	Administração Pública Federal
BONO	Boletim de Ordens e Notícias
C4I	Comando, Controle, Comunicações, Computação e Inteligência
CASNAV	Centro de Análise de Sistemas Navais
CCA	Centro de Computação da Aeronáutica
CCTOM	Centro de Comando do Teatro de Operações Marítimas
CDCiber	Comando de Defesa Cibernética
CDN	Conselho de Defesa Nacional
CEAGAR	Centro de Estudo e Avaliação da Guerra Aérea
CEMA	Chefe do Estado-Maior da Armada
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CETELMA	Central Telefônica da Marinha
CGSI	Comitê Gestor da Segurança da Informação
CIAER	Centro de Inteligência da Aeronáutica
CLTI	Centro Local de Tecnologia da Informação
COE	Centro de Operações da Esquadra
COMCITEM	Comissão de Ciência e Tecnologia da Marinha
COMCONTRAM	Comando do Controle Naval do Tráfego Marítimo
COM	Comando de Operações Navais
COPRI	Copenhagen Peace and Research Institute
CPESC	Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações
CREDEN	Câmara de Governo de Relações Exteriores e Defesa Nacional
CSN	Conselho de Segurança Nacional
CTIM	Centro de Tecnologia da Informação da Marinha
CTIR	Centro de Tratamento de Incidentes de Segurança em Redes de Computadores
CVE	*Common Vulnerabilities and Exposures*
DCTIM	Diretoria de Tecnologia da Informação
DDoS	*Distributed Denial of Service*
DE	Diretoria Especializada
DGMM	Diretoria-Geral de Material da Marinha
DIPNAV	Diretrizes para o Planejamento Naval
DIRTI	Diretoria de Tecnologia da Informação
DITEL	Diretoria de Telecomunicações
DN	Distritos Navais
DOU	Diário Oficial da União
DSIC	Departamento de Segurança da Informação e Comunicação
EB	Exército Brasileiro
EEM	Estudo de Estado-Maior
EMA	Estado Maior da Armada
EMAER	Estado-Maior da Aeronáutica
END	Estratégia Nacional de Defesa

ESG	Escola Superior de Guerra
EUA	Estados Unidos da América
FA	Forças Armadas
FAB	Força Aérea Brasileira
GC	Guerra Cibernética
GERN	Grupo Europeu de Pesquisa de Normas
GMDSS	*Global Maritime Distress and Safety System*
GSI	Gabinete de Segurança Institucional
GT-TI	Grupo de Trabalho em Tecnologia da Informação
HTTP	*Hyper Text Transport Protocol*
ICPBrasil	Infraestrutura de Chaves Públicas Brasil
IME	Instituto Militar de Engenharia
IN	Instrução Normativa
INMARSAT	Sistema que emprega satélites geoestacionários
IP	*Internet Protocol*
ISIS	*Islamic State of Iraq and Syria*
ITA	Instituto Tecnológico da Aeronáutica
ITI	Instituto Nacional de Tecnologia da Informação
ITU	União Internacional da Telecomunicação
LABGENE	Laboratório de Geração de Energia Nucleoelétrica
LRIT	Sistema de Identificação e Acompanhamento de Navios a Longa Distância
MB	Marinha do Brasil
MD	Ministério da Defesa
MIT	*Massachusetts Institute of Technology*
MJ	Ministério da Justiça
MP	Medida Provisória
NIC	*Network Internet Council*
NSA	*National Security Agency*
ODS	Órgãos de Direção Setorial
OEA	Organização dos Estados Americanos
OI	Organismos Internacionais
OM	Organizações Militares
ONU	Organização das Nações Unidas
OPEP	Organização dos Países Exportadores de Petróleo
ORCOM	Orientações do Comandante da Marinha
OTAN	Organização do Tratado do Atlântico Norte
PEM	Plano Estratégico da Marinha
PETIM	Plano Estratégico de Tecnologia da Informação da Marinha
PF	Polícia Federal
PR	Presidência da República
PREPS	Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite
PROSUB	Programa de Desenvolvimento de Submarinos
RECIM	Rede de Comunicação Interna da Marinha
RETELMA	Rede de Telefonia da Marinha
RI	Relações Internacionais
SIC	Segurança da Informação e Comunicação

SID	Segurança da Informação Digital
SIMMAP	Sistema de Monitoramento Marítimo de Apoio às Atividades de Petróleo
SISBIN	Sistema Brasileiro de Inteligência
SISCOM	Sistema de Comunicações da Marinha
SISTRAM	Sistema de Informações Sobre o Tráfego Marítimo
SMDC	Sistema Militar de Defesa Cibernética
SOA	Supervisor Operacional de Área
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
EU	União Europeia
URSS	União das Repúblicas Socialistas Soviéticas
VoIP	*Voice over IP*
V-RMTC	*Virtual Regional Maritime Traffic Centre*
WAN	*Wide Area Network*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O estudo da segurança e dos conflitos são objetos de análise desde os primórdios da criação dos Estados nacionais. A segurança nacional e internacional encontra-se presente na agenda e nos discursos de muitos Estados e seus governos, assim como o estudo da guerra toma a atenção de várias gerações de estudiosos nos setores estratégicos e militares.

A Era da Informação, da comunicação e do conhecimento traz elementos fundamentais para as questões de Estado e dos conflitos internacionais.

O espaço cibernético[1] proporciona conectividade e integração global em tempo real. Contudo, essa fluidez nas relações carrega em si uma fragilidade a qual gera uma grande ordem de vulnerabilidades que, aliada à existência de novos atores de caráter transnacional, agrava a preocupação com a proteção da informação, dando origem à segurança da informação e, num segundo momento, evolui para os conceitos de segurança e defesa – momento que o Estado preocupa-se também com a proteção das Infraestruturas Críticas[2] em seu entorno para sua própria sobrevivência.

O fenômeno da guerra e a agenda de segurança transformaram-se ao longo da história, principalmente após o término da Guerra Fria. Os instrumentos, as finalidades, as táticas de combate, a tecnologia utilizada, entre outros, fizeram parte da evolução das gerações e da natureza dos conflitos.

Como resultante do considerável salto tecnológico dos anos 1990 e 2000, novos elementos tornaram-se relevantes nos litígios e negociações interestatais. Dessa forma, as tecnologias de informação e comunicação (TICs) denotam importância para a formação de um novo campo de batalha na arena internacional: o espaço cibernético.

Sendo utilizado inicialmente como: meio de espionagem, sabotagem, ataques contra sistemas computacionais, mapeamento e enfraquecimento de forças militares hostis, o espaço

[1] 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. 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 sinéticos e, frequentemente, decisivos. (BRASIL, 2014).

[2] Infraestruturas críticas (IC): instalações, serviços, bens e sistemas exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras infraestruturas críticas, mais complexas ou não. Com o passar dos anos, a interdependências verticais das infraestruturas críticas, caracterizadas por um baixo acoplamento entre elas, deu lugar às interdependências horizontais altamente acopladas, com muitos pontos de interação em suas dimensões. (BAGHERY, 2007).

cibernético pode tornar-se um dos domínios de defesa mais importante do novo século.

No complexo tabuleiro das Relações Internacionais, a resolução de conflitos através da "política por outros meios" é cada vez mais inovadora ao fazer uso da arena virtual em detrimento do conflito tradicional que é bem definido, regrado e caracterizado pela responsabilidade dos Estados.

O conflito cibernético possui aspectos *sui generis*, como: a ordem de motivações para ações e a composição do grupo hostil (que pode ou não possuir vínculo com um Estado), tornando difícil a responsabilização.

As hostilidades nesse campo possuem a vantagem do anonimato, podendo interagir igualmente com outros domínios, auxiliando em uma guerra convencional. A cada regra imposta ao uso da força, novas formas de conflito são criadas.

No entanto, o conflito no espaço cibernético não perde algumas características da ortodoxia do modelo de guerra proposto por Clausewitz enquanto impregnam-se das diversas conotações das chamadas novas guerras[3].

No transcorrer desse processo evolutivo, a agenda de segurança perde seu caráter primordialmente militar e acolhe novas matérias no debate. Onde outrora prevaleciam tópicos de caráter relevantes para a Guerra Fria, agora são seguidos por temas econômicos e ambientais e também pela questão cibernética. Nesse sentido, os estudos abrangentes da agenda de segurança sob a perspectiva construtivista das Relações Internacionais colocam-se como uma opção para embasamento do trabalho.

A presença de novos atores na arena internacional revelou uma tendência de assimetria nos conflitos cibernéticos, ampliando o sentido de ameaça, cada vez mais transnacional, e trazendo consigo novos temas de segurança. Os ataques no espaço cibernético ocorrem de forma autônoma, ligados diretamente ou não a atores Estatais.

Além do mais, vale ressaltar o crescimento dos chamados exércitos eletrônicos ou organizações por procuração[4], como acontece na Rússia, na China, nos Estados Unidos da

[3] Novas Guerras: ver Kaldor, Mary – New and Old Wars – Organized Violence in a Global Era.Stanford, Ca., Stanford University Press, 1999, 206 páginas. A linha analítica seguida pela autora diferencia-se de outras abordagens, definindo as novas guerras como civis, étnicas ou resultantes da mera privatização da violência, uma vez que destaca o caráter essencialmente político das novas guerras.

[4] Organizações por procuração: a articulação entre atores estatais e não estatais para efeitos de ciberataques, parece existir em vários países. Um caso é o da China que integra, desde inícios da década passada, na sua organização militar, unidades preparadas para atividades de ciberguerra. Por exemplo, "a milícia da cidade de Guangzhou criou um batalhão de guerra de informação organizado em torno das instalações da empresa de comunicações dessa província chinesa. Esse batalhão abrange companhias de guerra de redes de computadores e de guerra eletrônica". A referida estratégia coloca o problema das múltiplas identidades dos seus intervenientes. Assim, "é possível, para uma mesma unidade de milícia de ações de ciberguerra, ser, ao mesmo tempo, um departamento de tecnologias de informação numa universidade, uma agência de publicidade on-

América (EUA) e na Síria.

A comunidade internacional apresenta um entendimento de que a segurança do espaço cibernético é um tema novo: uma nova agenda que se abre para as Relações Internacionais contemporâneas, observando-se um movimento no processo de securitização desse espaço por parte dos Estados. Em paralelo, observa-se uma crescente utilização dos elementos do setor cibernético de forma cada vez mais ofensiva entre Estados e Organizações numa perspectiva primariamente realista.

A abordagem securitizada no tratamento da insegurança do espaço cibernético no Brasil alinha-se ao esforço mais amplo de redefinir o papel das forças armadas no país para o século 21.

Na crescente consolidação do estado democrático no Brasil, as forças armadas reavaliam seu papel e postura relativos às ameaças não tradicionais: por um lado, solidificando suas preocupações com temas historicamente vinculados às suas ações como o controle de fronteiras e a presença brasileira em espaços geográficos de interesse estratégico; por outro lado, ampliando seu alcance e influência no domínio dinâmico e em constante evolução do espaço cibernético.

O desenvolvimento de capacidade inicialmente militarizada para a resposta cibernética possui inspiração no esforço e desejo do Estado brasileiro em estabelecer-se geopoliticamente nessa arena e na manutenção de sua autonomia no cenário internacional.

1.1 MOTIVAÇÃO PARA A PESQUISA

O cenário da segurança e defesa do espaço cibernético no Brasil carece de uma investigação sobre o grau de organização e atuação de seus atores estatais. A relevância da questão de segurança e defesa cibernética é preconizada na Estratégia Nacional de Defesa como item estratégico.

A Marinha do Brasil, instituição pioneira no emprego da Tecnologia da Informação e Comunicação no Brasil, em 2008 realizou uma reestruturação organizacional significativa em torno da questão de segurança e defesa cibernética, mostrando seu avançado grau de politização[5].

A análise desse arcabouço político-administrativo do Poder Naval é o propelente desta

---

line, um clã de jogo online, uma equipe de hackers patrióticos e um sindicato do cibercrime local envolvido em pirataria informática". (KLIMBURG, 2011, p.42).

[5] Politização: ocorre quando o assunto torna-se parte de políticas públicas, exigindo decisão governamental e alocação de recursos. (BUZAN et al.,1998, p. 23).

proposta de pesquisa, visando contribuir com o autoconhecimento institucional.

1.2 HIPÓTESE

Dada a relevância das ações cibernéticas nos conflitos interestatais modernos, as práticas organizacionais da Marinha do Brasil denotam que seu espaço cibernético é securitizado.

1.3 OBJETIVOS

1.3.1 Geral

O objetivo geral do trabalho é realizar um estudo exploratório na questão de segurança e defesa do espaço cibernético sob o ordenamento político-administrativo da Marinha do Brasil em seu entorno e confrontá-los com uma base científica sob a óptica construtivista das Relações Internacionais da Escola de Copenhagen[6].

1.3.2 Específicos

a) Revisar os conceitos básicos de segurança de acordo com os fundamentos teóricos das Relações Internacionais;
b) revisar os conceitos relacionados ao espaço cibernético (terminologias, componentes e características);
c) identificar no ordenamento da Administração Pública Federal a organização e tratamento dado à questão de segurança e defesa do espaço cibernético brasileiro;
d) analisar as ações da Marinha do Brasil para o seu entorno cibernético, tendo como base seu conjunto regulatório, organizacional e estrutural.

[6] A Escola de Copenhagen de Estudos de Segurança é uma escola de pensamento acadêmico com suas origens nas teorias de Relações Internacionais publicadas na obra de Barry Buzan: *Povos, Estados e o Medo*: O Problema de Segurança Nacional em Relações Internacionais. A Escola de Copenhagen coloca particular ênfase nos aspectos sociais da segurança. Seus principais teóricos associados com a escola são: Barry Buzan, Ole Wæver e Jaap de Wilde. Muitos dos membros da escola trabalharam no Instituto de Pesquisa da Paz de Copenhagen. A principal contribuição da Escola de Copenhagen é a obra *Segurança*: Um Novo Enquadramento para Análise, escrita por Buzan, Wæver e de Wilde. A teoria centra-se em três conceitos-chave: Setores; Complexos de Segurança Regionais; Securitização. (Eriksson, Johan. Revisiting Copenhagen Observers or Advocates?: On the Political Role of Security Analysts, *Cooperation and Conflict*, n. 3, p. 311-313, 1999).

1.4 JUSTIFICATIVA

O movimento convergente das Forças Armadas brasileiras na questão da segurança e defesa do Espaço cibernético com o discurso do Estado brasileiro e a comprovada politização da matéria através de estatutos, normas, procedimentos e capacitação de pessoal no segmento das Tecnologias de Informação e Comunicação.

1.5 METODOLOGIA DA PESQUISA

O presente trabalho foi desenvolvido por meio de uma abordagem metodológica exploratória com procedimento monográfico utilizando as seguintes estratégias:

a) Revisão de literatura: em um primeiro momento, serão analisadas a epistemologia do conceito de segurança, as transformações do conceito de segurança, as principais linhas de pensamento nas Relações Internacionais e a apresentação da Teoria da Securitização da Linha Construtivista e sua correlação conceitual apresentados nas obras de Barry Buzan e Ole Waever;
b) revisão de literatura e delimitação do objeto em estudo: espaço cibernético, sua interdisciplinaridade, a relação Estado-Tecnologia e sua correlação conceitual apresentada nas obras de Wiener, Lévy, Moreira e Ventre;
c) análise de citação: identificação dos pesquisadores da questão cibernética que citam a Securitização e Defesa do Estado como motivador de trabalhos acadêmicos;
d) análise de conteúdo: análise formal por leitura técnica dos artigos no intuito de identificar neles a fundamentação do emprego cibernético como um Novo Domínio de Defesa. Momento no qual se realiza uma análise dos conceitos e construtos teóricos adotados nos trabalhos identificados;
e) análise interpretativa: com base nas questões apresentadas procurando identificar como tais questões aparecem e como são afeitas às Forças Armadas e em particular à Marinha do Brasil;
f) simulação de um cenário de planejamento de um ataque cibernético a um sistema operativo; e
g) análise crítica-qualitativa quanto ao grau de securitização do espaço cibernético no âmbito da Marinha do Brasil ante o fato do grau de evolução de seus processos de Segurança.

1.6 ESTRUTURA DE DESENVOLVIMENTO DO TRABALHO

A estrutura de desenvolvimento deste trabalho está definida numa sequência que parte da revisão da literatura sobre o conceito de segurança nas RI e dos conceitos basilares sobre espaço cibernético, seguida da organização do espaço cibernético brasileiro. Por fim, com a organização da MB em seu entorno cibernético, simula-se o planejamento de um ataque cibernético a um sistema operativo e apresentam-se as considerações finais.

No capítulo 2, realiza-se uma revisão da literatura sobre conceitos segurança nas RI e trata-se dos seguintes temas: a evolução do conceito no transcurso da história, a evolução dos conflitos e natureza da agenda de segurança dos Estados, a escola de pensamento construtivista e a Teoria da Securitização, utilizando como base as produções acadêmicas de autores como Barry Buzan e Ole Waever.

O capítulo 3 traz a revisão dos conceitos sobre espaço cibernético, os componentes e as características relacionadas a esse meio, fazendo uma análise de como uma ameaça cibernética pode se manifestar no cenário internacional. Também será abordado o papel dos atores no espaço cibernético brasileiro e da base normativa brasileira e sua evolução nessa primeira década dos anos 2000. As fontes primárias tomadas para auxiliar na construção desse capítulo serão produções acadêmicas dos autores: Claudia Cannongia e Raphael Mandarino JR, Walfredo B. Ferreira Neto, Myrian Dunn, Hanssen, Nissenbaum e Thomas Rid. As principais fontes secundárias e auxiliares serão artigos científicos depositados na Escola de Comando e Estado Maior do Exército (ECEME), artigos científicos depositados na Escola de Guerra Naval (EGN) e a publicação de Desafios Estratégicos para a Segurança e Defesa Cibernética da Secretaria de Assuntos Estratégicos.

No capítulo 4, identifica-se a estrutura politico-administrativa da Marinha do Brasil (MB) quanto à questão cibernética e seu conjunto normativo, além de examinar o escopo do espaço cibernético da Marinha do Brasil.

O capítulo 5 ilustra uma simulação do planejamento de um eventual ataque a um sistema operado pelo Centro de Controle de Tráfego Marítimo.

Por fim, o capítulo 6 conclui a pesquisa com uma síntese do conceito de segurança das RI e o modelo securitizador sob a ótica construtivista e seu emprego na questão de segurança e defesa cibernética, além de apontar as transformações organizacionais na MB sobre a questão de cibernética e propor um conjunto de ações para a manutenção da securitização

cibernética.

2 INTRODUÇÃO AOS ESTUDOS DE SEGURANÇA

Antes de iniciarmos nossa pesquisa sobre a evolução da segurança cibernética e a investigação de um possível processo de securitização no âmbito do Poder Naval Brasileiro, faz-se mister o estudo aprofundado do conceito de segurança em si; sua evolução ao longo da história e a forma como os estudiosos das Relações Internacionais abordam o tema.

"O conceito de segurança se relaciona com uma diferente tradição filosófica, da mesma forma que remete a uma interpretação histórica específica das Relações Internacionais". (HAFTENDORN, 1990, p. 4). No transcorrer do trabalho, a concepção do que é segurança está inicialmente baseada em questionamentos de ordem epistemológica, ontológica e metodológica na Teoria das Relações Internacionais. Lembrando ainda que o conceito de segurança possui uma relação íntima com os desenvolvimentos históricos que têm lugar no sistema internacional com interação dos atores que o compõem.

Dessa forma, a ideia de segurança deve ser necessariamente considerada como um constructo sociopolítico que lhe confere significado. Constata-se nesses termos que:

> '**Segurança**' é um conceito socialmente construído. Ele tem um significado específico somente dentro de um contexto social particular. O significado do conceito recebido está, dessa forma, sujeito a mutações que resultam das mudanças materiais no ambiente externo [à teoria] e nos modos em que pensamos estas questões (SHEEHAN, 2005, p. 43, grifo nosso).

O trabalho, em sua primeira parte, é conduzido pela história do conceito de segurança e investiga se o sentido contemporâneo diverge de sua origem ao analisar a etimologia da palavra. Em sequência, propõe-se uma análise da literatura buscando o debate da questão segurança dentro das escolas de pensamento da disciplina de Relações Internacionais.

Partimos do pressuposto de que não existe significância simples para o conceito de segurança, nem de forma pretérita ao ***Estado-nação***[7] tampouco em suas acepções posteriores emergentes da história, tais como: segurança nacional, Segurança Internacional ou segurança global (HAFTENDORN, 1990, p. 3-5), sendo que cada um desses significados históricos deriva de diferentes raízes filosóficas, permitindo diferenciados usos e aplicações a distintos objetos de referência ao longo de diferentes contextos históricos.

[7] O Estado-nação é a unidade político-territorial própria do capitalismo. Embora tenha naturalmente pontos de contato com o império pré-capitalista, dele diferencia-se essencialmente porque a nação busca, no seu território, constituir-se em uma sociedade nacional integrada e voltada para o desenvolvimento econômico, enquanto que as oligarquias dominantes nos impérios não sabem o que seja o desenvolvimento econômico, e não buscam integrar econômica e culturalmente suas colônias das quais apenas exigem o pagamento de impostos. (GELLNER, 1993).

Uma forma simplista, e analiticamente limitada, seria adotar o entendimento de segurança como a ausência de ameaças militares de origem externa à sobrevivência ou soberania do Estado-nação em um sistema internacional anárquico, pois, de acordo com McSweeney (1999, p. 1): "segurança é um termo escorregadio", visto que seu uso é feito por uma diversidade de agentes políticos, tais como: acadêmicos, atores governamentais, organizações internacionais ou mesmo o cidadão comum – para propósitos distintos nos mais diversos contextos.

Em não havendo consenso sobre o significado do termo (segurança), ele habita discursos de públicos divergentes tanto de militantes de direitos humanos quanto de militares, e, dessa forma, há necessidade de se realizar um levantamento abrangente da história do conceito de segurança e de seus usos tanto em tempos pretéritos quanto na atualidade (quando intensivamente associado aos estudos da área de Relações Internacionais).

2.1 O ESTUDO DA SEGURANÇA

A inspiração original que institucionalizou a disciplina (RI) ao longo primeira metade do século XX advém da necessária compreensão do fenômeno da guerra com o intuito de evitar que os flagelos da Primeira Grande Guerra se repetissem no futuro. Dessa forma, pensar as Relações Internacionais implicava em pensar a Guerra e pensar a Guerra era pensar a violência; e pensar a violência nos levaria a pensar a segurança.

Sendo assim, ao longo das décadas pós-conflito mundial, a corrente de pensamento realista[8] foi aceita como a teoria dominante no estudo das Relações Internacionais, ao ditar os limites aos quais poderiam se desenvolver a disciplina. Nesse período, essa corrente de pensamento sobrepôs-se às demais abordagens que não se alinhassem à sua ortodoxia.

[8] A teoria realista (realismo) é, sem dúvida alguma, a mais importante de todas quando se trata de Relações Internacionais, e talvez, quando se fala em política internacional, o realismo seja a mais adequadamente nominada. Isso porque o realismo trata basicamente, quase exclusivamente, das relações políticas entre os estados, considerando válidas apenas as variáveis políticas, isto é, diplomáticas e militar-estratégicas. Inspirada em Maquiavel e principalmente em Hobbes, com seu estado de natureza de "guerra de todos contra todos", a teoria realista surgiu em contraposição ao idealismo, e no século XX – período de maior sistematização seus primeiros autores foram Edmund Carr (1981) e principalmente Hans Morgenthau (1985). Uma grande fonte de inspiração teórica é a filosofia de Thomas Hobbes, para quem os homens, quando no estado de natureza, ou seja, quando vivem sem uma autoridade superior capaz de determinar as regras mútuas de convivência e de implementar essas regras (isto é, de impor a ordem), vivem em uma situação de permanente conflito e de "anarquia", na qual cada um é responsável por sua própria preservação, buscando o máximo de poder possível a fim de manter sua integridade física. Como essa atitude é compartilhada por todos, o que ocorre é uma constante disputa pelo acúmulo de poder, em um jogo claramente de soma zero. (LACERA, Gustavo Biscaia de. Algumas teorias das Relações Internacionais: realismo, idealismo e grocianismo, *Revista Intersaberes*, v..1, n. 1, p. 56-77, jan./jun. 2006).

Consequentemente, inúmeros conceitos sofreram forte influência do pensamento realista. O conceito de segurança não fugiria a regra.

Ao longo de sua história, o conceito de segurança sofreu significativas mudanças, adquirindo caráter central no estabelecimento dos limites e da própria identidade das Relações Internacionais. Mas, apesar do papel de central relevância, o conceito de segurança permaneceu longo tempo sem ser problematizado pelos teóricos.

2.2 A HISTÓRIA DO CONCEITO

Todos os autores iniciam suas respectivas narrativas a partir da origem do conceito de segurança no latim, levando-nos posteriormente até seus usos mais contemporâneos na língua inglesa (o idioma em que seus textos são originalmente escritos), mas, no transcorrer da análise do conceito de segurança, não devemos pressupor que sejamos capazes de definir o que se entende por segurança de forma universal no tempo e no espaço.

A investigação sobre o que a noção de segurança "se tornou" através da história conduz a diferentes sentidos que a terminologia adquiriu no passado e evidencia suas recorrentes mutações semânticas, em que observamos a multiplicidade e a diversidade dos debates acerca da ideia de segurança. E identifica pontos de aproximação, até onde seja possível, observando as diferentes conotações semânticas que o conceito de segurança veio a adquirir ao longo de sua trajetória histórico-etimológica, analisando sua complexidade e variedade, ao invés de buscar a definição de uma essência.

De acordo McSweeney (1999, p. 1), a etimologia da palavra inglesa *secure* (ao referir-se ao estado do sujeito que desfruta de segurança) advém da expressão latina *se cura*, na qual seu significado é: "livre de preocupação" (*free from concern*). O mesmo radical latino exerceu influência na palavra de origem inglesa ***sure*** e no vocábulo francês ***sûr***. Nessa última língua, segundo o Larousse Modern Dictionary, uma importante distinção se faz necessária: o significado de *securité/safety* (a percepção subjetiva de não ter nada a temer) difere consideravelmente do sentido de *sûreté/surety* (a situação objetiva de não ter nada a temer).

A língua portuguesa, de origem latina, não opera essa diferenciação, como demostrado no primeiro dicionário da língua portuguesa da história, o *Vocabulário portuguez e latino*, de autoria do padre Raphael Bluteau[9] (1638-1734).

[9] O padre Raphael Bluteau (1638-1734) nasceu em Londres, mas se mudou para Portugal em 1668 a mando de seus superiores da Ordem de São Caetano (os teatinos, de Caetano de Thiene). Foi então que escreveu o *Vocabulário*. Em 2008, o dicionário foi inteiramente digitalizado por alunos e docentes do Instituto de Estudos

A obra define que está "seguro" aquele sujeito que se vê "livre de algum perigo, ou de receio dele" (p. 556), convergindo no português aquilo que se distingue nas línguas francesa e inglesa. Seguro é "coisa, que não tem perigo, em que não há que recear" é o "lugar seguro das violências do inimigo" (p. 555). "Segurança", por sua vez, é o "Estado em que não há que recear maus sucessos [isto é, maus acontecimentos]" (p. 553). E o verbo "segurar" é "afirmar como coisa certa" (p.554), é assegurar, dar certeza (aproximando-se das concepções de *sure/sûr*), mas é também "livrá-lo [a alguém] de todo gênero de medo" (próximo agora da noção de *free from concern*). Numa primeira abordagem, um determinado sujeito detentor de conhecimento poder estar seguro de alguma opinião. Nesse sentido, ele teria certeza sobre algo, como na frase "estou seguro de que alcançaremos nossas metas". Em uma segunda conotação, um determinado sujeito poder estar seguro contra alguma ameaça. Nesse caso, ele teria segurança *versus* algo ou em contraposição a alguém, tal como na frase "estou seguro contra agressões, pois tenho equipamentos de proteção".

Em resumo: embora posteriormente os termos analisados venham a sofrer uma espécie de "bifurcação semântica", originalmente as expressões: *se cura* (do latin) e *being secure* (do inglês), das quais derivam o conceito de segurança, faziam referência à ideia de "estar seguro" de algo e não contra algo. Em momentos anteriores, pois "a liberdade da segurança está relacionada: 1) à possessão do conhecimento; 2) à convicção na previsibilidade das coisas e/ou; 3) a estar ciente da ordem objetiva". (MCSWEENEY, 1999, p. 17). Observamos a relevância do substantivo (segurança) e seu significado (estar seguro é ter, sim, certeza) que somente *a posteriori* viria a adquirir um sentido adicional que o definiria também por negação (ser seguro é não ser ameaçado ou não perceber ameaça). Numa contraposição de ideias, temos num primeiro momento a presença de certeza e num segundo momento a ausência de ameaça.

Ole Waever caminha num entendimento semelhante ao de Mcsweeney em sua identificação, no mesmo radical latino, *se cura*, como a origem do termo (segurança), conforme nos revela o autor:

> As palavras usadas nas línguas inglesas e românicas [isto é, latinas] derivam do [termo] romano 'securus', 'se' significando 'sem' e 'cura' significando

Brasileiros (IEB) da Universidade de São Paulo (USP) e está disponível para consulta pública e gratuita na internet. Segundo informações da Agência FAPESP (ROMERO, 2008), "os primeiros oito volumes que compõem o dicionário foram publicados ao longo de dez anos: volumes 1 e 2 em 1712, volumes 3 e 4 em 1713, volume 5 em 1716, volumes 6 e 7 em 1720 e o volume 8 em 1721. Juntaram-se a esses oito volumes dois suplementos publicados entre 1727 e 1728, contendo mais de 5 mil vocábulos que não constavam nas edições anteriores". Para consultar a página com a versão digital do *Vocabulário portuguez e latino*, acessar: <http://www.ieb.usp.br/online/>.

> ‘preocupação’. Quando foi introduzida no primeiro século antes de Cristo, provavelmente pelos Epicuristas e Estoicos, [a noção de segurança] se referia originalmente a um estado da mente [...]. Era, visivelmente, uma negação [pois fala do estado de não ter preocupação]. Hoje tendemos a pensar a segurança como alguma ‘coisa’ (e sua ausência como a insegurança), mas para os romanos, uma palavra [que fosse utilizada para designar o estado de] insegurança seria uma dupla negativa [que lhes pareceria] desprovida de sentido [algo como a expressão ‘sem-ausência-de-preocupação’] (2004, p. 54).

Entende-se nesse período que a ideia de segurança está intimamente relacionada ao indivíduo, pois, em última instância, era o próprio indivíduo seu portador da certeza e o beneficiário do estado de “se cura”. Acompanhando o pensamento de Waever, Rothschild revela também a percepção psicológica estritamente subjetiva.

> O substantivo latino “securitas” se referia, em seu uso clássico primário, a uma condição dos indivíduos, [um estado] particularmente de tipo interno. Ele denotava serenidade, tranquilidade de espírito, estar livre de preocupações, a condição que Cícero chamou de “objeto do supremo desejo” ou “a ausência de ansiedade da qual depende a vida feliz depende”. Um dos principais sinônimos para “securitas”, no Lexicon Taciteum, é [a expressão alemã] “Sicherheitsgefuhl”: o sentimento de estar seguro. A palavra assumiu depois um significado diferente e oposto, ainda relacionado à condição interna do espírito: ela denotou não o estado de liberdade frente à preocupação, mas descuido e negligência [que derivam da certeza acrítica, em uma ideia de segurança como uma condição de confiança cega e equivocada em algo. (1995, tradução nossa).

O contrassenso do termo ora com uma conotação positiva ora negativa foi uma constante no pensamento filosófico do cristão europeu durante todo o período medieval. A ideia de segurança como ausência de preocupação sempre representou uma ambiguidade do referencial teológico-filosófico, pois se partia do pressuposto de que somente o criador (Deus) poderia ter pleno conhecimento sobre a real possibilidade da salvação.

Não obstante, seria uma grande presunção do ser humano pensar que um mero mortal pudesse aspirar à condição de “se cura”. Dessa forma, ao cristão, na condição de criatura e sujeito à mortalidade, seria impossível estar seguro/certo de sua salvação e, assim, se desvencilhar de toda preocupação quanto ao seu futuro espiritual, já que essa certeza está somente ao alcance de Deus.

2.3 AS MUTAÇÕES DO CONCEITO

Para pensadores como Thomas Hobbes, em sua evolução vocabular da Antiguidade até o final da Idade das Trevas, o conceito tanto físico quanto psíquico sobre segurança prevalecia vinculado ao indivíduo. Contudo, há teóricos políticos – com destaque para aqueles de viés

liberal – que entendem que a segurança é um atributo individual, embora o Estado seja concebido como seu garantidor por excelência.

"O direito do individuo à autopreservação é o ponto de partida para o argumento de Hobbes sobre o Leviatã. O significado último e a medida de segurança é a segurança do indivíduo, mas ela é alcançada investindo-se autoridade no Estado". (WAEVER, 2004, p. 55).

O exposto por Thomas Hobbes traz à baila uma inflexão do conceito segurança que até então excluía a presença de uma Entidade Estatal como garantidora do *status quo*.

O período Liberal da Revolução Francesa marca uma mutação significativa quando a segurança como direito individual ganha fundamento em oposição à ideia de segurança pública promovida pelo Comitê para Salvação Pública[10] (Terror 1793 – 1794). Uma das vítimas desse período foi o Marques de Condorcet[11], que foi um dos principais expoentes intelectuais do movimento revolucionário francês e o responsável por exprimir de forma clara os traços liberais, racionalistas e individualistas que o conceito iluminista de segurança veio a adquirir a partir de então: em sua contribuição para a nova Declaração dos Direitos do Homem e do Cidadão de 1793, Condorcet estipularia que "a segurança consiste da proteção que cada sociedade confere a cada cidadão [que dela faz parte], para a conservação de sua pessoa, sua propriedade e seus direitos" (CONDORCET apud ROTHSCHILD, 1995).

Nesse momento, observa-se que a segurança seria garantida ao indivíduo mediante ao estabelecimento de um contrato social, conforme Hobbes. O medo em si era a representação do pensamento liberal. Essa movimentação lógica veio a incitar a distinção entre as palavras "*sûreté*" e "*securité*" na língua francesa, assim como viabilizou o novo conceito de "security", o qual não se restringia ao seu uso tradicional e passa a denotar também a ausência de ameaças externas à comunidade política.

---

[10] O nome original do Comitê era Comité de Salut Publique. O termo francês salut é mais comumente traduzido como "salvação", sobretudo quando aplicado à termologia militar como na expressão *l'armée du salut*, traduzida como "o exército da salvação". No contexto de nossa discussão, a tradução mais adequada de *salut* parece ser segurança, como também parecem crer os tradutores para a língua inglesa, que se referem ao Comité de Salut Publique com a expressão Committee for Public Safety. (vide ROTHSCHILD, 1995).

[11] Marie Jean Antoine Nicolas de Caritat, o Marquês de Condorcet (1743-1794), foi uma das mais importantes figuras políticas e intelectuais da Revolução Francesa. Condorcet foi membro do Comitê Constitucional, responsável por escrever a nova constituição da França e apoiou o julgamento do Rei Luis XVI, embora tenha se oposto à pena de morte. Conforme o grupo dos Montagnard (jacobinos liderados por Robespierre) ganhava importância dentro da Convenção em detrimento dos girondinos (dos quais Condorcet era próximo), Condorcet começou a sofrer pressões e seu esboço de constituição foi distorcido por Marie-Jean Hérault de Seychelles, que propôs uma "Constituição Montagnard" em substituição. Condorcet discordou da proposta e foi acusado de traição. Em outubro de 1793, foi expedido um mandado de prisão. Condorcet fugiu para a clandestinidade, mas foi capturado em março de 1794, quando, temendo por sua segurança, tentou fugir de Paris. Poucos dias depois de preso, foi encontrado morto em sua cela. A explicação mais aceita para sua morte é que seu amigo Pierre Jean George Cabanis teria lhe fornecido veneno para suicídio, mas acredita-se também que possa ter sido morto longe dos olhares públicos para evitar comoções daqueles que o admiravam.

O desdobramento desse último movimento é a nova face do conceito de segurança; uma face coletiva implícita na individual.

> A segurança individual, no pensamento liberal do Iluminismo, é tanto um bem individual quanto coletivo. Ela é uma condição e um objetivo dos indivíduos. Entretanto, ela pode somente ser alcançada por meio de algum tipo de empreendimento coletivo. Sendo assim, esta nova acepção é bastante diferente, nesse sentido, da segurança de caráter interno e introspectivo do pensamento político romano. Ela diferencia-se também da segurança com a qual os indivíduos podiam ser dotados por uma autoridade benevolente, caridosa e humanitária [mas que lhes é exógena, tal como Deus no pensamento cristão medieval]. É [agora] algo que os indivíduos obtêm por si mesmos, em um empreendimento coletivo ou contratual. O empreendimento, por sua vez, é algo a ser eternamente revisado e revisto. A segurança não é algo bom em si mesmo, se não levar-se em consideração o processo através do qual ela foi alcançada. O Estado (assim como pequenas coletividades dotadas de muito poder como as **guildas**[12] ou comunidades operando sob a proteção estatal) pode ser fonte tanto de insegurança, quanto de uma segurança que seja opressiva. [Do ponto de vista dos liberais que foram vítimas da repressão política organizada como Condorcet] a função mais importante, da segurança, é garantir a justiça para os indivíduos, resguardando-os de potenciais excessos oriundos da tirania do Estado. (ROTHSCHILD, 1995, tradução e grifo nosso).

Ainda no período revolucionário francês, durante a fase napoleônica, o conceito de segurança sofre um novo revés, em que a semântica dele carrega em si o aspecto coletivo sobrepondo-se ao individual, mesmo que timidamente. A questão de segurança passa a ser tratada como um bem coletivo que deveria ser garantido com esforços diplomáticos e militares, ou seja, a presença significativa do Estado nessa equação.

Estado e Indivíduos equiparar-se-iam na busca pela segurança, e, dessa forma, esse antropomorfismo faz com que a segurança do Estado se torne condição para a segurança do Indivíduo.

Nesse sentido, é durante o período militar da Revolução Francesa que a segurança dos indivíduos passa a depender intimamente da segurança da nação.

> A segurança se tornaria o vínculo crucial entre estes dois objetos de referência: ela converte-se em condição, ou objetivo que constitui a relação entre os indivíduos e os seus respectivos Estados ou sociedades. (ROTHSCHILD, 1995, tradução nossa).

Comparativamente com a evolução do processo histórico do conceito na Antiguidade e na Idade Média, observa-se que o pensamento político moderno, em curto espaço temporal, sofre duas transformações significativas: embora a segurança seja concebida como um

[12] Guildas: antigas associações ou ligas profissionais criadas com a finalidade de defender os interesses de seus integrantes, tinham como base, de acordo com Russomano (1992, p. 9-10), "um sentimento transcendental de companheirismo, lealdade e, inclusive, justiça. [...] As guildas espiritualizaram as relações humanas associativas e estimularam a formação de vínculos de solidariedade recíproca entre seus membros". Vide RUSSOMANO, M. V. *Princípios gerais de Direito Sindical*. Rio de Janeiro: Forense, 2000.

atributo inerente ao indivíduo, passa-se a crer que somente por um processo político de caráter coletivo ela possa ser alcançada. A segunda transformação dá-se pelo entendimento de que as coletividades nacionais são dotadas de interesse único, monolítica e indivisível e, sendo assim, tornam a lógica da segurança individual extensível à segurança nacional.

O intervalo temporal da segunda metade dos anos 1700 até o primeiro quarto dos anos 1800 alicerçaram o uso extensivo da ideia de Segurança Nacional, com destaque para o marco histórico do fim das Guerras Revolucionárias Napoleônicas em 1815.

Em nome da Segurança Nacional, em caso de extrema necessidade, o indivíduo teria o dever de abdicar de seus direitos e como último recurso da própria vida em defesa da coletividade representada agora pela ideia de Estado-nação.

> A busca e a luta pela preservação incondicional da soberania e integridade do Estado-nação ganham progressivamente mais terreno no campo da política e adquirem reforçada expressão no âmbito conceitual. (HAFTENDORN, 1990, p. 6, tradução nossa).

A proximidade do século XX reforçou o vínculo do conceito de segurança à ideia de paz doméstica; noutras palavras, a noção de segurança permanece voltada temporariamente ao âmbito interno, conforme nos revela Weaver:

> No período de consolidação interna dos estados nacionais – que vai das décadas que se seguiram ao Congresso de Viena até o fim da Primeira Guerra Mundial – o conceito de segurança também esteve fortemente associado à realização da "paz doméstica". (WAEVER, 2004, p. 59).

O período entre guerras (1918-1939) testemunha um novo ponto de inflexão no conceito de segurança subvencionado pelo flagelo causado pelo primeiro conflito mundial (1914-1918). As nações aliadas e vencedoras desse modificaram o discurso da segurança de forma inovadora e vislumbraram que interesses divergentes à ordem interna vigente poderiam causar consequências políticas avassaladoras ao "***establishment***" de poder local.

Pressupondo-se agora que haveria a necessidade de se distinguir os âmbitos nacional e internacional na busca da estabilização do *status quo* e a paz nesses dois cenários, de forma inovadora a segurança adquire servindo de fundamento ao entendimento de Segurança Coletiva e Segurança Nacional.

> Esta ideia de Segurança Coletiva foi gerada com base no paralelo teórico entre, de um lado, a atuação dos cidadãos dentro de seus respectivos Estados-nação e, de outro, a ação destes Estados-nação no Sistema Internacional. Propunha-se, nesse sentido, que instituições internacionais regulariam a interação entre os Estados, impediriam seus conflitos, garantiriam a paz e a estabilidade, assim como

> promoveriam tanto a cooperação quanto o bem-estar mútuo de suas partes componentes. Concebia-se, dessa maneira, uma equivalência entre as funções que o Estado realizaria junto a seus cidadãos e as funções que uma organização internacional de segurança coletiva deveria operar junto a seus Estados-membros. (CLAUDE, 1984).

Em contraposição à filosofia da Balança de Poder[13] (de caráter seletivo e excludente, com a formação de alianças entre um restrito grupo de membros), a Segurança Coletiva está dotada de estratégias inclusivas, até mesmo entre potenciais agressores, sob a égide de instituições universais (a exemplo da ONU), trazendo à arena institucional a ideia de que a ameaça a um de seus membros seja encarada como se de todos o fossem. Um exemplo clássico de política pública fundamentada na Segurança Coletiva deu-se com a proposição do presidente norte-americano Woodrow Wilson (1913-1921) preterir a ideia de Equilíbrio de Poder[14] em favor de uma "Comunidade de Poder" através dos seus 14 pontos que resultaria na criação da Liga das Nações[15].

2.4 SEGURANÇA NO MUNDO POLARIZADO

O fracasso da Liga das Nações e o início das hostilidades no teatro europeu que dariam início à Segunda Guerra Mundial abalou a credibilidade do conceito de Segurança

---

[13] Balança de Poder: vide: DINIZ, Eugenio. *Política internacional*: guia de estudo das abordagens realistas e da balança de poder. Belo Horizonte: Editora PUC-Minas, 2007.

[14] Equilíbrio de Poder: vide NYE, Joseph. *Compreender os conflitos internacionais*. Lisboa: Gradiva, 2002.

[15] A Liga das Nações foi proposta originalmente pelo "Coronel" Edward M. House (diplomata norte-americano e conselheiro do Presidente Wilson em assuntos internacionais) para os britânicos em setembro de 1915. Em maio de 1916, Wilson delineia a instituição, embora só venha incluir os Estados Unidos no projeto em janeiro de 1917. Em abril desse último ano, os Estados Unidos entram na Primeira Guerra Mundial. Os 14 Pontos são considerados a base para as negociações de paz que resultaram no Tratado de Versailles e a fonte de inspiração original da ideia de Segurança Coletiva. As proposições somente são articuladas sistematicamente pelo Presidente Wilson no dia 8 de janeiro de 1918 perante o Congresso norte-americano. Na ocasião, os Estados Unidos ainda estavam em guerra, o que justifica o conteúdo em parte geral (político-diplomático) e em parte específico (tático-estratégico) das demandas. Wilson dividiu os pontos originalmente em dois conjuntos. Os oito primeiros pontos eram as demandas de cumprimento obrigatório, ou seja, as condições que devem (*must*) necessariamente serem cumpridas para a resolução do conflito. Os seis outros pontos são negociáveis, apesar de imperativos (should). O oitavo ponto trata especificamente da criação da Liga das Nações. Os 14 Pontos são: [oito obrigatórios] (1) A diplomacia aberta ou pública [abolição da Diplomacia Secreta]; (2) A liberdade nos altos mares em tempos de guerra ou de paz; (3) O desarmamento geral começando pela redução dos arsenais até níveis compatíveis com a segurança doméstica; (4) A remoção das barreiras comerciais e o estabelecimento da igualdade nas trocas entre todas as nações; (5) A resolução imparcial das disputas coloniais, acomodando interesses dos nativos e das potencias coloniais envolvidas; (6) A restauração de Bélgica; (7) A evacuação do território russo; (8) O estabelecimento da Liga das Nações para assegurar as garantias mútuas de independência política e integridade territorial para grandes e pequenos estados; [6 negociáveis] (9) A evacuação de Restauração do território francês, incluindo a Alsácia-Lorena; (10) A autonomia para as minorias nos Impérios Austro-húngaro e Otomano; (11) O reajustamento das fronteiras italianas; (12) A evacuação dos Bálcãs; (13) A internacionalização dos Dardanelles; (14) A criação de um Polônia independente com acesso ao mar. (KISSINGER, 1994).

Coletiva e alavancou o conceito de Segurança Nacional. Isso permitiu que realistas clássicos como Edward H. Carr (1939) e Hans J. Morgenthau (1948) contestassem as pressuposições do Presidente Wilson, elencando que as relações entre Estados fundamentavam-se nas relações de poder e no interesse nacional.

A retomada dos princípios do realismo nos anos 1940 ainda esbarraria numa última tentativa dos preceitos da Segurança Coletiva, que seria materializada pela Carta do Atlântico[16] de agosto de 1941, a qual inseria dois novos elementos ao conceito tradicional de Segurança Nacional como condições necessárias à sustentação de um sistema de segurança duradouro: (1) a renúncia à força e (2) os direitos humanos (HAFTENDORN, 1990).

Ao término da Segunda Guerra Mundial, o conceito de Segurança Coletiva ainda materializado pela ONU como instituição garantidora das articulações em prol da estabilidade dos seus membros começa a ter sua eficácia questionada e a busca pela Segurança Nacional predomina sobre a coletividade, em que os discursos tornam-se baseados em preceitos realistas e começam a permear os debates acadêmicos e políticos, tornando aos olhos do ocidente a ameaça soviética, sob vários aspectos (político, ideológico, econômico e societal), cada vez mais eminente.

Na medida em que a URSS obteve domínio sobre a tecnologia de produção de artefatos nucleares e a corrida armamentista com os Estados Unidos da América se dinamizou, essa concepção mais ampla de ameaças deu lugar a um conceito de segurança cada vez mais estreito (BUZAN, 1997, p. 6, tradução nossa).

O conceito de Segurança Nacional, agora carrega um viés militarizado e altamente técnico e passa a ser predominante nos debates dos decisores norte-americanos.

> [...] dois fatores explicam esta rápida adoção no contexto norte-americano: (1) o efeito mobilizador do conceito, que serviu como ferramenta útil para superar a (até então) tradicional reticência norte-americana em manter esforços contínuos de guerra e (2) seu potencial de expressar e catalisar a então nascente rivalidade geopolítica com a URSS, justificando-a e, em certo sentido, exigindo uma maior congruência e empenho entre os setores militares e não militares da sociedade norte-americana. (WAEVER, 2004, p. 56, tradução nossa).

O novo discurso de Segurança Nacional (agora militarizado) daria fundamentação a setores de governo que viabilizassem uma ordem de políticas públicas extraordinárias para contraposição ao antagonista externo e às tentativas de infiltração do "inimigo" ideológico na

[16] A Carta do Atlântico foi o documento base que fundamentou os princípios que viriam a nortear a reestruturação da ordem internacional ao longo da segunda metade do século XX, ao servir de base para a Carta das Nações Unidas em 1942.

comunidade política dos EUA. Dessa forma:

> A Segurança Nacional foi uma ideia, uma doutrina e uma instituição delineada para conectar a tradicional divisão entre os interesses do Estado no exterior e seus interesses domésticos, assim como para fundir a cultura da vida cotidiana à da Defesa do interesse nacional. [...] Esta mutação da [ideia de] Defesa para a de Segurança foi exigida para [que se pudesse] escapar aos limites materiais e territoriais impostos pelo legado semântico da [noção de] Defesa, com seu foco estritamente militar [voltado para a proteção contra ameaças de caráter exclusivamente externo], [um sentido] que se mostrou inadequado para o escopo [cada vez mais] abrangente requerido neste [novo] momento. (MCSWEENEY, 1999, p. 20, tradução nossa).

As mutações conceituais no período da Guerra Fria consolidam a inversão semântica iniciada ao fim das Guerras Napoleônicas. Assim, se no início dos anos 1800 o indivíduo compartilha a prerrogativa de segurança com o Estado (coletividade política), a segunda metade dos anos 1900 marca o momento que a segurança do indivíduo, agora, está plenamente sujeita (subordinada) à Segurança Nacional. Em similaridade ao período pós-Napoleônico, as variações da concepção de segurança no Estado (Segurança Nacional) transformariam as concepções de segurança na arena mundial (relações interestatais), realizando a incorporação gradual do conceito de Segurança Internacional[17], à medida que a Guerra Fria evoluiu da sua fase inicial marcada pela promoção de políticas de segurança nacional para momentos críticos como a Crise dos Mísseis em Cuba, no ano de 1962, havia servido de alerta para o risco iminente de enfrentamento massivo entre as duas superpotências nucleares, que confiavam suas seguranças a um sistema de ***dissuasão*** passível de falhas e de mal-entendidos [*misperceptions*] potencialmente catastróficos (JERVIS, 1978, grifo nosso).

Ademais, o episódio operou como catalisador para transformações na forma de perceber as reações internacionais: demonstrou-se a possibilidade e a necessidade de se superar ao menos parcialmente o Dilema de Segurança (HERZ, 1950) – segundo o qual incrementos na segurança de um determinado Estado implicam necessariamente em decréscimos de igual proporção na segurança dos demais atores internacionais –, pensando agora na possibilidade de cooperar mesmo em um ambiente de autoajuda regido por essa lógica de soma-zero (JERVIS, 1978; AXELROD; KEOHANE, 1985).

[17] "[...] O conceito de Segurança Internacional é baseado em um mútuo interesse em sobrevivência sobre condições de dissuasão nuclear e no reconhecimento de que um adversário vai ser dissuadido a não atacar por causa de seus próprios autointeresses. [Dessa forma] a Segurança Internacional, em contraste com a segurança nacional, implica que a segurança de um Estado está profundamente ligada àquela de outros Estados, mesmo que apenas um único outro qualquer. Os Estados são interdependentes em temas de segurança de tal modo que a segurança de um é fortemente afetada pelas ações do outro, e vice-versa" (HAFTENDORN, 1990, p. 9, grifo do autor, tradução nossa).

Os anos 1970 apontavam para uma melhora nas Relações Internacionais (*détente*), abrindo espaço para uma ideia de controle sobre a dinâmica de escalada do conflito entre as superpotências para proteger o sistema internacional contra a possibilidade de um confronto nuclear, pois a busca irrestrita pela segurança nacional, tanto por parte dos EUA quanto da URSS, traria consequências nefastas ao conjunto mais amplo de atores internacionais.

Com isso, amplia-se o escopo da segurança, que não mais se referia somente aos atores internacionais separadamente enquanto unidades, mas também ao Sistema Internacional de Estados. Nesse sentido, a ideia de Segurança Internacional surge como uma reação às consequências não previstas das políticas de Segurança Nacional de Estados Unidos e URSS: paradoxalmente, a busca desenfreada pela segurança, ao invés de aliada, tornara-se uma ameaça à paz internacional (WAEVER, 2004).

> Com o reconhecimento de que mesmo uma estratégia de segurança nacional modificada não poderia evitar um holocausto nuclear, a ênfase [do conceito] mudou de um paradigma de Segurança Internacional ao invés de [segurança] nacional. [...] O conceito de Segurança Internacional é baseado em um mútuo interesse em sobrevivência sobre condições de dissuasão nuclear e no reconhecimento de que um adversário vai ser dissuadido a não atacar por causa de seus próprios interesses. [Dessa forma] a Segurança Internacional, em contraste com a segurança nacional, implica que a segurança de um Estado está profundamente ligada àquela de outros Estados, mesmo que apenas um único outro qualquer. Os Estados são interdependentes em temas de segurança de tal modo que a segurança de um é fortemente afetada pelas ações do outro, e vice-versa (HAFTENDORN, 1990, p. 9, tradução nossa).

À medida que o conceito de Segurança Internacional evoluía não representou de imediato, o abandono do conceito de Segurança Nacional, contrariando os argumentos, as agendas políticas associadas a ambos encontrariam pontos associativos visto que a Segurança Internacional tornava-se elemento crucial (a base) para manutenção do segundo. De acordo com Weaver a afinidade dos dois conceitos remete ao momento cronológico entre guerras com a representatividade da Liga das Nações num cenário Histórico comparativo com o contexto da Guerra Fria e a ação institucional da ONU.

> A Segurança Internacional não nega à Segurança Nacional; ao invés disso ela contém em si própria a suposição que a verdadeira Segurança Nacional só pode ser concretizada enquanto uma manifestação particular da Segurança Internacional, ao mesmo tempo em que se crê que a Segurança Internacional não visa garantir a segurança de algo de natureza internacional, mas a prover Segurança Nacional de um modo saudável para cada Estado que compõem o Sistema Internacional" (WAEVER, 2004, p. 59, tradução nossa).

O movimento articulado no âmbito internacional torna-se crucial para a segurança

individual dos Estados e essa articulação assume características muito próximas à ideia de Equilíbrio de Poder. Contudo, o Estado mantém sua referência como objeto-alvo do conceito de segurança, embora perseguindo, por meios distintos, a adoção de práticas coletivas relegadas ao passado. O Estado permanece como o núcleo ao qual deveria ser garantida sua existência e proteção.

2.5 O PROBLEMA DE ESTUDO

Um ponto de contestação na comunidade acadêmica dá-se pela carência da "problematização" do conceito de segurança. Além disso, as correntes tradicionalistas (neorrealismo) persistiam como a linha de pensamento dominante, principalmente no período da Guerra Fria.

As primeiras críticas à visão convencional do conceito de segurança e de suas teorias tradicionalistas dos Estudos de Segurança Internacional manifestam-se no campo acadêmico, de forma tímida, na primeira metade dos anos 1980. O insucesso das forças norte-americanas na Guerra do Vietnã[18] (1959-1975) havia promovido um questionamento sobre a eficiência de ações militares para a resolução de problemas na ordem política e econômica.

Ainda nesse período (1980), havia o entendimento crescente de que um conflito convencional tornara-se um recurso dirimido na centralidade das questões estratégico-

[18] A Guerra do Vietnã foi um conflito armado que começou no ano de 1959 e terminou em 1975. As batalhas ocorreram nos territórios do Vietnã do Norte, Vietnã do Sul, Laos e Camboja. Essa guerra pode ser enquadrada no contexto histórico da Guerra Fria. A relação entre os dois Vietnãs, em função das divergências políticas e ideológicas, era tensa no final da década de 1950. Em 1959, vietcongues (guerrilheiros comunistas), com apoio de Ho Chi Minh e dos soviéticos, atacaram uma base norte-americana no Vietnã do Sul. Esse fato deu início à guerra. Entre 1959 e 1964, o conflito restringiu-se apenas ao Vietnã do Norte e do Sul, embora Estados Unidos e também a União Soviética prestassem apoio indireto. Em 1964, os Estados Unidos resolveram entrar diretamente no conflito, enviando soldados e armamentos de guerra. Os soldados norte-americanos sofreram num território marcado por florestas tropicais fechadas e grande quantidade de chuvas. Os vietcongues utilizaram táticas de guerrilha, enquanto os norte-americanos empenharam-se no uso de armamentos modernos, helicópteros e outros recursos. No final da década de 1960, era claro o fracasso da intervenção norte-americana. Mesmo com tecnologia avançada, não conseguiam vencer a experiência dos vietcongues. Para piorar a situação dos Estados Unidos, em 1968, o exército norte-vietnamita invadiu o Vietnã do Sul, tomando a embaixada dos Estados Unidos em Saigon. O Vietnã do Sul e os Estados Unidos responderam com toda força. É o momento mais sangrento da guerra. No começo da década de 1970, os protestos contra a guerra aconteciam em grande quantidade nos Estados Unidos. Jovens, grupos pacifistas e a população em geral iam para as ruas pedir a saída dos Estados Unidos do conflito e o retorno imediato das tropas. Neste momento, já eram milhares os soldados norte-americanos mortos no conflito. A televisão mostrava as cenas violentas e cruéis da guerra. Sem apoio popular e com derrotas seguidas, o governo norte-americano aceitou o Acordo de Paris, que previa o cessar-fogo, em 1973. Em 1975, ocorre a retirada total das tropas norte-americanas. É a vitória do Vietnã do Norte. O conflito deixou mais de 1 milhão de mortos (civis e militares) e o dobro de mutilados e feridos. A guerra arrasou campos agrícolas, destruiu casas e provocou prejuízos econômicos gravíssimos no Vietnã. O Vietnã foi reunificado em 2 de julho de 1976 sob o regime comunista, aliado da União Soviética. Vide: VIZENTINI, Paulo Fagundes. *Guerra do Vietnã*. 3. ed. Porto Alegre: Editora: UFRGS, 2006.

militares, fundamentado em três fatores significativos, quais sejam: (1) o relativo sucesso das estratégias de dissuasão nuclear em estabilizar as relações entre o Leste e o Oeste; (2) as políticas de desmilitarização promovidas por Gorbatchev[19]; e (3) a conformação de uma incipiente comunidade de segurança entre os Estados Unidos da América, o Japão e a Europa. Esses três fatores permitiram tanto a acadêmicos quanto a tomadores de decisão a pensar que a URSS poderia participar dessa esfera de paz entre os principais centros geoeconômicos do mundo (BUZAN, 1998, p. 6, tradução nossa).

Ao passo que a suscetibilidade de um conflito bélico entre atores do sistema internacional era colocada em dúvida, as questões de ordem militar sustentadas pelo paradigma tradicionalista foram renegadas da centralidade dos debates e obrigadas a dividir espaço com uma nova ordem de analistas que, desde a segunda metade dos anos 1970, propunham uma agenda mais abrangente com temas vinculados ao cenário econômico mundial, ambientalistas e que influenciavam significativamente a dinâmica da segurança nacional de um determinado ator, ou até mesmo a estabilidade regional.

A identificação de novas ameaças emerge no foco dos debates sobre segurança agindo através de um movimento conhecido como: ampliação da agenda de Estudos de Segurança Internacional.

Neste momento, encerra-se o estudo sobre epistemologia de segurança e sua evolução ao longo de um intervalo temporal transcorrido da Antiguidade até a segunda metade dos anos 1900 com a ascensão do período dominado pela bipolaridade ideológica entre as superpotências do Ocidente e do Oriente. Nesse desfecho, auxiliado pela literatura, identificam-se os dois movimentos que permitiram uma ampla problematização do conceito de segurança a partir da pluralização das fontes de ameaça (ULLMAN, 1983; MATTHEWS,

[19] Mikhail Gorbachev nasceu em 2 de março de 1931, na aldeia de Privolnoye, Krasnogvardeisky District, Stavropol Território, no sul da república russa, numa família de camponeses russo-ucranianos que se mudou para o Território Stavropol a partir de Voronezh Região Russa e da Chernigov, província da Ucrânia. Em março de 1985, Gorbachev foi eleito secretário-geral do Comitê Central do PCUS. Gorbachev iniciou o processo de mudança na União Soviética – o que mais tarde foi chamado perestroika (1985-1991). A Glasnost e abertura tornaram-se a força motriz da perestroika. Um programa de reformas foi planejado para colocar a economia do país no caminho certo para uma economia de mercado socialmente orientada Essa política pôs fim ao regime totalitário da URSS: em 1990, o poder do Estado na URSS mudou do partido comunista para o Congresso dos Deputados do Povo da URSS – o primeiro parlamento em história soviética, formado com base em eleições livres, democráticas e contestáveis. O Congresso dos Deputados do Povo elegeu Gorbachev Presidente da URSS em 15 de março de 1990. Uma grande mudança nos assuntos internacionais foi efetuada. Gorbachev lançou uma política ativa de amenização das relações (détente) com base num novo pensamento associado ao seu nome e se tornou uma figura-chave na política mundial. O período de 1985-1991 foi o momento de uma mudança fundamental nas relações da URSS com o Ocidente – transformando a imagem de um inimigo, um "império do mal", para a imagem de um parceiro. Gorbachev desempenhou um papel proeminente no fim da Guerra Fria, parando a corrida armamentista e unificando a Alemanha. Disponível em: <http://www.gorby.ru/en/gorbachev/biography/>. Acesso em: 10 abr. 2016.

1989) e na expansão dos objetos de referências para os cinco setores (BUZAN, 1983) e debruçamos nossos esforços sobre a ampliação da agenda de segurança nas Relações Internacionais, em particular nas ideias da Escola de Copenhagen, sobretudo no desenvolvimento da Teoria da Securitização de Ole Weaver (1989).

2.6 O CAMINHO PARA CONPENHAGEN

Neste momento da pesquisa, dá-se enfoque aos conhecimentos e debates promovidos pelo grupo acadêmico que buscou na segunda metade dos anos 1980 a ampliação da agenda de segurança, dessa forma concentrado no debate deve-se, antes de tudo, analisar o conjunto de produções da linha acadêmica tradicionalista do estudo de Segurança Internacional (em referência as teorias que emergem após a Segunda Guerra Mundial) considerada a "Idade Dourada" (a Golden Age de WALT, 1991) dada a incontestável preponderância de que dispunham sobre as demais alternativas teóricas.

2.6.1 Abordagens tradicionais

Um dos mais representativos exemplos do pensamento sobre Segurança Internacional advém do Dilema de Segurança formulado por John Herz, o qual, em um ambiente anárquico onde não havendo autoridade superior que possa regular os conflitos entre seus constituintes em contínua interação, as partes contam somente com si mesmas para garantir sua segurança: trata-se de um ambiente de autoajuda onde se opera um jogo de soma-zero no qual o poder adquirido por um Estado "A" implica o declínio da segurança de um Estado "B", e assim sucessivamente. Isso implica na dificuldade de cooperação interestatal no campo da segurança num ambiente internacional anárquico.

A deflagração da Segunda Guerra Mundial trouxe à tona esse pensamento ortodoxo, e nomes como Hans Morgenthau (1948) e Kenneth Waltz (1979) foram agentes que contribuíram para a nova leva de conservadorismo teórico na qual o direcionamento dá-se pela questão: como garantir a constante autonomia do Estado em um ambiente de insegurança? Invoca-se, assim, a narrativa realista – em sua versão clássica ou em sua leitura estrutural neorrealista, em que o objetivo primeiro, último e único dos Estados é maximizar seu poder (MORGENTHAU, 1948) e/ou sua segurança (WALTZ, 1979), com vistas a garantir sua sobrevivência em um sistema internacional anárquico e, consequentemente, ameaçador

(HERZ, 1950).

As décadas de 1970 e 1980 observavam a prevalência do neorrealismo, atribuindo à balança de poder o status de garantidor da Segurança Internacional, da ordem entre os Estados, da própria estabilidade sistêmica e, consequentemente, da paz.

Waltz defende que, se há uma teoria das Relações Internacionais, essa seria a da balança do poder[20] (WALTZ, 1979, p. 118), e, em clara ruptura com os realistas clássicos, entende o poder não como um fim em si mesmo, mas como um instrumento utilizado pelos Estados para assegurar sua posição no sistema. No entendimento de Morgenthau, o objetivo dos Estados é maximização do poder (pois apenas o poder limita o poder). Em Waltz, a meta definitiva das unidades no sistema internacional é a maximização de sua própria segurança, independente se esta será alcançada reforçando-se o equilíbrio de poder ou abalando-o. Em suma, a busca dos Estados pela segurança é a determinante da estabilidade e a paz.

A visão ortodoxa de segurança pela corrente realista permanece imune a críticas mesmo com o fim da Guerra Fria, John Mearsheimer (1990) revela em seus escritos uma crescente preocupação com a fragmentação do poder com o surgimento de um novo grupo de atores no contexto internacional e o sensível decréscimo da influência norte-americana sem seu tradicional algoz ideológico e sendo considerado como um herdeiro teórico de Waltz, Mearsheimer aponta para três fatores que contribuíram para a estabilidade no teatro europeu após a Segunda Guerra Mundial, a saber: (1) a bipolaridade, (2) um balanço militar igualitário e (3) a existência de armas nucleares. Resumindo, a principal responsável pela manutenção da paz na região foi a eficiente e robusta dissuasão (*detérrence*) viabilizada pela dinâmica de poder própria da Guerra Fria.

A visão de Mearsheimer, inspirada pelo realismo estrutural e permeada por uma preocupação primeira com a sobrevivência estatal, identifica as causas da guerra na distribuição e no caráter do poder militar. Trata-se de uma teoria que busca na estrutura do sistema internacional, e não na natureza individual dos Estados, a explicação para a guerra e violência internacional. A racionalidade, quase cartesiana, dos atores perpassa a análise e explicita-se na referência do autor aos cálculos de custos, riscos e benefícios (como se houvesse a possibilidade de se definir uma métrica) que tanto dissuadem os Estados quanto favorecem a sua agressividade. A igualdade de poder é apontada como fator explicativo para a paz; a desigualdade de poder abre uma premissa para a incitação de conflitos armados, visto o

[20] Para o autor, o equilíbrio de poder é o resultado inerente e inescapável de um sistema internacional anárquico e marcado pela lógica de autoajuda. Ele deriva da distribuição das capacidades materiais e não da ação voluntária de estadistas, como pretendia Morgenthau (entendimento nosso).

aumento probabilístico de sucesso de uma agressão.

A visão neorrealista de Waltz e Mearsheimer dá-se resumidamente pelo entendimento do modelo de Balança de Poder como mantenedor da Segurança Internacional e da estabilidade sistêmica lançando mão do uso efetivo do poderio militar ou do potencial uso do mesmo (dissuasão).

Essa visão de Segurança Internacional não engloba elementos como a ideologia (motivadora de ações de cunho terrorista) ou a economia (operações de restrição da produção de petróleo coordenadas pela OPEP[21], que ainda nos anos 1970 abalariam o sistema econômico mundial), tidos como secundários e derivados da distribuição do poder militar. A Segurança Internacional é intimamente relacionada à segurança estatal: a sobrevivência do Estado é a meta última. Nesse sentido, os autores apontam como em Morgenthau, para a percepção de uma estabilidade dinâmica, permeada por um profundo pessimismo frente a transformações sistêmicas potencialmente ameaçadoras.

Podemos resumir a agenda tradicional desta forma:

Os Estudos de Segurança se dedicam basicamente à segurança do Estado, medida em termos de seu poder material disponível para lidar com ameaças de cunho essencialmente militar em um sistema internacional anárquico (WALT, 1991).

Ou ainda: "Em sua Idade Dourada, a segurança é uma condição do Estado, a ser alcançada pelo Estado, através de instrumentos do poder militar do Estado". (MCSWEENEY, 1999, p. 36, tradução nossa).

2.6.2 A agenda ampliadora

Conforme apontado na sessão anterior, identificamos na primeira metade dos anos 1980 a primazia das teorias tradicionalistas no contexto das Relações Internacionais, contudo percebe-se uma inquietação no meio acadêmico com relação à "problematização" do conceito de Segurança Internacional e identificamos o início, ainda que incipiente, de um debate sobre os conceitos vigentes.

[21] Organização dos Países Exportadores de Petróleo (OPEP) é uma organização intergovernamental permanente, criada na Conferência de Bagdá (10-14 setembro de 1960), por parte do Irã, Iraque, Kuwait, Arábia Saudita e Venezuela. Os cinco membros fundadores se juntaram posteriormente a outros nove membros: Qatar (1961); Indonésia (1962) – suspensa de janeiro de 2009 a dezembro de 2015; Líbia (1962); Emirados Árabes Unidos (1967); Argélia (1969); Nigéria (1971); Equador (1973) – suspenso de dezembro de 1992 a outubro de 2007; Angola (2007); e Gabão (1975) – afastado em janeiro de 1995 e reativado em julho de 2016. A OPEP tinha a sua sede em Genebra, Suíça, nos primeiros cinco anos de sua existência, sendo transferida para Viena, Áustria, em 01 de setembro de 1965. Disponível em: <http://www.opec.org/opec_web/en/about_us/24.htm>. Acesso em: 15 de maio de 2016

Diante de uma série de eventos transcorridos ao longo do período da Guerra Fria (exemplo: derrota dos EUA no Vietnã), cada vez mais se dissemina a percepção de que as perspectivas realistas clássicas tornam-se insuficientes, e começa a ganhar terreno uma abordagem mais ampla na agenda de segurança que englobasse outros setores e domínios além da esfera militar.

O ano de 1983 tornar-se-ia um marco com a publicação, na Revista *International Security*[22], do artigo de Richard Ullman, apresentando a defesa de uma redefinição do conceito de Segurança Internacional e defendendo uma ampliação da agenda sobre o tema. Nesse artigo, Ullman faz críticas a respeito do demérito quanto a diversas fontes de ameaças e equivoco da militarização no tratamento das questões de segurança nacional abrindo espaço para "[...] imagem profundamente falsa da realidade" (ULLMAN, 1983, p. 129), fazendo assim apontamentos para ameaças não militares.

Richard Ullman define segurança da seguinte forma:

> Uma ação ou sequência de eventos que (1) ameace drasticamente e em um relativo curto espaço de tempo à qualidade de vida dos habitantes de um Estado, ou (2) ameace significativamente estreitar a gama de escolhas política disponíveis a um estado ou a entidades privadas não governamentais (pessoas, grupos, corporações) dentro do Estado. (1983, p. 133).

Ao apresentar essa nova definição, Ullman abriu um precedente para inclusão de novas "*dimensões*", em que questões de ordem ambiental, energia (controle de recursos) e até mesmo catástrofes naturais[23] orbitavam como elementos de análise na agenda de segurança com aspectos tão relevantes quanto os de ordem militar.

Ainda em 1983, Barry Buzan apresenta uma contribuição no movimento de ampliação da agenda de estudo de segurança ao enumerar cinco setores (militar, político, econômico, societal e ambiental) que deveriam ser estudados como potenciais fontes de ameaça. Em detrimento desses setores, a segurança se debruçaria especificamente sobre cada um deles: segurança militar, segurança econômica, segurança política, segurança societal e segurança ambiental.

---

[22] A publicação no periódico *International Security* é bastante significativa, dado o viés claramente tradicionalista do periódico. "O artigo de Ullman não é particularmente radical. Em muitos sentidos, ele é importante tanto por onde e quando ele aparece quanto pelos detalhes aos quais ele realmente mencionava. [...] Talvez a significância do artigo esteja [relacionado ao fato de] ele ter sido publicado na International Security, o principal [flagship] periódico dos estudos realistas de segurança, [...] gerando a exigência de se refletir sobre premissas anteriormente implícitas, [um movimento] que foi tão saudável quanto longamente adiado". (SHEEHAN, 2005, p. 45).

[23] Grandes catástrofes naturais devem ser inseridas nas agendas de segurança nacional, pois geram grandes danos e simplesmente "não podem ser dissuadidas" (ULLMAN, 1983, p. 138).

Dessa ampliação, deriva a distinção operada por Buzan entre os Estudos de Segurança Internacional, que englobam os cinco setores dos Estudos Estratégicos que se dedicam unicamente ao setor militar (BUZAN, 1991, p.23-25). Contrariando WALT (1991), que considera as ameaças desses outros setores como meros "problemas", Buzan as eleva ao *status* de questões de "segurança", considerando-as como perigos significativos à sobrevivência do Estado.

Ainda que a ampliação dos setores de estudo tenha relevância na agenda, para Buzan a ampliação dos "objetos de referência" da segurança é ainda mais relevante. Segundo o autor, não somente o Estado deveria ter sua segurança garantida, mas também o Sistema Internacional, e os indivíduos, conforme declara:

> Enquanto um conceito, a segurança claramente requer um objeto de referência, pois sem uma resposta para a questão "A segurança de que?" a ideia não faz sentido. Responder simplesmente "o Estado" não resolve o problema [...]. Rapidamente se descobre que a segurança tem muitos objetos de referência possíveis. Estes objetos da segurança multiplicam-se não só conforme aumenta o número de membros na Sociedade de Estados, mas também na medida em que olhamos "para abaixo e através" dos Estados para o nível individual, assim como "para cima e além" [dos mesmos Estados] para o nível do sistema internacional como um todo. (BUZAN, 1991, p. 26).

O caráter inovador do argumento de Buzan, quando comparado ao de Ullman, dá-se pela ampliação não só dos tipos de ameaças, mas insere objetos de referência no campo da análise, contudo, ainda que inovador o argumento de Buzan, tem-se o Estado como o mais relevante objeto de referência mesmo sem alcançar a exclusividade. A teoria ampliadora aponta que o Estado compartilha com indivíduos e o sistema internacional a prerrogativa de ser um objeto de segurança. Os fundamentos teóricos para a ampliação e o revisionismo da agenda de segurança foram alicerceados por Buzan e Ullman, em que a não hierarquização das questões de segurança elimina a separação entre *high politics* (de cunho militar) e *low politics* (focada sobre outras questões). Com isso, abre-se o caminho para a contribuição da Escola de Copenhagen para os Estudos de Segurança Internacional.

2.6.3 A Escola de Copenhagen

Em 1996, Bill McSweeney, um dos principais críticos da vertente à agenda ampliadora, criou a expressão "Escola de Copenhagen". O autor se referia a um grupo de pesquisadores europeus, liderados por Barry Buzan e Ole Waever, que, desde 1988, desenvolvem pesquisas sobre o campo da segurança no âmbito do *Copenhagen Peace and*

Research Institute (COPRI)[24], sediado na capital da Dinamarca.

Em 1998, com a publicação de "*Security: a New Framework for Analyses*", Buzan, Waever e Wilde condensam em um mesmo volume os principais conceitos e proposições da Escola de Copenhagen com o propósito de reestruturar o campo dos Estudos de Segurança Internacional. Essa obra e o posterior *Regions and Powers* (BUZAN; WAEVER, 2003) podem ser considerados os textos mais representativos da perspectiva desses teóricos.

Numa análise sucinta, resumimos as principais ideias que informam a análise de segurança proposta pela Escola de Copenhagen em três pontos: (1) os setores, (2) os complexos regionais de segurança e (3) a teoria da securitização.

> A originalidade da Escola de Copenhague reside precisamente em (1) servir de espaço para fazer convergir em um arcabouço coletivo, teorias que haviam sido desenvolvidas originalmente de forma individual pelos diferentes pesquisadores associados ao grupo e (2) articular o "desenvolvimento criativo" destes novos conceitos com os contextos empírico e teórico europeu (TANNO, 2003; HUYSMANS, 1998).

O grupo de estudiosos analisa os mecanismos de produção do conjunto de domínios que compõem o quadro de ameaças e suas consequências políticas na articulação de discursos de segurança, adotando uma perspectiva de análise independente de comprometimentos normativos rígidos.

Desse o arcabouço construtivista desenvolvido pela Escola de Copenhagen parece adequado à análise de como a segurança cibernética foi inserida na agenda do Estado Brasileiro, condizendo com objetivo de entender as dinâmicas discursivas e institucionais de inserção da matéria na Estratégia Nacional de Defesa e suas repercussões nas forças armadas brasileiras, em especial na Marinha do Brasil.

2.6.4 A teoria da securitização

Ole Waever retoma em 1995 de forma mais abrangente e aprofundada seu trabalho de 1989 no qual defende que a segurança caracteriza-se como uma "problemática específica" e seu entendimento dá-se pela análise do campo da segurança e pelas operações que lhe são típicas, tornando-se difícil aos olhos do autor "identificar um campo específico de interação social, com um conjunto específico de ações [...]" (WAEVER, 1995).

[24] O COPRI é derivado do Centre for Peace and Conflict Research, criado três anos antes, em 1985. Ole Wæver participa do projeto desde este inicio, enquanto Buzan somente adere só ao grupo em 1988, quando se tornou diretor do projeto Non-military aspects of European Security (HUYSMANS, 1998).

A discussão é articulada de forma mais evidente em sua obra conjunta com Barry Buzan *Security*: a new framework for analysis, na qual os autores propõem uma visão extremada dos estudos de segurança, sintetizando elementos que combinem perspectivas tradicionalistas e ampliadoras, operacionalizando através da análise e exploração de ameaças a objetos de referência, tendo como consequência a securitização destas ameaças. Essas medidas securitizadoras podem ser de caráter militar ou não.

Esse posicionamento deflagrou a ruptura com as abordagens até então desenvolvidas, trazendo a contribuição da teoria socioconstrutivista e o entendimento do processo de construção de ameaças para o estudo de segurança, além de ter se revelado a tentativa de resolução para indefinição do conceito de segurança gerado pela ampliação da agenda em resposta direta às críticas (WALT, 1991) aos ampliadores.

Com essa visão, os teóricos da Escola de Copenhagen definem o fenômeno de segurança como sinonímia ao termo securitização, nas palavras de Buzan: "[...] o movimento que leva a política além das regras do jogo estabelecidas e enquadra a questão como um tipo especial de política ou como [algo] acima da política" (BUZAN et al., 1998, p. 119).

> As questões securitizadas são apresentadas como ameaças existenciais, requerendo medidas de emergência e justificando ações que fogem das restrições normais do procedimento político (Ibidem, p. 24).

Em outros termos, a retórica de segurança toma para si dois argumentos implícitos: (1) um de que sem a segurança contra uma determinada ameaça estaríamos em uma situação indesejável e (2) de que temos a necessidade de pagar um preço específico para combater eficientemente esta mesma ameaça. E, quando elencadas no cenário político da segurança, tais questões tomam ordem de sobrevivência do Estado e, dessa forma, são tratadas com mais importância que as demais, consequentemente tomando para si prioridade absoluta. Porém, o discurso de um potencial ator securitizante por si só não basta para criar uma "questão de segurança": um tema somente será definitivamente securitizado se a audiência (ou plateia) a qual este ator se dirige e a qual ele requisita as prerrogativas excepcionais para lidar com a ameaça aceita voluntariamente o pedido.

"O agente securitizador precisa de permissão dos demais sujeitos de sua comunidade política para transgredir legitimamente as regras do jogo político ordinário". (KELSTRUP, 2004, p. 113).

Dessa forma, o ato securitizador não é definido pelo agente, mas pela audiência que acolhe a sugestão do ato de securitização.

Securitização é, antes de tudo, uma construção de discurso: o ato de dizer "segurança" é capaz de invocar um sentimento de emergência e constituir identidades até então inexistentes, entre elas os antagonistas: inimigo e protetor. Nesse sentido, a segurança não se refere a algo "real"; ela não é palpável e se constitui a partir de seu próprio proferimento, sendo o ato em si.

Uma definição sistemática do conceito de securitização é oferecida por Buzan e Waever:

> O processo discursivo através do qual uma compreensão intersubjetiva é construída dentro de uma comunidade política para tratar algo como uma ameaça existencial a um objeto de referência e possibilitar a requisição de medidas emergenciais e excepcionais para lidar com a ameaça. (2003, p. 491).

A escola de pensamento construtivista das Relações Internacionais, que, em sua proposta de ampliação da agenda dos estudos de segurança nos traz uma ferramenta muito oportuna no que diz respeito à questão de segurança cibernética.

O modelo proposto por Buzan e Weaver acomoda todos os elementos necessários para realização da análise, onde temos por objeto o espaço cibernético, uma miríade de ameaças, agentes securitizadores e uma plateia convalidadora dos argumentos necessários à securitização do supracitado objeto.

Na era da informação, o espaço cibernético, originariamente um bem comum, assume importância significativa para o estudo do conceito de segurança, pois através dele novos tipos de conflitos são deflagrados e a arena internacional nele se manifesta não só com a presença do Estado, mas também com uma significativa ordem de atores, revelando a assimetria das forças presentes no que se questiona como um novo domínio.

3 UM NOVO DOMÍNIO

O presente capítulo inicia-se com a busca das definições do objeto de securitização da pesquisa: o espaço cibernético.

A contextualização mais apropriada ao nosso esforço exploratório procura afastar neologismos e tecnicismos (ainda que presentes para melhor compreensão do objeto) e faz uso de um enfoque geopolítico, contribuindo com o entendimento de conceitos tecnológicos numa nova arena onde atores de ordem diversa atuam no embate pelo poder.

> A Internet alterou os parâmetros de ação humana. O próprio conceito de realidade foi expandido pelo espaço digital. A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, a terra, ao ar e ao espaço. Aberto à ação humana, o domínio cibernético abre-se também ao conflito. (AMORIM, 2012).

3.1 INFORMAÇÃO, O PRINCÍPIO DE TUDO

A informação – e a garantia de seu sigilo – foi considerada, pelo Cardeal Richilieu, ainda em 1641, o objeto mais importante de um Estado (DEIBERT, 2012). Na verdade, a informação é o objeto de desejo que antecede à organização sociopolítica, acompanhando a trajetória humana desde a ocupação de seu espaço geográfico natural à apropriação de recursos.

Esse mesmo objeto foi produzido, processado, transmitido e recebido por muitos meios ao longo de nossa existência: do manifesto rudimentar sob a forma de mímica aos rabiscos e gravuras rupestres; dos escritos de Hamurabi aos sons de tambores e instrumentos sonoros e sua utilização nos campos de batalhas da Antiguidade.

Sinais de fumaça, clarins, mensageiros e arautos, cartas, telegramas, telex, telefone, rádio e displays digitais são alguns dos veículos registrados na história responsáveis por transportar mensagens, isto é, veículos transmissores da informação, de signos e de seus derivados significados.

Chegamos à Era da Informação ou do Conhecimento, que contém, em seu cerne, a informação em si, na qual Estados, organizações e indivíduos estão conectados, interdependentemente e na forma “on-line”. A informação, agora, é transmitida na velocidade da luz, por meio de signos digitalizados por processadores cada vez mais versáteis e menores, porém de amplo alcance, e em maior abrangência.

> Para conhecer, conceber ou divulgar uma “vontade” e também para avaliar a

> "capacidade" operacional, o poder demanda informação. Por isso também se afirma que informação é poder, ou mais que isso, é fator multiplicador e também medida de avaliação do poder. (DIZARD, 1982).

Nossa convivência, sobretudo a partir deste século, com noticiários, agendas e discursos políticos acerca de um "novo" termo que, embora não trate de um objeto de tão novo emprego, vem recebendo uma atenção muito especial. Talvez isso se justifique, além de sua relação com a informação, pela capilaridade e transversalidade que possui, envolvendo não só assuntos relativos à segurança interna dos Estados e à de suas estruturas estratégicas ou infraestruturas críticas, como também à política externa. Tratamos, pois, da cibernética, termo originário ainda na Antiguidade Clássica, relacionado à arte de pilotar uma embarcação, ou, segundo Platão, à arte de governar (MOREIRA, 1980).

3.2 O ESPAÇO CIBERNÉTICO

O Estado constatou que o exercício de poder sobre determinado espaço continua sendo um pressuposto à manutenção e sobrevivência do modelo atual no sistema internacional. Essa é uma das características mais marcantes do vigente modelo e que o difere dos Estados tradicionais (GIDDENS, 2001, p. 75-78), tendo por seus elementos intrínsecos espaço e poder, com base em um processo de construção política que teve na Paz de Westphalia[25] um marco simbólico resultante de inúmeras reconstruções ao longo da história.

A soberania estatal é legitimada e legalizada perante o reconhecimento das bases territoriais, e dos direitos sobre essas, pelos integrantes do sistema; logo, à medida que o espaço, em sua multidimensionalidade, torna-se objeto passível de utilização pelo homem, como fonte de recurso, por meio de inovações tecnológicas, a prática desse poder e seu domínio sobre esse espaço torna-se crucial. Se, inicialmente, surgem os conflitos, deliberando, às vezes, o mais elevado nível da violência, em seguida, pelo fio condutor

[25] Paz da Westphalia: encerrava a Guerra dos Trinta Anos. No dia 24 de outubro de 1648, o imperador Ferdinando 3º assinou a Paz da Westphalia com a Suécia e a França. O documento marcou o fim do primeiro grande conflito europeu. A conferência foi encerrada com três tratados independentes e o anúncio do armistício, que levou o nome da região da Westphalia. Seus resultados mais importantes: suíços e holandeses tornaram-se autônomos; o poder do imperador da dinastia Habsburg foi reduzido, em favor do dos príncipes e dos membros do Reich; o império manteve sua constituição federalista; e católicos e protestantes passaram a ser considerados fiéis com os mesmos direitos. A Alemanha saiu arrasada da guerra, com a população reduzida de 16 milhões para 8 milhões. No império constituído por 300 territórios soberanos, não sobrou nenhum sentimento nacional comum. A França foi a grande vitoriosa: anexou a Alsácia e consolidou o caminho para sua expansão. Por sua vez, a Espanha prosseguiu em luta contra os franceses até que, derrotada pela aliança franco-inglesa, aceitou a Paz dos Pirineus, em 1659, o que confirmou o declínio de sua supremacia. (Disponível em: <http://www.dw.com/pt-br/1648-paz-da-vestf%C3%A1lia-encerrava-guerra-dos-trinta-anos/a-660411>. Acesso em: 1 out. 2016).

histórico, aparece o Direito, garantindo a manutenção do status quo ou a expectativa de uma solução pacífica pelo estabelecimento de um ordenamento racional, a fim de minimizar os impasses, que ainda ocorrem com as dimensões terrestre, marítima, aérea e extra-atmosférica (cósmica). (FERREIRA NETO, 2011).

Da mesma forma, embora já usada de uma forma pretérita (no tocante ao espaço extra-atmosférico), hoje possuímos uma nova concepção de espaço, ou, uma "nova" dimensão espacial, oriunda do aprimoramento tecnológico humano: o espaço cibernético, que emerge dessa maneira como objeto de discussão política, no limite extremo do uso da força visto ora como espaço em si mesmo, ora como mais um recurso do poder.

"Os conflitos nesse novo domínio são cada vez maiores, quantitativa e qualitativamente, à medida que o aparato não só estatal descobre suas novas possibilidades de uso." (MORAN, 2010, p. 138, tradução nossa). Sob esse ponto de vista, entendemos que o espaço cibernético deixou de ser um dos *global commons*, conforme denomina Barry Posen ao se referir aos "espaços internacionais de uso comum", ou aos "bens comuns globais" (POSEN, 2003, p. 7-8), pois nesse "espaço" já é exercido realmente um domínio específico, inclusive de natureza militar:

> A força militar dos EUA possui atualmente o comando dos "bens comuns" globais. Comando dos bens comuns é análogo ao comando sobre o mar, ou nas palavras de Paul Kennedy, é análogo à naval maestria. Os bens comuns, no caso do mar e do espaço (cósmico), são áreas que não pertencem a nenhum Estado. Até mesmo o acesso para grande porção do espaço aéreo global não pertence tecnicamente aos países abaixo dele, pois há poucos países que podem negar o seu espaço aéreo acima de 45.000 pés para aviões de guerra americanos. (POSEN, 2003, p. 8, tradução nossa).

Nas palavras de Ferreira Neto, ao analisar Posen, sob uma óptica neorrealista, conclui-se que um Estado que possui o domínio sobre esses espaços "pode dificultar as operações e movimentações de Estados rivais, não só bloqueando o uso, mas constrangendo os demais, de tal forma que seja necessário que o país que domina a região dê um consentimento tácito para ações na área" (FERREIRA NETO, 2013, p. 70).

Ainda reforçando a tese de Posen, incluindo nesses o espaço cibernético, afirma Alexandre Rodrigues que *global commons* são:

> espaços que não estão sob o controle direto de qualquer Estado, mas que são vitais para o acesso e ligação de quaisquer pontos do mundo. Incluem águas e o espaço aéreo internacional, o espaço exterior e o ciberespaço. [...] Implicam uma nova e, sobretudo mais alargada visão dos espaços de interesse, por forma a incluir as suas quatro dimensões, em vez das duas tradicionais. Aliás, o nosso atual grau de dependência em relação aos dois novos espaços (cibernético e espaço exterior) é

> hoje quase idêntico ao que se verifica em relação aos tradicionais (mar alto e espaço aéreo). O espaço cibernético é uma área crítica para a segurança dos Estados e para o funcionamento das economias. Amanhã, será, com grande probabilidade, também um espaço de projeção de poder. (2012, p. 5).

Ainda que formalmente o espaço cibernético seja considerado um espaço internacional, na prática, tem o seu uso e controle pelos mais aptos, o que proporciona a esses poucos a possibilidade de territorialização desse novo domínio e, a partir desse, uma redefinição dos espaços tradicionais, que se encontram expostos ao que se convencionou chamar fenômeno da globalização[26], e que, por consequência, estariam passíveis a um processo de redesenho territorial.

O entendimento da cibernética em si pode ir além da noção de espaço-território ao configurar-se como recurso de poder proporcionado por redes de comunicação e informação cada vez mais velozes, aprofundando a concepção de "território em rede". É dessa forma que o general norte-americano Robert Elder, à época diretor do *Cyberspace Operations Task Force*, refere-se: "Se você não dominar o ciberespaço, você não pode dominar os outros domínios". (CLARKE, 2010).

Por conseguinte, sob iniciativa dos Estados tecnologicamente mais desenvolvidos, o fenômeno da territorialização vem ocorrendo no espaço cibernético e, a partir desse espaço, vem projetando sua iniciativa de poder aos demais domínios. É dessa forma que os Estados acenam com uma reação, face às descobertas das inúmeras possibilidades desse novo ambiente, o que nos remete à constatação de Marcos Saquet:

> O fato é que território e rede se condicionam reciprocamente. [...] As redes de circulação e comunicação são meios na articulação interna do território e, ao mesmo tempo, são território e interligam-no a outros territórios, tornando o território 'inicial/local' um nó ou um território articulado a outros territórios, econômica,

[26] Globalização: podemos dizer que é um processo econômico e social que estabelece uma integração entre os países e as pessoas do mundo todo. Através desse processo, as pessoas, os governos e as empresas trocam ideias, realizam transações financeiras e comerciais e espalham aspectos culturais pelos quatro cantos do planeta. O conceito de Aldeia Global se encaixa nesse contexto, pois está relacionado com a criação de uma rede de conexões, que deixam as distâncias cada vez mais curtas, facilitando as relações culturais e econômicas de forma rápida e eficiente.
Muitos historiadores afirmam que esse processo teve início nos séculos XV e XVI com as Grandes Navegações e Descobertas Marítimas. Nesse contexto histórico, o homem europeu entrou em contato com povos de outros continentes, estabelecendo relações comerciais e culturais. Porém, a globalização efetivou-se no final do século XX, logo após a queda do socialismo no leste europeu e na União Soviética. O neoliberalismo, que ganhou força na década de 1970, impulsionou o processo de globalização econômica. Com os mercados internos saturados, muitas empresas multinacionais buscaram conquistar novos mercados consumidores, principalmente dos países recém-saídos do socialismo. A concorrência fez com que as empresas utilizassem cada vez mais recursos tecnológicos para baratear os preços e também para estabelecerem contatos comerciais e financeiros de forma rápida e eficiente. Nesse contexto, entra a utilização da Internet, das redes de computadores, dos meios de comunicação via satélite etc. (BARBOSA, Alexandre de Freitas. *O mundo globalizado* – política, sociedade e economia. Contexto, S. Paulo, SP, 2001).

> política e culturalmente. (SAQUET, 2007, p. 72).

Como decorrência inicia-se a busca por um maior monitoramento dentro do próprio espaço cibernético, visando um maior controle, esse no significado que lhe atribui Rodrigues:

> Controlar, nesse contexto, significa conseguir utilizar esses espaços em maior extensão do que qualquer outro país; ter meios para impedir que outros tenham sucesso em qualquer tentativa de negar o seu uso; e, finalmente, ter capacidade de interditar a sua utilização a terceiros. (2012, p. 6).

Inicialmente, o Estado encontra nas redes de informações digitalizadas (infovias) a oportunidade de projeção do poder sobre as demais dimensões espaciais, até mesmo porque tal infraestrutura decorre de aplicação de uso estatal (exemplo: *DArpaNet*). Num segundo momento, entes não estatais alcançam a mesma compreensão e absorvem para si ações que almejam o poder através de conflitos irregulares.

Nesse novo cenário, os Estados respondem às alterações provocadas por essa nova ordem de ameaças, e por novos atores não estatais, preparando-se para a disputa de poder nessa nova dimensão. O território do Estado, que tem como epiderme suas fronteiras, deixa de ser visto apenas sob as naturezas terrestre, marítima, aérea e cósmica, e passa a ser constituído também por esse particular ambiente, o cibernético, com características bem peculiares e diferentes das outras dimensões, inteirando-se com os demais domínios transcendendo fronteiras físicas, organizacionais, institucionais e geopolíticas, em que o anonimato e a assimetria são as novas características.

> Situar as fronteiras cibernéticas é um desafio que intriga por sua virtualidade, pois à medida que áreas diferentes do globo são postas em interconexão umas com as outras, ondas de transformação social atingem virtualmente toda a superfície da terra (GIDDENS, 1990).

"Nem mesmo os Estados Unidos da América consegue, efetivamente, se defender de um ataque cibernético" (CLARKE, 2010). Analisar como a Grande Estratégia vem sendo elaborada para essa nova dimensão do combate torna-se essencial e, sendo assim, necessitamos enxergar a cibernética sob dois enfoques:

a) Como um espaço em si mesmo, no qual funciona na forma de um sistema semelhante ao que ocorre com o de comunicações e telecomunicações, agregando-se o fato do uso de computadores e de redes. Nesse sentido, o espaço cibernético traria novos desafios ao estabelecimento da ideia de território e delimitação, pois goza de uma série de aspectos que dificultam a apreensão e a compreensão humana

e, por conseguinte, da política de Estado;

b) como recurso de poder, pelo qual a cibernética traz em si a capacidade de ampliação da centralização do poder por parte tanto do Estado, por meio do controle, do monitoramento e do armazenamento das informações sobre os outros domínios espaciais, como por organizações não estatais e seu projeto de poder (ex: ISIS e seu Califado Cibernético).

As abordagens apresentadas em primeiro plano (enfoque inicial) apresentam a importância do estabelecimento de limites no Espaço Cibernético – sua territorialização –, o que demanda as etapas de definição, delimitação e demarcação fronteiriça da competência e responsabilidades a fim de se evitar o conflito. No segundo enfoque, identificamos o seu uso em razão do poder, em que os reflexos (possibilidades) advindos desse domínio podem servir, inclusive, para a guerra.

Resumindo-se:

> O espaço de lugares, no qual as relações de poder são hierárquicas, é substituído pelo espaço de fluxos, consequência da combinação entre mudanças econômicas, tecnológicas e sociais. Nesse novo espaço, a informação passa a ter importância primordial, pois é ela que permite a conexão global e local, ao mesmo tempo. A informação passa a ser transportada por meio da comunicação, principalmente eletrônica, e os sistemas de informação se tornam essenciais para o predomínio estrutural dos espaços de fluxos. (CASTELLS, 1999).

3.3 AS ORIGENS DO TERMO: CIBERNÉTICA

O significado moderno da palavra relaciona-se ao uso do termo *governator* (do inglês) em Mecânica. Em 1790, James Watt usou a expressão para designar um mecanismo que estabilizasse a velocidade de rotação do motor a vapor. Em 1868, o físico escocês James Clerk Maxwell descreveu certo tipo de mecanismo de controle no ensaio "The Theory of Governors". Foi nesse ensaio de Maxwell que o professor de matemática do Instituto de Tecnologia de Massachusetts (M.I.T) Norbert Wiener diz ter-se inspirado para, em 1948, escrever a obra *Cybernetics, or Control and Communcation in the Animal and the Machine*. Contudo, admitiu Norbert Wiener que, mais tarde, casualmente, descobriu que essa palavra já tinha sido empregada, nos primórdios do século XIX, tanto por Ampère, no contexto da ciência política, quanto por um cientista polonês (WIENER, 1973).

Em 1950, Wiener publicou *Cibernética e Sociedade*: O uso humano de seres humano, cujo texto revisado pelo autor em 1954 foi traduzido para o português, por José Paulo Paes, e publicado pela Editora Cultrix Ltda, em 1973. Por meio dessa obra, o matemático do M.I.T.

tornou acessíveis a um público maior os conceitos fundamentais acerca da cibernética e algumas de suas implicações.

Ao contrário do que se poderia imaginar, as aplicações dessa ciência, assim considerada por Wiener, vão desde o campo da Filosofia, inserindo-se na Sociologia e na Psicologia, e alcançando o da Tecnologia (Engenharia). A obra de Wiener acerca da cibernética vai muito além de questões ligadas a mecanismos e a autômatos. Pela cibernética, disse esse autor, o homem seria capaz de compreender o que acontece com qualquer organismo, por meio da análise de seu sistema de funcionamento, principalmente no que concerne à informação e à reação do sistema a essa. Tanto o organismo dos seres humanos, por meio dos sentidos, quanto na estrutura de uma máquina (por sensores artificiais), o papel que a informação exerce é a chave de seu entendimento e de sua prospecção.

O professor Wiener transporta, inclusive, a cibernética para a condução do corpo social, tanto por meio das leis, as quais para o autor exercem papel de emissoras de informações – mensagens – que formatam o comportamento da sociedade, como por meio do papel da comunicação, que para ele "cimenta a estrutura da sociedade" e, ao mesmo tempo, expande a cultura (WIENER, 1973, p. 27). Assim chega a afirmar esse matemático: "A minha tese é a de que o funcionamento físico do indivíduo vivo e o de algumas máquinas de comunicação mais recentes são exatamente paralelos no esforço [sic] análogo de dominar a entropia[27] através da realimentação". (WIENER, 1973, p. 26).

O ponto da questão para Wiener são as ramificações possíveis da Teoria das Mensagens, cujo conteúdo consiste na informação. O interesse do matemático por esse tema tem origem em um projeto de pesquisa iniciado nos primeiros anos da década de 1940, quando, como parte do esforço de guerra norte-americano, ele recebeu a incumbência de desenvolver um "sistema de controle de baterias antiaéreas que fosse capaz de acompanhar a trajetória em que se movia um avião, predizer sua posição futura e disparar fogo levando em conta, senão só os hiatos humanos do canhão e do avião envolvidos". (MOREIRA, 1980, p. 32).

Wiener explicou que, por meio desse poder de comando e controle, as máquinas atuais seriam capazes de interagir com o ambiente externo, por meio de sensores. Dessa forma, de um sistema fechado[28], comum nas máquinas pretéritas, as máquinas modernas se

[27] A entropia, para esse autor, fisicamente tratando, significa uma medida de desordem.

[28] Sistema fechado: aquele que não sofre influência do ambiente no qual está inserido. Por isso, basicamente, seu funcionamento depende de si mesmo. É, por si, um sistema isolado. Por sua vez, sistema aberto caracteriza-se por estar exposto a interações com o ambiente onde está inserido. Dessa forma, essa interação gera

caracterizariam por um sistema aberto, pelo qual a troca de informações/mensagem serviria como fenômeno de realimentação (feedback) constante, como ocorre em um monitoramento e uma reflexiva ação.

Os exemplos, aponta o matemático do M.I.T, podem ser encontrados nos mísseis controlados, na espoleta de proximidade, no abridor automático de portas, no elevador, entre outros. Tudo isso se torna possível, uma vez que essas "novas" máquinas possuem partes responsáveis pelo sensoriamento, órgãos sensoriais. São esses órgãos que permitem à máquina receber mensagem do exterior, como uma espécie de receptores e atualizadores de informação, a fim de evitar a entropia. Daí também advém a conhecida nomenclatura utilizada pela teoria do sistema, como o input (entrada) e o output (saída), além do "feedback".

Segundo o próprio Wiener, a cibernética envolveria "o estudo do que em contexto humano é às vezes descrito genericamente como o ato de pensar e o que em engenharia é conhecido como controle e comunicação" (MOREIRA, 1980, p. 33). Em suma, pretendia-se estudar, compreender e dominar uma trilogia: transmissão, entendimento (processamento), e resposta (retorno/resultado), cujo objeto interior é a mensagem e, por conseguinte, a informação nessa contida. Dessa forma, Norbert Wiener configuraria uma teoria sobre a comunicação e o controle. Para ele, o propósito da cibernética seria o de desenvolver uma linguagem e técnicas que fossem capazes, de fato, de habilitar os homens no tratamento dos problemas relacionados ao controle e à comunicação em geral através de máquinas. (WIENER, 1973).

Assim, os primeiros projetos, cujo termo cibernética foi utilizado com esse significado, tratavam do desenvolvimento de mecanismos destinados a regular, automaticamente, artefatos industriais e bélicos, capazes de substituir o homem na tarefa de corrigir desvios dos sistemas projetados por dispositivos reguladores programados especificamente para essa finalidade (EPSTEIN, 1986, p. 13-14).

De forma geral, cibernética, no século XX, passou-se a sugerir o estudo das funções humanas de controle e dos sistemas mecânicos e eletrônicos que se destinam a substituí-las (THEOPHILO, 2011). É também essa ideia registrada na *American Society for Cybernetics*: "o termo foi criado em 1948 pelo matemático Norbert Wiener para abranger todo o campo da teoria do controle e comunicação, seja na máquina ou no animal". (AMERICAN SOCIETY FOR CIBERNETICS FOUNDATIONS, 2008).

O sentido atual, que é também o utilizado neste trabalho e que justifica a constituição

---

realimentações que podem ser positivas ou negativas. Nesse caso, há maior chance de entropia.

de uma defesa específica para esse setor, versa, de maneira geral, sobre o controle e a comunicação por meio de uma máquina processadora de mensagem: o computador.

3.4 EMPREGO ATUAL

Com o advento das redes de computadores, especialmente a Internet, a conotação da cibernética se aproxima cada vez mais da ideia de infovias (sistemas de informação interligados). Nesse sentido, o controle dos sistemas de comunicação passa a dominar a "agenda cibernética". Temas como segurança, defesa e guerra cibernética passam a fazer parte do dia a dia, indo justamente ao encontro da tese de Alvim e Heidi Toflller de que a forma do homem combater está, em muito, atrelada à forma como ele produz e a como são tratados os meios de produção (TOFFLER, 1995, p. 17).

É nesse sentido que acompanhamos acerca de duas décadas o enxugamento da produção, o incremento na velocidade das inovações, a maior necessidade da integração dos sistemas e de sua infraestrutura, a diminuição do tamanho dos componentes eletroeletrônicos simultaneamente ao aumento da precisão, e o deslocamento do trabalho calcado na força bruta para o que demanda profunda qualificação técnica. É também nesse sentido que observamos mudanças na forma de se combater.

Em abril de 2007, foram divulgados ataques maciços a instituições públicas e privadas da Estônia; em agosto de 2008, ocorreram ações cibernéticas em setores estratégicos da Geórgia; em 2010, foram noticiadas ações nos complexos industriais da China, da Indonésia e do Irã, incluindo neste último o seu setor nuclear, e, recentemente, tornou-se público o caso Wikileaks, que divulgou cerca de 250.000 mensagens confidenciais envolvendo o governo dos Estados Unidos da América.

Em 2011, empresas brasileiras, como a Petrobras, sofreram alguma forma de tentativa de "intrusão cibernética", com ou sem êxito, e até a Administração Pública Federal (APF) foi vitimada no website da Presidência da República.

Em tom alarmante, um artigo publicado na *Revista Info Exame* (2011) sugere que qualquer computador pessoal pode estar sendo utilizado por hackers em ações criminosas. Ele apresenta uma tabela contendo a cotação de trabalhos no mercado negro das fraudes: com aproximadamente US$ 1, podemos adquirir dados pessoais roubados para abrirmos uma conta bancária; com o valor de US$ 150, compramos o envio de spams para 1 milhão de e-mails; e, com um pouco mais de investimento, aproximadamente US$ 300, podemos infectar uma

centena de máquinas (MACHADO, 2011).

Como resposta, vários atores do sistema internacional vêm organizando seus respectivos sistemas de Segurança e de Defesa nessa área, como é o caso dos EUA; da UE, por cada um de seus membros e por meio da OTAN; da Rússia; da China; de Taiwan, da Coreia do Norte e do Irã, alguns, inclusive, constituindo uma nova Força Armada, além das convencionais: Marinha, Exército e Aeronáutica, como apontou àquele tempo o general de divisão do Exército Brasileiro José Carlos dos Santos, então Comandante do Centro de Defesa Cibernética do Exército, em entrevista à *Revista Época*. (SANTOS, 2011).

Nessa linha (CLARK, 2010), segue o pesquisador francês Daniel Ventre (2012, p. 43), sobre segurança da informação, informando que a China anunciou, ainda em 2003, a criação de unidades de guerra cibernética alojadas na base naval da Ilha de Hainan, sul da Província de Cantão. O autor também relata que os chineses treinam o emprego de "armas" técnicas nesse setor para dez objetivos possíveis: 1) plantar minas de informação; 2) realizar reconhecimento de informações; 3) alterar dados da rede; 4) liberar bombas de informações; 5) difundir lixo de informações; 6) difundir propaganda; 7) liberar informações enganosas; 8) liberar informações de clones; 9) organizar defesa de informações; 10) estabelecer estações de espionagem de rede.

Também quanto à China, com relação às ações de cyber-espionagem, o presidente dos Estados Unidos, Barack Obama, discursando para o Congresso em 12 de fevereiro de 2013[29], anunciou a preocupação que vem enfrentando, a fim de evitar os ciberataques:

> Sabemos que empresas e países estrangeiros furtam nossos segredos industriais. Agora, nossos inimigos estão tentando se capacitar para sabotar nossa rede de energia elétrica, instituições financeiras e controle de tráfego aéreo. (OBAMA, 2013).

Todavia, por outro lado, os mesmos Estados Unidos, em ação conjunta com Israel,

[29] Obama, State of The Union Speech – "América também deve enfrentar o rápido crescimento a ameaça de ataques cibernéticos. Sabemos que os hackers roubam identidades das pessoas e se infiltram em suas caixas postais eletrônicas pessoais. Sabemos que países estrangeiros e empresas roubam nossos segredos corporativos. Agora nossos inimigos também estão buscando a capacidade de sabotar nossa rede elétrica, as nossas instituições financeiras, e os nossos sistemas de controle de tráfego aéreo. Não podemos olhar para trás daqui a alguns anos e nos questionar por que não fizemos nada em face de ameaças reais à nossa segurança e de nossa economia. É por isso que, mais cedo hoje, assinei uma nova ordem executiva que fortalecerá nossas defesas cibernéticas aumentando o compartilhamento de informações e desenvolvendo padrões para proteger nossa segurança nacional, nossos empregos e nossa privacidade. Agora, o Congresso deve agir também, através da aprovação de legislação para dar ao nosso governo uma maior capacidade de garantir nossas redes e impedir ataques". (Obama, State of Union Speech, 12 de Fevereiro, 2013. Disponível em: <https://www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address-prepared-delivery>. Acesso em: 1 ago. 2016, tradução nossa).

foram acusados de sabotarem o sistema referente ao enriquecimento de urânio do Irã, em 2010.

Os Organismos Internacionais (OI) também vêm demonstrando grande interesse na exploração e na segurança dessa dimensão espacial e recurso de poder. No final de 2011, a ONU, por meio da União Internacional da Telecomunicação (ITU), realizou um exercício de simulação contra ataques cibernéticos, contando com a participação de países do sudeste asiático, entre esses o Laos, o Camboja e o Vietnã. Para o responsável pela condução da simulação, Hamadoun Touré (2011), Secretário Geral da ITU: "Ataques cibernéticos não têm fronteiras, por isso é vital cada país compartilhar informações e experiências". Por essa declaração, dois pilares básicos para o ente estatal e seu sistema são postos em questão: primeiro, a alegação sobre a inexistência de fronteiras nesse espaço, consoante H. Touré; depois, a abordagem sobre a necessidade do compartilhamento de informação está como um dos principais recursos do poder estatal (GIDDENS, 2001). Nesses termos, assim também lembra Ron Deibert, como apontamos no início do capítulo: "Informação (seu sigilo), disse o Cardeal Richilieu, em 1641, é o assunto mais fundamental do Estado" (DEIBERT, 2012, p. 18, tradução nossa).

Para ilustrar o enorme potencial que traz essa nova dimensão, tem-se o caso ocorrido na Geórgia, em agosto de 2008, no qual, pela primeira vez, uma operação de Ataque Contra Redes de Computadores de grande escala foi executada em conjunto com importantes operações de combate terrestres. Apesar de o ataque cibernético não ter sido admitido pelo governo russo, esse foi o maior beneficiário, pois conseguiu "isolar e silenciar" os georgianos, produzindo efeitos psicológicos e de informações, reduzindo a capacidade de comunicar-se com o mundo externo, não apenas pela mídia e pelo governo, mas também pela população local. Para Paul Shakarian (2011, p. 72), professor assistente no Departamento de Engenharia Elétrica e Ciência da Computação da Academia Militar dos EUA (USMA), "independentemente do Kremlin estar ou não envolvido nos ataques cibernéticos […] talvez devamos passar a considerar as capacidades cibernéticas como um sistema operacional do campo de batalha, assim como o são a manobra, a artilharia, a defesa antiaérea, etc.".

Do ponto de vista militar, ameaças cibernéticas se relacionam a um grande espectro de temas, que envolvem desde tópicos de guerra eletrônica até segurança de sistemas de informação, conforme inferimos do Quadro 1, a seguir.

Quadro 1 – Temas relacionados à guerra cibernética

GUERRA ELETRÔNICA: conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas.
GUERRA CENTRADA EM REDES: guerra que reúne em rede os mais diversos elementos das forças armadas de um país, permitindo-lhe administrar diversas tarefas que vão desde a coleta até a distribuição de informações críticas entre esses muitos elementos. Outorga-lhe maior capacidade de combate ao ligar em rede os elementos de sensoriamento, de combate e de comando. Visa obter melhor sincronismo entre aqueles elementos e os efeitos que podem proporcionar, assim como o incremento na velocidade das operações bélicas e do processo decisório de comando.
GUERRA DE INFORMAÇÃO: conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo que garante as informações e os processos amigos.

Fonte: BRASIL. *Glossário das Forças Armadas*, 2015.

O envolvimento militar, tanto defensivo quanto ofensivo, em uma guerra cibernética, sugere sensoriamento (monitoramento e detecção), processamento e atuação (AMARANTE, 2010). Nesse aspecto, o circuito **Detecção-Processamento-Atuação** apontado por José Amarante (2010, p. 3-8) corresponderia à ideia de Guerra Centrada em Redes (Network Centric Warfare) (FONTENELLE, 2008, p. 16; SILVEIRA, 2011, p. 33), que busca a consciência situacional, isto é, que "a otimização do fluxo informacional numa rede de computadores e comunicações provê informações mais consistentes para tomadas de decisão mais adequadas e oportunas". (FONTENELLE, 2008, p. 16).

Faz-se ainda necessário diferenciar o campo eletromagnético (telecomunicações e ondas hertz), das redes de computadores e do controle da informação (sistema de informação) que, consoante Lévy, compõe o ciberespaço:

> Eu defino o ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Essa definição inclui o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes hertzianas e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização. (1999, p. 94-95).

Ainda para Pierre Lévy, a palavra "ciberespaço" foi inventada por William Gibson, em 1984, no romance de ficção científica Neuromancer. Nesse sentido, Ron Deibert denomina o canadense William Gibson como o "pai" do ciberespaço (DEIBERT, 2012).

Para W. Gibson, o ciberespaço designa o universo das redes digitais, descrito como campo de batalha entre empresas multinacionais, palco de conflitos mundiais e nova fronteira econômica e cultural. Esse espaço criado por Gibson torna sensível a geografia móvel da informação, normalmente invisível, pois, pela sua criação, alguns heróis tornam-se capazes de

entrar “fisicamente” nesse espaço de dados e lá viverem todos os tipos de aventura.

Dessa forma, cibernética envolve muito mais temas que o simples controle de sistemas computacionais de informação via Internet, como sugere o senso comum. Oliveira prefere não definir o termo, por considerar um tanto quanto prematura a apresentação de conceito, sobretudo de uma área extremamente dinâmica, apenas falando em entendimento acerca de um “ambiente ou espaço cibernético, que contém a interação de pessoas, empresas e instituições públicas e privadas, nacionais e internacionais, utilizando modernos recursos de Tecnologia da Informação e das Comunicações (TIC).” (OLIVEIRA, 2011, p. 108).

Nessa linha segue também Raphael Mandarino Jr., que optou por não conceituar cibernética, mas sim o seu espaço, o ciberespaço, como “conjunto de pessoas, das empresas, dos equipamentos e suas interconexões, dos sistemas de informação e das informações que por eles trafegam [...]” (MANDARINO JÚNIOR, 2009, p. 43).

No VI Congresso de Relações Internacionais da *Universidad Nacional de La Plata*, em novembro de 2012, os pesquisadores Sergio Eissa, Sol Gostaldi, Iván Poczynok e Maria Di Tullio, da *Universidad de Buenos Aires*, também demonstraram preocupação em diferenciar os termos ligados à cibernética. Em seu artigo, esses pesquisadores expõem a confusão geralmente feita sobre os termos: operações cibernéticas e ataques cibernéticos, ciberguerra e guerra de informação.

Tal perturbação incide, segundo esses autores, sobretudo na forma como serão definidas as responsabilidades e a tomada de decisões, mais precisamente com a preocupação em separar questões voltadas para a Segurança (*Seguridad Interior*) das questões que envolvem diretamente o Instrumento Militar (*Defensa Nacional*). Apesar disso, em um ponto os pesquisadores da *Universidad de Buenos Aires* concordam: o núcleo do ciberespaço se constitui da produção e da transferência de informação (EISSA et al., 2012, p. 2-3).

Mais adiante, neste mesmo artigo, Sergio Eissa define operações cibernéticas como aquelas “ações contra um computador, ou através de um computador ou um sistema de computador, utilizando fluxo de dados” (EISSA et. al., p. 8, tradução nossa), assumindo como cerne da questão, além da informação, o uso de computador e assim vinculando-se à ideia de rede. Esse teor também pode ser encontrado na publicação do Conselho de Pesquisa Nacional dos EUA *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities on Offensive Information Warfare*: “[…] ciberataque refere-se a deliberar ações para alterar, interromper, enganar, degradar ou destruir sistemas de computador ou redes ou programa de informação residente ou em trânsito nesses sistemas ou

redes." (SALES, 2010).

Em todos esses estudos há um ponto de contato – a informação –, o seu uso ou negação de uso. Dessa forma, diante dos objetivos do trabalho, estabeleceremos um recorte na abrangência que o termo sugere, levando em consideração os aspectos que dizem respeito à comunicação e ao controle de sistemas de informação pautados em rede de computadores ao utilizarmos a sigla C^4I[30], que engloba Comando, Controle, Comunicações, Computação e Inteligência.

> [...] cibernética é um termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por: instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC), bem como os sistemas de armas e vigilância. (CARVALHO, 2011, p. 17).

Abordando especificamente a segurança nessa dimensão espacial, isto é, a segurança no espaço cibernético, o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, do Departamento de Segurança da Informação e Comunicação, do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR), traz que segurança cibernética é "arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2010a).

Desse modo, passando pelo estudo que visava à substituição das funções humanas de controle por sistemas mecânicos e eletrônicos, a cibernética alcança, hoje, uma conotação que compreende as ideias de informação e de comunicação, daí o termo infovias utilizado para representar os meios pelos quais as informações digitalizadas circulam.

A defesa e a segurança dessas infovias, essas constituídas por ferramentas de Tecnologia da Informação e das Comunicações, passam a ser mais um objetivo perseguido pelo Estado, a fim de garantir o fluxo de suas mensagens e de impedir ou negar o acesso ao conteúdo que por essas vias transitam: a informação digitalizada.

Apesar de a estrutura física ou dos meios de comunicação ser, por muito, considerado espaço cibernético, a informação que trafega nesse espaço não o é. Talvez por isso Ron Deibert, Diretor do Centro de Estudos de Segurança Global, da Munk School of Global Affairs, da Universidade de Toronto, em documento publicado pelo Canadian Defence &

[30] Internacionalmente, emprega-se, hoje, a sigla C4ISR (Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento). Na Argentina, C4IVR (EISSAR et al., 2012, p. 9).

Foreign Affairs Institute, afirme que o:

> Ciberespaço se tornou um objeto de intensa contestação, não só entre os diferentes sistemas de governo, mas entre uma multidão do setor privado e da sociedade civil, vez que todos usam e dependem desse domínio, e tem interesse em moldar a sua vantagem estratégica. (2012, tradução nossa).

Lembra ainda Deibert que o modo como solucionar ou evitar conflito nesse novo espaço vai depender em grande parte do regime de governo de cada país. Para ele, Rússia, China e outros países em ascensão defendem uma maior territorialização desse espaço, um maior controle por parte do ente estatal, enquanto os países democrático-liberais, como os Estados Unidos e seus aliados, entre esses o Canadá, são favoráveis a manterem o ciberespaço como um "espaço de uso comum" (DEIBERT, 2012, p. 21), correspondente ao *global common* de Barry Posen (2003, p. 7-8), de Rodrigues (2012, p. 5) e de Ferreira (2012, p. 70).

Deibert conclui seu raciocínio dizendo que o momento em que vivemos é bastante decisivo com relação ao ciberespaço (DEIBERT, 2012, p. 23) e que a visão mais territorializante desse espaço vem atraindo e formando uma rede com vários atores, inclusive dentro dos organismos internacionais. O Canadá, segundo ele, é favorável à garantia do ciberespaço como um *global common*, defendendo sim uma normatização, mas não o cerceamento dos serviços possibilitados por esse meio.

Nessa visada, notamos que há traços que coincidem bastante com as discussões acerca de princípios ligados a teorias das relações internacionais: de um lado, a visão realista da anarquia do sistema e de sua condução inexorável ao dilema de segurança, sendo o poder mensurado principalmente em termos de capacidades militares; do outro, os liberais, idealistas ou neoliberais, que veem a discussão sob o enfoque da interdependência, da pluralidade de atores internacionais e do papel das organizações/instituições no regramento de comportamento do sistema, procurando, entre outros, no Direito Internacional a fonte de solução de conflitos.

Porém, ao que tudo indica, os mais aptos hoje na utilização desse espaço como recurso não pretendem ceder a uma regulamentação mais profunda, ou até mesmo à sua delimitação, sobretudo no tocante ao uso para a guerra. Permanecendo formalmente como *global common*, o espaço cibernético, para uns, já significa, materialmente, um espaço territorializado, apesar de considerado "ilimitado".

3.5 ESPAÇO CIBERNÉTICO E O PODER

Como vimos, para Pierre Lévy o espaço cibernético corresponde a um espaço de comunicação aberto pela interconexão de computadores e das memórias dos computadores, incluindo os sistemas de comunicação tanto por meio de ondas hertz quanto pela telefonia clássica, a partir do momento em que essas participarem do processo de transmissão de informações digitalizadas (LÉVY, 1999).

Para Raphael Mandarino, antigo diretor do DSIC-GSI/PR, o espaço cibernético compreende também as pessoas, as empresas e os equipamentos que porventura estejam interconectados, participando, de alguma maneira, do tráfego de informações digitalizadas.

Investigando o que seria o espaço cibernético e indicando, incialmente, que o termo mais parecia, em um exercício de imaginação, outra dimensão (CLARKE, 2010), em seguida, o autor atesta que esse novo espaço é realmente bem mundano, no qual está inserido o laptop que nós conduzimos ou o que as crianças levam para a escola ou, ainda, um computador de nosso local de trabalho ou uma tubulação instalada sob uma rua. Para Clarke, hoje o espaço cibernético está em toda parte, em todo lugar em que encontramos um computador, ou um processador, ou um cabo de ligação. (CLARKE, 2010).

O espaço cibernético, para esses autores, já é hoje uma zona de guerra. Como conceito, trazem esses norte-americanos que o espaço cibernético corresponde a todas as redes de computadores, em todo o mundo, e tudo que conecte ou controle. Espaço cibernético inclui outras redes de computadores além da Internet, que, supostamente, não são acessíveis a partir dessa. (CLARKE, 2010).

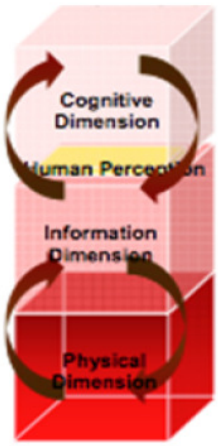
Nesse sentido segue Derek Reveron, baseando-se na definição de espaço cibernético do Departamento de Defesa dos EUA, e informando que esse espaço é “um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores embarcados, e controladores.” (REVERON, 2012, tradução nossa). Prossegue esse autor, afirmando que o espaço cibernético, assim como o ambiente físico, é muito abrangente, incluindo o hardware, como redes e máquinas; as informações, como dados e mídia; o cognitivo, como o processo mental das pessoas; e o virtual, onde as pessoas se conectam socialmente (REVERON, 2012).

Tratando do espaço das informações, de forma *lato sensu*, a Joint Publication 3-13 (EUA, 2014), primeiramente aprovada em 1998 pelo Chefe do Estado Maior Conjunto das

Forças Armadas dos EUA, após orientação do Departamento de Defesa daquele país, e atualizada em 2014, traz três dimensões "onde humanos e sistemas observam, orientam, decidem e agem sobre as informações, constituindo-se assim no principal ambiente onde são tomadas as decisões". (CORRÊA, 2012, p. 6).

Figura 1 – Ambiente da informação

Ambiente da Informação
Dimensão Cognitiva – onde são tomadas as decisões humanas. É a dimensão do intangível, onde residem a moral, a coesão das unidades militares, a opinião pública, a consciência situacional, entre outros.
Dimensão da Informação - onde são tomadas as decisões automatizadas, pois é nesta dimensão que as informações são coletadas, processadas, armazenadas, disseminadas, mostradas e protegidas. Possui uma natureza ambígua, pois trata-se da própria informação e o meio pelo qual ela tramita, ocupando-se do conteúdo, da qualidade e do fluxo das informações. Esta dimensão une a outras duas.
Dimensão Física - onde ocorre a interseção do ambiente da informação com o mundo físico. São os computadores e as redes que compõe os sistemas de dados e de comunicações, e que suportam toda a infra-estrutura.



Fonte: JP 3-13 (2006 apud CORRÊA, 2012).

Daniel Ventre, pesquisador do Centro de Investigações Científicas e secretário-geral do Grupo Europeu de Pesquisa de Normas (GERN), ambos de Paris, elaborou uma proposta interessante quanto aos componentes do espaço cibernético. Para Ventre, esse espaço é composto por três "capas", assim denominada cada parte desse domínio. Colocando em um quadro, a proposta de Ventre fica assim ilustrada:

Quadro 2 – Espaço cibernético – "capas" e respectiva composição

Capa	COMPONENTES
Inferior	Dísica, material, condizente à infraestrutura (hardware, redes...).
Intermediária	Softwares de aplicações.
Superior	Cognitiva.

Fonte: Elaborado pelo autor a partir de VENTRE (2012, p. 34).

A visão do pesquisador do GERN-Paris coaduna com a tríade formulada por especialistas das áreas de análise de sistemas e de informática que entendem o hardware como a parte rígida ou os componentes do sistema; o software como o que diz respeito à programação; e o peopleware refere-se às pessoas que atuam nesse setor, por meio do conhecimento. Além disso, representando graficamente, Daniel Ventre expõe o domínio

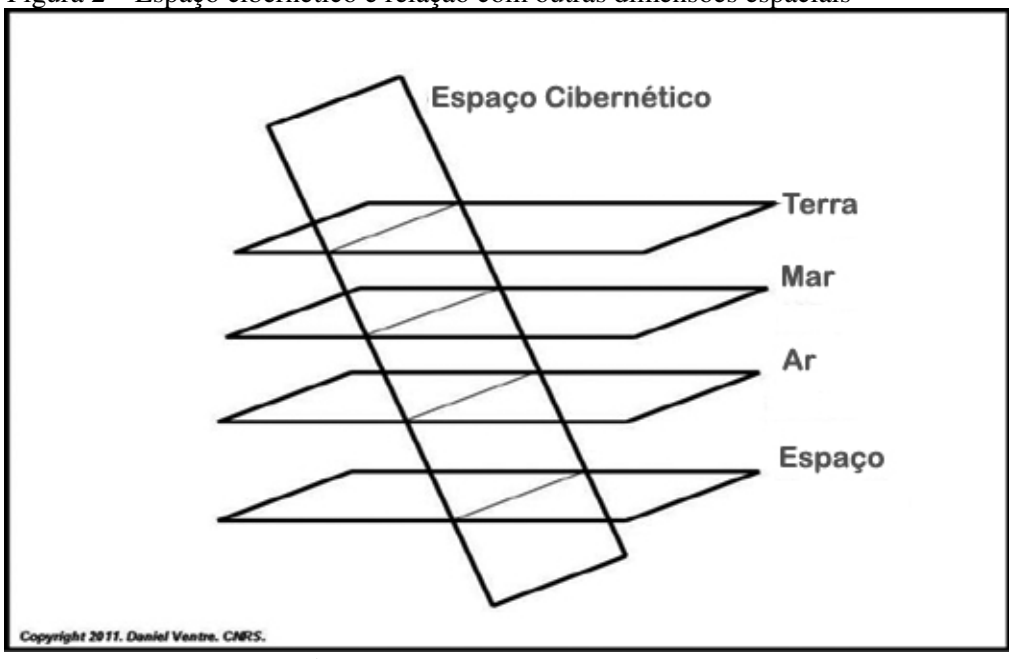
cibernético face às outras dimensões espaciais, conforme figura a seguir, afirmando que uma das características mais marcantes desse novo domínio é a sua transversalidade (VENTRE, 2012, p. 34).

Essa representação corrobora nosso entendimento exposto até o presente momento em que essa transversalidade se torna uma característica bem significativa do espaço cibernético, uma vez que permite a projeção de poder e seus reflexos nos demais domínios espaciais.

Ainda se atendo ao espaço cibernético, sobretudo quanto às suas características e composição, Joseph Nye (2012) enxergou essa dimensão espacial dividida em duas partes principais: o "intraespaço" e o "extra-espaço" cibernético.

> Ao analisarmos essa forma de simplificação, chegamos à conclusão que muito condiz com a visão do então Chefe do Comando Cibernético dos Estados Unidos, General Keith Alexander, que vê o Espaço Cibernético "sendo usado por militares no futuro (operando de dentro ou através dele) para atacar pessoal, instalações, ou equipamentos [...]." (REVERON, 2012, tradução nossa).

Figura 2 – Espaço cibernético e relação com outras dimensões espaciais



Fonte: VENTRE (2012, p. 35).

Dessa forma, ambos mencionam a possibilidade de operações ocorrerem dentro (no intraespaço) e através (no extra-espaço) do espaço cibernético. J. Nye chega a comparar o poder advindo da cibernética com o poder marítimo, que também se distingue em poder naval sobre os oceanos – o que, por sua teorização, corresponderia ao intraespaço marítimo –, do poder naval sobre outros domínios, isto é, o poder projetado do ambiente marítimo para outro domínio espacial, no caso o extra-espaço cibernético.

Joseph Nye também aborda a utilização do poder nesse ambiente espacial com exemplificações de uso que podem ocorrer na forma branda (softpower) ou na forma dura (hardpower), tanto dentro (intraespaço) quanto fora (extra-espaço) do espaço cibernético, conforme exposto no quadro a seguir.

No "intraespaço" de Nye, na "capa" inferior e intermediária de Ventre, ou no que denominamos ao longo do trabalho espaço cibernético considerado em si mesmo, algumas ações são efetuadas a partir do, e com reflexos no, próprio espaço, como constam os exemplos dos ataques de negação de serviço (Distributed Denial of Service – DDoS[31]) do quadro a seguir, ou do controle de companhias e empresas, no caso da estrutura física do ambiente cibernético, ambas caracterizando formas de utilização hard do poder.

Quadro 3 – Dimensões: informacional e física do poder cibernético e algumas possibilidades

Alvos do poder cibernético		
	Intraespaço cibernético	**Extra-espaço cibernético**
Instrumentos de informação	Duro: ataques de negação de serviço. Brando: determinação de normas e padrões.	Duro: ataque em sistema SCADA[32]. Brando: campanha de diplomacia pública para influenciar a opinião pública.
Instrumentos físicos	Duro: controle das companhias por parte do governo. Brando: software para ajudar ativistas dos direitos humanos.	Duro: roteadores de bomba ou corte de cabos. Brando: protestos para denunciar os provedores cibernéticos.

Fonte: Elaborado e adaptado pelo autor a partir de J. NYE (2012, p. 166).

Concomitantemente, a relação política e seus conflitos nesse espaço podem ocasionar reflexos externos, digamos no mundo sensorial humano, como no ataque ao sistema SCADA, em 2010, nas usinas nucleares iranianas ou na possibilidade de rupturas de serviços essenciais à população, como no caso de danos às estruturas estratégicas de um Estado: energia elétrica, distribuição de água, serviço de telecomunicações, sistema financeiro etc.

Dessa forma e por suas várias interpretações e possibilidades, o espaço cibernético, apesar de considerado virtual e um *global common*, já há algum tempo o deixou de ser.

Alguns atores empoderam-se desse espaço, delimitando-o unilateralmente, dispondo de seu controle. É nesse sentido que enxergamos o espaço cibernético não mais como um espaço comum, e sim um território. Tentar entendê-lo, teorizá-lo, saber defini-lo e demarcá-lo,

[31] DDos Ou DoS Attack ocorre a partir da sobrecarga do sistema e não de uma invasão. Geralmente, um computador mestre comanda milhares de computadores denominados zumbis, que passam a funcionar como máquinas escravizadas.

[32] SCADA – Supervisory Control and Data Acquisition – sistemas que utilizam software para monitorar e supervisionar as variáveis e os dispositivos de sistemas de controle conectados através de drivers específicos.

com as respectivas responsabilidades advindas, seria um bom começo.

3.6 O ESPAÇO CIBERNÉTICO BRASILEIRO

Um marco significativo da organização da Administração Pública Federal, como hoje a conhecemos, foi estabelecido pela publicação do Decreto-Lei 200, de 25 de fevereiro de 1967, o qual se rege pelos princípios fundamentais do planejamento, da coordenação, da descentralização e da delegação de competências, com destaque em seu artigo 30, no qual as atividades que mereçam a coordenação central devem ser organizadas em forma de sistemas.

Com o uso cada vez mais gradativo e complexo da informática na administração pública, e os problemas de segurança daí derivados, o assunto segurança da informação somente é abordado especificamente pela primeira vez na legislação federal em 13 de junho de 2000 no Decreto nº 3.505, que Instituiu a Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal por iniciativa Conselho de Segurança Nacional – CSN. Note-se, entretanto, que, dentre as atribuições que foram citadas para a emissão desse Decreto, encontram-se a Lei nº 8.159 de 8 de janeiro de 1991 que dispunha sobre a política nacional de arquivos públicos e privados e o Decreto nº 2.910 de 29 de dezembro de 1998, que estabelecia normas para salvaguarda de documentos, materiais, áreas e sistemas de informação de natureza sigilosos. Em nenhum trecho dessas legislações o termo segurança da informação é encontrado, apesar de estar implícito o seu sentido.

Em seguida, é editada a Medida Provisória – MP nº 2.216-37, de 31 de agosto de 2001, publicada em edição extra do *Diário Oficial da União* – D.O.U. de 1 de setembro de 2001 que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998, dispondo sobre a organização da Presidência da República e dos Ministérios e citando o termo "segurança da informação". Nessa MP, dentre outras alterações, foi criado o Gabinete de Segurança Institucional da Presidência da República, que recebe como uma de suas competências a responsabilidade de coordenar as atividades de segurança da informação na Administração Pública Federal.

A regulamentação do assunto permaneceu inalterada e válida como proposto no Decreto nº 3.505/2000 que estabelece em seu artigo 2º o conceito de Segurança da Informação:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados

> ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Nesse conceito, arrojado para a época, percebe-se a preocupação dos legisladores em proteger as informações governamentais de ações de agentes internos e externos, antecipando-se aos incidentes e problemas de segurança, que hoje chegam à casa dos milhares[33] e que constituem ameaças existentes.

O Decreto institui também, em seu artigo 6º, o Comitê Gestor da Segurança da Informação – CGSI, com atribuição de:

> Art. 6º - Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos neste Decreto. (Decreto nº. 3.505/2000).

Ocorre que, em 16 de julho de 1997, data anterior à promulgação do Decreto 3505, foi sancionada a Lei nº 9.472, que dispunha sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador da área: a Agência Nacional de Telecomunicações, com competência e poderes muito maiores e superpostos àquela diretriz. Decorrente das superposições de competências e do momento político à época, fez-se com que algumas ações fossem priorizadas, como, por exemplo, a criação do modelo e implementação das infraestruturas de chaves públicas e de certificação digital do país.

Ocorre que o incremento das TICs por toda a Administração Pública Federal, e a falta de um órgão executivo que coordenasse de fato as ações de SIC, fez com que as atividades relativas à segurança da informação fossem implementadas, não como promulgadas naquele decreto, mas sim de acordo com a visão sobre a sua importância de cada administrador nos órgãos e entidades da Administração Pública Federal (APF).

O Estado Brasileiro, diante da necessidade de exercer a coordenação efetiva das atividades de segurança da informação, entendeu que essa competência deveria permanecer concentrada em uma só organização, e, com a promulgação da Lei nº 10.683, de 29 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios do novo Governo, manteve essa atribuição no Gabinete de Segurança Institucional da

[33] Disponível em: <http://www.cert.br/stats/incidentes>. Acesso em: 20 de maio de 2016.

Presidência da República – GSI/PR, estruturando ainda um órgão subordinado ao GSI/PR para exercer especificamente essa atividade, regulamentando aquela Lei com a edição do Decreto Presidencial Nº 5.772 de 8 de maio de 2006, que criou o Departamento de Segurança da Informação e Comunicações – DSIC.

Em 13 de junho de 2008, o DSIC, depois de demorados estudos e negociações no âmbito do CGSI, consegue consenso para fazer publicar a Instrução Normativa nº 001/GSI, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta. É importante destacar que o entendimento sobre a necessidade de se legislar sobre o assunto segurança da informação tem se mostrado uma ação de Estado, pois ultrapassa os limites temporais de governos.

Ademais da legislação existente, como já referenciado, a necessidade dessa medida ficou comprovada por uma pesquisa realizada pelo Tribunal de Contas da União – TCU, que se transformou no Acórdão nº 1602, de 15 de agosto de 2008 (TCU, 2008), sobre segurança da informação nos órgãos e entidades da Administração Pública Federal, e que aponta as seguintes impropriedades no que concerne à prática da segurança da informação e comunicações na APF.

Da totalidade de órgãos da APF:

a) 48% não possuem procedimentos de controle de acesso;

b) 64% não têm política de segurança da informação;

c) 64% não têm área específica de segurança da informação;

d) 75% não adotam análise de riscos;

e) 76% não têm gestão de incidentes;

f) 80% não classificam as informações;

g) 88% não têm Plano de Continuidade de Negócio.

Em função da sensibilidade de algumas informações com que lida a Administração Pública Federal, assegurar que essas informações estejam de acordo com os preceitos da SIC, além da transparência e da proteção contra ameaças internas e externas, requer entender a questão da segurança da informação e comunicações e por extensão à segurança cibernética, como conceituada neste trabalho, são funções típicas de Estado.

De acordo com o mandato legal, cabe ao Gabinete de Segurança Institucional – GSI, em articulação com os demais órgãos e entidades da Administração Pública Federal, exercer a coordenação da função SIC em três dimensões:

a) na presidência da Câmara de Governo de Relações Exteriores e Defesa Nacional –

CREDEN, elaborar as propostas de diretrizes estratégicas de segurança cibernética brasileira;

b) como Secretaria do Conselho de Defesa Nacional – CDN, estimular as discussões no âmbito do Comitê Gestor de Segurança da Informação – CGSI, entidade que preside, do detalhamento daquelas diretrizes; e

c) mediante a ação dos órgãos que pertencem à sua estrutura, em especial ao Departamento de Segurança da Informação e Comunicações – DSIC, consubstanciada em ações de regulamentação e normatização do setor, além do seu papel indutor da capacitação dos servidores públicos federais nas questões de SIC. (MANDARINO, 2009).

As organizações públicas ainda não se adaptaram às mudanças introduzidas pela Sociedade da Informação, apesar do tempo que se utilizam as tecnologias da informação na APF. Essa adaptação, parece-nos, ainda exigirá um longo caminho, principalmente porque o seu uso evidencia dois aspectos que impactam sobremaneira o modelo de gestão hierárquico disseminado na APF. Damos destaque ao incremento do grau de autonomia que os escalões inferiores alcançaram, com o uso maciço de TI, em que informações não mais circulam hierarquicamente e os subordinados podem delas tomar conhecimento, independentemente de suas chefias.

3.6.1 Órgãos e atores de segurança e defesa cibernética

Este trabalho divide as atuações dos principais atores e órgãos em duas vertentes:

a) segurança cibernética, contemplando ações que podem compreender aspectos e atitudes tanto preventivas ou repressivas (ESG, 1983)[34]; e.

b) defesa cibernética, contemplando ações operacionais, de caráter eminentemente ofensivo, caracterizadas por ataques cibernéticos. Este capítulo apresenta apenas os órgãos relacionados direta ou indiretamente à segurança e defesa cibernética.

Entende-se por medidas preventivas aquelas que evitam que ações maléficas possam criar danos maiores ou que se perpetue ao longo do tempo. Abrangem, portanto, a criação e a aplicação de metodologias de gestão de risco e o desenvolvimento de planos de contingências e continuidade para as infraestruturas críticas e principais sistemas sensíveis, essenciais ao bom funcionamento do Estado e da Sociedade Brasileira. Nesses sistemas, estão inclusos

[34] *Escola Superior de Guerra* – Manual Básico, 1983, p. 217; 245.

equipamentos, sistemas de comunicação e softwares, bem como a capacitação dos profissionais encarregados e dos usuários dos diversos sistemas e infraestruturas a serem protegidos. Aqui se encontram também as atividades de resposta a incidente de redes; coleta, estudo e disseminação de correções contra artefatos maliciosos; e disseminação de boas práticas e medidas de proteção das redes informatizadas e de segurança das informações.

Caracteriza-se ainda como prevenção, conforme previsto na Instrução Normativa 001/2008 do GSI (GSI, 2008), o desenvolvimento de Plano Diretor de Segurança da Informação e das Comunicações, Modelos de Gestão, e a especificação e o desenvolvimento de algoritmos criptográficos e de softwares e equipamentos de segurança cibernética como telefones seguros e proteção de VOIP (voz sobre IP).

Por medidas repressivas entenda-se o trabalho de identificação e combate de toda conduta criminosa caracterizada como crime cibernético. Nesse caso, encontram-se as medidas contra o terrorismo cibernético e a sabotagem, desde que ainda não caracterizadas como Guerra Cibernética, quando seriam tratadas no contexto de Defesa Cibernética.

Esse modelo foi estabelecido em 9 de outubro de 2008, como resultado de uma reunião da Câmara de Relações Exteriores e Defesa Nacional – CREDEN, órgão de governo estabelecido pela Lei nº 10.683, de 29 de maio de 2003, convocada para discutir o tema Segurança e Defesa Cibernética. Dessa reunião, deliberou-se pela criação de um Grupo de Trabalho intitulado Segurança Cibernética, com o objetivo de elaborar estudos de segurança da informação e comunicações e esboçar propostas de segurança e de defesa das infraestruturas críticas de informação. Também ficou decidido que a questão da defesa cibernética, por encontrar-se na esfera de beligerância entre Estados, não foi objeto de deliberação, já que decisões desse escopo cabem ao Conselho de Defesa Nacional.

As subseções seguintes apresentam uma lista de órgãos, sem esgotá-la, os quais têm em algum grau, por suas competências ou pelas competências das entidades a eles vinculadas, importância na elaboração e funcionamento de uma Estratégia de Defesa Cibernética.

3.6.1.1 Conselho de Defesa Nacional (CDN)

O Conselho de Defesa Nacional é um órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático. Suas competências constitucionais são (BRASIL, 1988):

> I - opinar nas hipóteses de declaração de guerra e de celebração da paz, nos termos

> desta Constituição;
> II - opinar sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal;
> III - propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo;
> IV - estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.

O Entendimento de tais competências constitucionais no âmbito do Espaço Cibernético torna-se um desafio. O próprio conceito de soberania neste domínio ainda não foi plenamente esclarecido. Entretanto, dada à sua importância estratégica, o CDN é palco para as decisões estratégicas relativas às ações de segurança e defesa cibernética.

3.6.1.2 Câmara de Relações Exteriores e Defesa Nacional (CREDEN)

A CREDEN é um órgão de assessoramento do Presidente da República nos assuntos pertinentes às relações exteriores e de defesa nacional. (Lei nº 10.683, 2003). Por tratar-se de um órgão de Governo, sua continuidade não está assegurada. Atualmente, é a ele reservado um papel importante, e, portanto, essa instância de poder pode assegurar agilidade na construção de diretrizes estratégicas para a segurança das informações e comunicações, bem como para a segurança cibernética, já que o assunto está dentro de suas atribuições. Ela é formada pelos seguintes Ministros de Estado:

a) Chefe do Gabinete de Segurança Institucional da Presidência da República, que a preside;
b) Chefe da Casa Civil da Presidência da República;
c) Justiça;
d) Defesa;
e) Relações Exteriores;
f) Planejamento, Orçamento e Gestão; e
g) – Meio Ambiente.

São convidados, em caráter permanente, os comandantes das Forças Armadas.

3.6.1.3 Casa Civil

A Casa Civil é um órgão essencial da Presidência da República, e de suas

competências extraímos aquelas que interagem com os assuntos segurança cibernética e segurança da informação: execução das políticas de certificados e normas técnicas e operacionais, aprovadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras (ICPBrasil).

Compõem a estrutura da Casa Civil três órgãos que são atores importantes na elaboração das normas e regulamentos da segurança da informação e comunicações e na segurança cibernética:

a) Instituto Nacional de Tecnologia da Informação (ITI), por sua própria missão;
b) Diretoria de Tecnologia da Informação (DIRTI); e
c) Diretoria de Telecomunicações (DITEL), pela posição estratégica que ocupam, pois seus serviços atendem ao primeiro mandatário.

3.6.1.3.1 Instituto Nacional de Tecnologia da Informação (ITI)

O ITI é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, sendo a primeira autoridade da cadeia de certificação – AC Raiz.

3.6.1.3.2 Diretoria de Tecnologia da Informação (DIRTI)

A DIRTI é parte integrante da Casa Civil da Presidência da República e é responsável pelo desenvolvimento, manutenção e acompanhamento de todos os sistemas informatizados utilizados na Presidência da República.

3.6.1.3.3 Diretoria de Telecomunicações (DITEL)

A DITEL é parte integrante da Casa Civil da Presidência da República e é responsável pela instalação, manutenção e acompanhamento de todos os sistemas de comunicações utilizados na Presidência da República.

3.6.1.4 Gabinete de Segurança Institucional da Presidência da República (GSI/PR)

O GSI/PR é um órgão essencial da Presidência da República que possui, dentre outras, as seguintes competências que dizem respeito ao assunto deste estudo:

III - Coordenação das atividades de inteligência federal e de segurança da informação;

3.6.1.4.1 Departamento de Segurança da Informação e Comunicações (DSIC)

O DSIC é um órgão subordinado ao GSI/PR que tem como atribuição operacionalizar as atividades de segurança da informação e comunicações – SIC na Administração Pública Federal, nos seguintes aspectos:

a) regulamentar a segurança da informação e comunicações para toda a APF;
b) capacitar todos os servidores públicos federais, bem como os terceirizados, sobre SIC;
c) realizar acordos internacionais de troca de informações sigilosas;
d) operar o sistema de credenciamento de pessoas e entidades no trato de informações sigilosas;
e) ser o ponto de contato junto à OEA para assuntos de terrorismo cibernético;
f) manter o centro de tratamento e resposta a incidentes nas redes de computadores da APF – CTIR.Gov. Destacamos de sua estrutura do DSIC o CTIR.Gov.

3.6.1.4.1.1 CTIR.GOV E CERT.BR

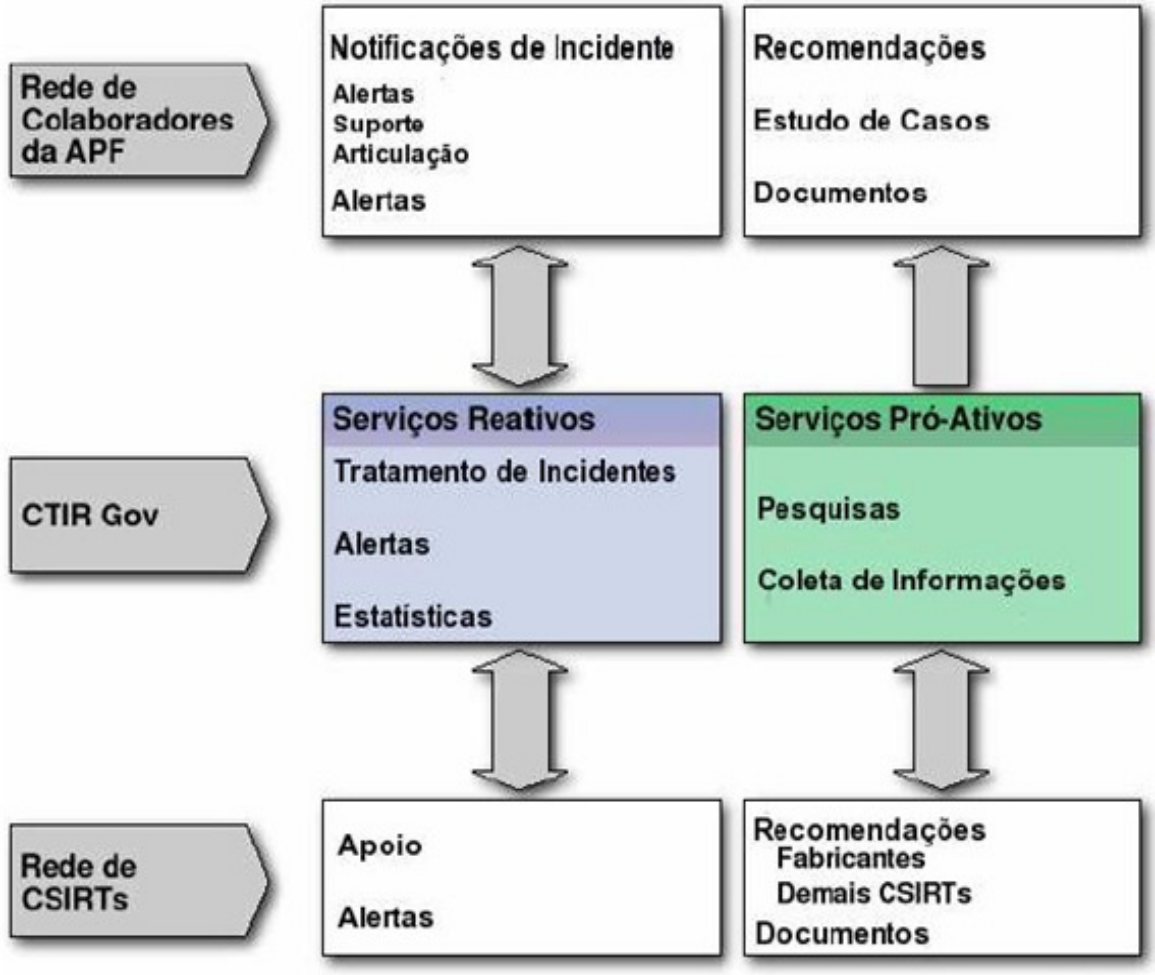
O Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal foi criado em portaria publicada no *Diário Oficial da União* de 30 de junho de 2003 e hoje integra a estrutura do DSIC. Seu objetivo é responder por incidentes de redes e pela busca do intercâmbio de informações necessárias à solução dos incidentes com outras redes e demais centros, no Brasil e no exterior.

Os serviços prestados pelo CTIR.Gov podem ser de caráter reativo e pró-ativo. Em ambos os casos, o Centro tem condições de determinar tendências e padrões das ameaças no espaço cibernético que afetam não só a APF, mas, trabalhando em conjunto com os demais Centros, também as instituições que compõem as infraestruturas críticas de Estado. A Figura 3 ilustra as interações entre o CTIR.Gov e outros órgãos.

O CTIR trabalha em consonância com outro órgão, este ligado ao Comitê Gestor da Internet Brasil (CGI.br), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

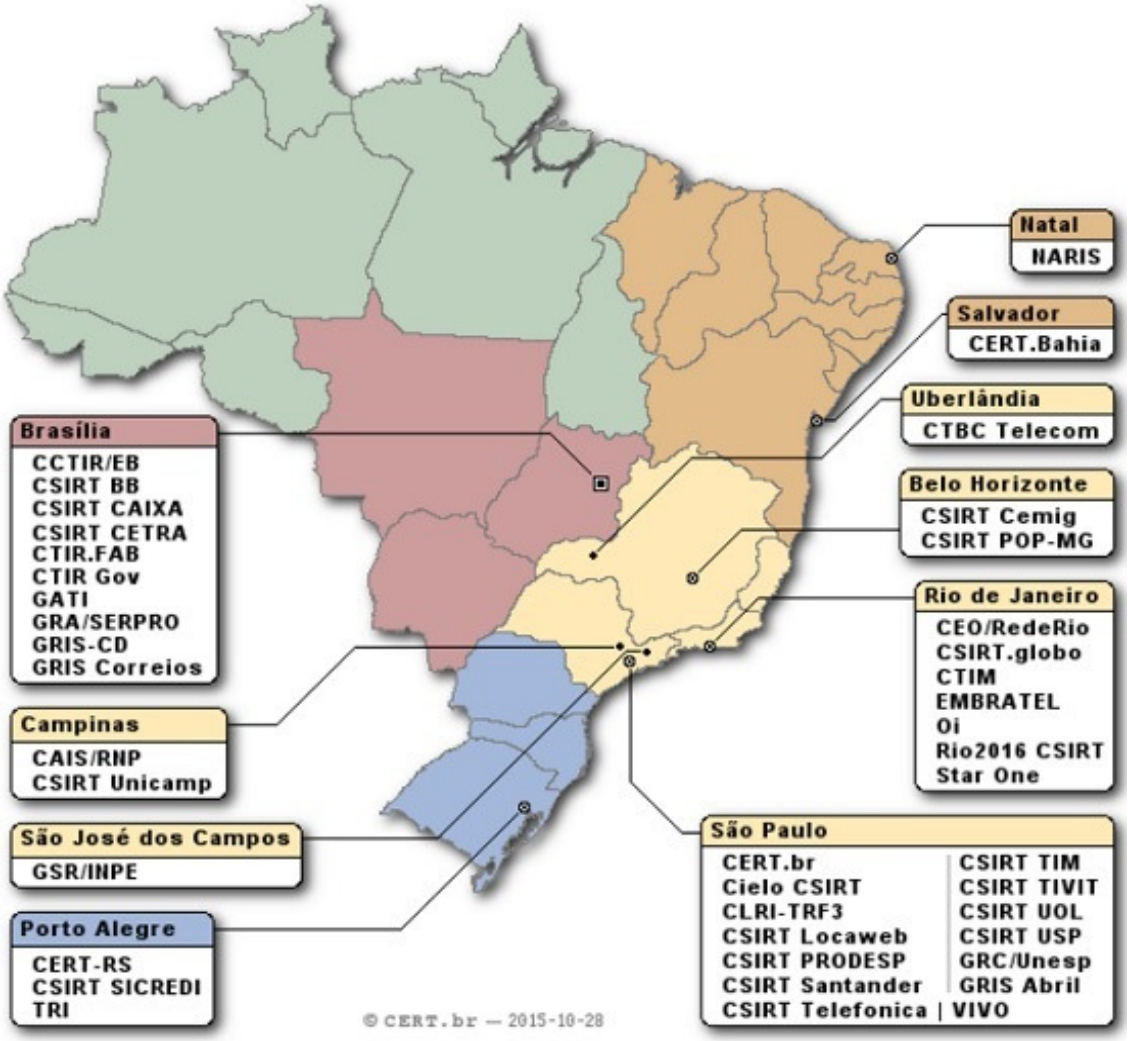
Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil.

Figura 3 – Interações do CTIR/Gov



Fonte: http://www.ctir.gov.br/sobre-CTIR-gov.html#interacoes

Figura 4 – Informações de contato de grupos de segurança brasileiros



Fonte: http://www.cert.br/csirts/brasil/

Essas atividades têm como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

As atividades conduzidas pelo CERT.br fazem parte das atribuições do CGI.br de:

> I – estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
> IV – promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
> VI – ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;

3.6.1.4.2 Agência Brasileira de Inteligência (ABIN)

A ABIN é o órgão central do Sistema Brasileiro de Inteligência – SISBIN, e é

subordinado ao GSI/PR e 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”. Atua nas vertentes inteligência e contra inteligência em prol do Estado e tem como competência, dentre outras, a que interessa especificamente ao tema deste trabalho: “Avaliar as ameaças, internas e externas, à ordem constitucional.” Em defesa e segurança cibernética, a percepção de ameaças em tempo útil permite que se construam mecanismos de defesa das redes brasileira de forma mais eficiente. Compõe ainda a estrutura da ABIN o CEPESC, que é o órgão com papel fundamental nas questões de criptografia.

3.6.1.4.2.1 Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC)

O CEPESC foi criado, em 19 de maio de 1982, para sanar a flagrante deficiência do Brasil em salvaguardar o sigilo das transmissões oficiais. Dentre outras atribuições, busca promover a pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações. Sua importância, no contexto deste trabalho, é a sua capacidade de programar soluções criptológicas construindo algoritmos de estado. Não se pode falar em segurança cibernética sem ter a capacidade de desenvolver suas próprias soluções de criptografia e de equipamentos de proteção e de transmissão de informações. Nesses tópicos, o CEPESC tem reconhecimento nacional.

3.6.1.5 Ministério da Defesa (MD) e Forças Armadas

O MD tem como missão exercer a direção superior das Forças Armadas e relaciona em sua página eletrônica vinte e três tecnologias de interesse da defesa nacional, dentre as quais se destacam como pertinentes ao presente trabalho:

a) fusão de dados;

b) sistemas de informação;

c) inteligência de máquinas e robótica;

d) sensores ativos e passivos;

e) controle de assinaturas; e

f) integração de sistemas.

Da estrutura do Ministério da Defesa, destacam-se a Marinha do Brasil, o Exército brasileiro e a Força Aérea Brasileira:

3.6.1.5.1 Marinha do Brasil (MB)

A MB já possui órgãos específicos para tratar do assunto em questão. Além do Estado-Maior da Armada e do Centro de Inteligência da Marinha (CIM), a MB conta com o Centro de Apoio a Sistemas Operativos (CASOP), que possui pessoal altamente especializado inclusive em atividades de guerra eletrônica (conforme consta de suas missões em sua página eletrônica), além do Centro de Análises de Sistemas Navais (CASNAV), cuja missão tem plena correlação com o desenvolvimento de uma doutrina de defesa cibernética.

3.6.1.5.2 Exército Brasileiro (EB)

O EB, além do Estado-Maior do Exército (EME) e do Centro de Inteligência do Exército (CIE), conta com o Departamento de Ciência e Tecnologia (DCT), um órgão de direção setorial que engloba determinados vetores de modernidade. Ao referido Departamento subordinam-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. Há ainda o Grupo Finalístico de Segurança da Informação, grupo este constituído por militares de organizações militares distintas e que tem diversas atribuições em instruções reguladoras do EB que tratam de segurança da informação.

Dando destaque ao estabelecido pela END, o Exército Brasileiro conta com o Comando de Defesa Cibernética CDCiber, principal centro de atividade de Defesa Cibernética para estrutura do Estado Brasileiro.

3.6.1.5.3 Força Aérea Brasileira (FAB)

A FAB, além do Estado-Maior da Aeronáutica (EMAER) e do Centro de Inteligência da Aeronáutica (CIAER), conta com o Centro de Estudo e Avaliação da Guerra Aérea (CEAGAR) e Centro de Computação da Aeronáutica (CCA). Assim como o IME no EB, a Força Aérea dispõe de um centro de excelência na área de ensino e pesquisa que é o Instituto

Tecnológico da Aeronáutica (ITA).

3.6.1.6 Ministério da Justiça (MJ)

O MJ tem por missão garantir e promover a cidadania, a justiça e a segurança pública, através de uma ação conjunta entre o Estado e a sociedade. Tem como área de competência, dentre outros, os seguintes assuntos que interessam ao escopo deste trabalho: Polícia Judiciária e Prevenção e repressão à lavagem de dinheiro e cooperação jurídica internacional. Da estruturado Ministério da Justiça, destaca-se a Polícia Federal.

3.6.1.6.1 Polícia Federal (PF)

A PF é órgão permanente, organizado e mantido pela União, conforme o texto constitucional, e tem as seguintes atribuições:

a) apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;

b) prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência;

c) exercer, com exclusividade, as funções de Polícia Judiciária da União.

Do texto constitucional extrai-se que a PF está vocacionada para o emprego na repressão a crimes que atentem contra “bens, serviços e interesses da União”.

Acerca de participar da estratégia de segurança e defesa do espaço cibernético brasileiro, outros órgãos poderiam ser relacionados. Na verdade, em uma leitura mais ampla, todos os órgãos e entidades, todos os servidores públicos federais, todas as empresas públicas ou privadas pertencentes a setores que compõem o que se convencionou chamar de infraestrutura crítica do Estado brasileiro podem estar aqui listados. Não se constrói uma estratégia de segurança cibernética sem a participação de todos os usuários de um determinado espaço cibernético, aqui inclusas pessoas físicas e jurídicas. Limitando a abrangência e o escopo deste trabalho, apontamos apenas alguns órgãos públicos diretamente envolvidos com a questão, enfatizando que todos são importantes, devendo estar presentes na

construção real dessa estratégia de segurança e defesa cibernética para o Estado brasileiro.

O Quadro 4 resume a participação dos atores listados quanto ao seu papel na estratégia de defesa e de segurança cibernética e que ação se espera deles.

Quadro 4 – Participação dos atores

Órgão	Papel			Ação		
Nome/Subordinação	Estratégico	Tático	Operacional	Preventiva	Repressiva	Defensiva
CND / Constituição	X			X	X	X
CREDEN	X	X		X	X	X
Casa Civil – CC	X			X		
ITI / CC		X		X		
DIRTI / CC			X	X		
DITEL / CC			X	X		
GSI	X	X		X		X
DSIC / GSI		X	X	X		
CTIR/DSIC/GSI		X	X	X	X	
ABIN / GSI			X	X		X
DEFESA - DF	X					X
MARINHA / DF	X	X	X			X
EXERCITO / DF	X	X	X			X
FAB / DF	X	X	X			X
MJ		X	X	X	X	
PF / MJ		X	X	X	X	

Fonte: MANDARINO JR, 2009.

De forma esquemática, o papel de cada ator é subdividido em três níveis:

a) estratégico, em que se espera que o ator construa diretrizes que servirão de guia para os demais órgãos atuarem em caso de uma necessidade;

b) tático, em que se espera que o ator, de posse das diretrizes desenhadas anteriormente, possa desenvolver ações de segurança e de defesa cibernética;

c) operacional, em que se espera que o ator aqui enquadrado possa desenvolver as ações estabelecidas.

Quanto às ações que se espera de cada ator, essas também se encontram subdivididas em três níveis, sendo que as preventivas e repressivas dizem respeito à segurança cibernética, ou seja, crimes cometidos por computador, ações de quadrilhas organizadas e terrorismo cibernético que não caracterizem uma guerra cibernética. A guerra cibernética, nesse caso, está representada por ações de defesa, representando a tradição brasileira que envolve tanto ações defensivas como ofensivas.

Com um pouco mais de detalhes, espera-se que:

a) ação preventiva: os atores protejam suas redes, desenvolvendo ações de capacitação de seu pessoal, que tenham submetido os seus ativos a um processo de gestão de risco e que tenham plano de contingência, por exemplo;

b) ação repressiva: desenvolvam-se as vertentes de detecção e detenção; na detecção cabe ao ator, valendo-se de seus conhecimentos, impedir que um ataque cibernético prospere nas redes nacionais, agindo em conjunto com outros centros de resposta a incidentes, para identificar o agressor e repassar a informação para a Policia Federal.

   Na detenção, cabe à Polícia Federal atuar em qualquer ação que se caracterize como ilícito contra as redes da Administração Pública Federal;

c) ação defensiva: os atores irão atuar em função de uma guerra cibernética.

Nota-se que os órgãos CDN e CREDEN aparecem nas ações nos três níveis, apesar de não serem entidades operacionais. Isso se deve, pelo entendimento do autor, ao fato de que, em qualquer ação que cause um sério impacto nas redes da Administração Pública Federal ou nas infraestruturas críticas do Estado Brasileiro, essas instâncias sejam mobilizadas e passem a atuar de forma permanente, em suas funções de órgãos de consulta da mais alta autoridade do país.

3.7 SEGURANÇA E DEFESA CIBERNÉTICA

A assertiva de Fernandes (2012) sobre a influência da cibernética em determinadas áreas do conhecimento como a informática ou ciência da computação fica bem clara com o advento da sociedade da informação, na qual o conceito de redes de computadores controlando e se comunicando com outras redes gera efeitos no mundo físico.

De acordo com o Glossário das Forças Armadas, o termo segurança pode ser entendido como:

> Condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. (BRASIL, 2015).

O termo defesa deve ser entendido como “o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança” ou ainda a “reação contra qualquer ataque ou agressão real ou iminente”.

Considerando que um dos objetivos da defesa é "recompor a condição reconhecida como segurança", pode-se concluir que as atividades de segurança e defesa são complementares, tendo essa última uma postura mais enérgica em relação à anterior. Derivando os conceitos de segurança e defesa ao espaço cibernético, teremos os conceitos de segurança cibernética e defesa cibernética.

Ambos os conceitos compõem a Segurança do Espaço Cibernético Brasileiro e requerem a definição de uma estratégia para serem implementadas de forma coordenada. Cabe ao CDN a formulação da estratégia de defesa cibernética.

A estratégia de segurança cibernética pode ser entendida como: "a arte de utilizar o espaço cibernético pela adoção de ações que assegurem disponibilidade, integridade, confidencialidade e autenticidade das informações de interesse do Estado brasileiro".

A segurança do espaço cibernético brasileiro na visão do presente trabalho tem por missão resguardar a interação entre órgãos vinculados à APF brasileira, bem como suas manifestações individuais no campo do ciberespaço, permitindo a produção de conhecimento de inteligência para aperfeiçoar o processo decisório em nível estratégico.

Ao contrário da proposta apresentada no Quadro 4, em que se expunha a atuação de cada um dos membros da APF na questão cibernética de segurança e defesa, o modelo acima nos revela a interação de informações entre estes agentes e a tênue fronteira entre segurança e defesa no espaço cibernético. Repare-se que as informações sobre incidentes (prevenção) são comunicadas à repressão, representada pela Policia Federal (seta menor à esquerda), e são também encaminhada a uma nova entidade, identificada como P&D – CEPRSC / FFAA (seta de dupla direção). Essa entidade é um laboratório de análise de malware para o qual as informações sobre os incidentes são encaminhadas para estudo e propostas de soluções para neutralização (por isso, as duas direções da seta). A seta pontilhada indica que o conhecimento adquirido nesse laboratório para a prevenção de acidentes pode gerar conhecimento para a construção de produtos que podem ser usados em caso de um conflito cibernético.

> Não tenho dúvidas, por exemplo, de que a proteção de estruturas críticas do país – usinas hidroelétricas, linhas de transmissão, bases de dados do sistema financeiro, para não falar dos próprios meios das Forças Armados – pertencem à Defesa. A identificação e perseguição de *hackers* ou *crackers* é tarefa da Segurança [pública]. **Mas há áreas cinzentas entre uma e outra**. (AMORIM, 2012, grifo nosso).

Figura 5 – Modelo de segurança e defesa no espaço cibernético brasileiro

Fonte: MANDARINO JR, 2011.

Ao seu exame, percebe-se que o uso do conhecimento está direcionado para uma nova entidade DCI/FFAA, outra instância formada pelo Departamento de Contra Inteligência da ABIN e por frações específicas do Ministério da Defesa, por intermédio das Forças Armadas, com foco nas ações de defesa. O aprofundamento das relações entre esses atores está fora do escopo deste trabalho.

3.8 RESPONSABILIDADES, POLÍTICAS E ESTRATÉGIAS NO ESPAÇO CIBERNÉTICO DO BRASIL

A segurança no âmbito cibernético contempla ações que compreendem aspectos e atitudes tanto preventivas quanto repressivas, enquanto defesa cibernética refere-se a ações operacionais, de caráter ofensivo, caracterizadas por ataques cibernéticos (nesse sentido, claramente composto por elementos estatais). Sendo assim, apesar de algumas diferenças conceituais, não se pode isolar completamente um conceito do outro.

Existe uma interligação de atribuições em relação ao setor cibernético que demanda atuação tanto em nível de defesa quanto no de segurança, haja vista que no meio cibernético a origem é de difícil determinação e os meios utilizados e os danos prováveis de um ataque podem atingir tanto sistemas militares como também serviços públicos da sociedade (CANONGIA, 2009, p. 98).

Dessa forma, no Brasil, o Gabinete de Segurança Institucional da Presidência da

República (GSI/PR) e o Ministério da Defesa (MD) – acompanhado ainda pela Secretaria de Assuntos Estratégicos, pela Marinha do Brasil, pela Força Aérea Brasileira e, pelo Exército Brasileiro (catalizador do assunto conforme indicado no Tópico CT&I, Item2, p. 37 da Estratégia Nacional de Defesa) – atuam na condução das políticas, debates públicos e projetos do setor cibernético para o país. No tocante à segurança pública, a identificação de hackers em território nacional, por exemplo, fica sob responsabilidade da Polícia Federal (PF) – subordinada ao Ministério da Justiça – como atributo de crime comum. Ou seja, a PF estaria encarregada por ações de prevenção de incidentes e de repressão também no âmbito cibernético. No entanto, se levarmos em consideração a participação das Forças Armadas (Exército) nas ações de segurança cibernética em grandes eventos que ocorreram no país, tais quais a Conferência Rio+20 em 2012, Copa das Confederações em 2013 e Copa do Mundo em 2014, notamos uma situação nebulosa, isto é, uma sobreposição de atribuição de funções em operações "não guerra".

Dessa forma, o GSI/PR e o MD destacam-se na construção de um ambiente politizado que caminha para a securitização da cibernética, tornando-se os líderes na elaboração das diretrizes desse setor. Nesse sentido, o GSI/PR tem como uma de suas funções coordenar a inteligência e a segurança da informação, transformando-a na engrenagem principal para a organização da estratégia da segurança cibernética no país (MANDARINO JR., 2009). Da estrutura do GSI/PR, destacam-se o DSIC e a ABIN.

O DSIC tem como atribuições, entre outras, regulamentar a segurança da informação e comunicações para toda a Administração Pública Federal (APF), realizar acordos internacionais de troca de informações sigilosas, ser o ponto de contato com a Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético e manter o centro de tratamento e resposta (CERT.br) a incidentes nas redes de computadores da APF. A ABIN atua nas tarefas de inteligência, por meio da produção de conhecimentos sobre fatos e situações de imediata ou potencial influência no processo decisório, na ação governamental, sobre a salvaguarda e sobre a segurança da sociedade e do Estado; e nas atividades de contrainteligência pela adoção de medidas que protejam os assuntos sigilosos relevantes para o Estado e a sociedade e que neutralizem ações de inteligência executadas em benefício de interesses estrangeiros.

A construção da securitização cibernética não ocorre tão somente por documentos legais e criação de órgãos da APF, mas também por meio de discursos públicos.

Primeiramente, durante a 68ª Assembleia Geral das Nações Unidas, em discurso de abertura, a então presidente do Brasil Dilma Rousseff proferiu as seguintes palavras:

> As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países (Discurso da Presidente, Dilma Rousseff, na abertura do Debate Geral da 68ª AGNU, 2013).

Percebe-se, nesse caso, a conclamação internacional para a construção de uma governança[35] global da Internet e uma real preocupação com os riscos de um ataque cibernético, especialmente quando coloca os sistemas e infraestruturas como objetos de referência e, portanto, como algo existencialmente ameaçado. O discurso da presidente ainda demonstrou preocupação com a privacidade e os dados pessoais dos cidadãos brasileiros, alvo de espionagem pela agência americana National Security Agency (NSA) em 2013, colocando, então, também a sociedade brasileira como um objeto referencial.

Ademais, o fato gerador provocado pelo incidente de violação de segurança cibernética foi estopim e motivador para que, em 2014, fosse aprovado o Marco Civil da Internet, projeto que estava com pauta de votação trancada desde sua criação em 2009. Ainda que não tenha propriamente fins de defesa ou segurança nacional, a Lei Ordinária de nº 12.965, de 23 de abril de 2014, regula a utilização da Internet no país, prevendo princípios, garantias, direitos, responsabilidades e deveres para usuários e empresas, tratando de neutralidade, privacidade, retenção de informações e dados, entre outros. Portanto, esse Marco Civil representa uma importante regulamentação interna e, igualmente, uma abertura ainda maior da discussão do tema para a sociedade.

Ainda, na apresentação do *Livro Verde*: Segurança Cibernética no Brasil (BRASIL, 2000), o então Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República, Jorge Armando Felix, não só defende a necessidade de garantir a segurança nacional, como também estabelece a formulação de uma Política Nacional de Segurança Cibernética, expressando o tema como uma ameaça à segurança estatal:

> Assim, motivado por esta missão e considerando a necessidade de assegurar dentro

[35] "Governança é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios." In: PERES, João Roberto. A vez da governança corporativa. *Revista Abinee*, n. 43, p. 25, out. 2007. Disponível em: <http://www.abinee.org.br/informac/revista/43j.pdf>. Acesso em: 16 ago. 2016.

> do espaço cibernético ações de segurança da informação e comunicações como fundamentais para a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação; a possibilidade real e crescente de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído Grupo Técnico para estudo e análise de matérias relacionadas à Segurança Cibernética. [...] Recomendo, portanto, a leitura desta obra, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Nacional, e convido-os a contribuir com propostas e sugestões para a evolução da mesma, visando formular, colaborativamente, à Política Nacional de Segurança Cibernética. (LIVRO VERDE, 2000, p. 5-6).

Ao final de suas palavras, percebemos uma chamada pública para que haja contribuições com propostas e sugestões, levando o tema mais uma vez para a esfera pública. Em relação ao papel do MD, num primeiro momento, a condução do setor cibernético no país foi designada ao Exército Brasileiro; havendo previsibilidade para a criação de um Comando de Defesa Cibernética das Forças Armadas – como acontece nos EUA com a USCYBERCOM[36] – no qual Marinha, Exército e a Força Aérea trabalhariam integradamente.

Segundo a END, "o Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nas áreas cibernética, espacial e nuclear" (BRASIL, 2008), colocando particular ênfase no "aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos" (BRASIL, 2008). Nota-se pelo documento, portanto, que a cibernética é colocada pela primeira vez como um setor decisivo para a conservação do país ao alegar que os "três setores estratégicos – o espacial, o cibernético e o nuclear – são essenciais para a defesa nacional" (Estratégia Nacional de Defesa. Decreto nº 6.703, De 18 de Dezembro de 2008).

Mesmo assim, como consequência da END de 2008, em 9 de novembro de 2009, o MD, por meio da Diretriz Ministerial 14, determinou as responsabilidades de coordenação e integração do setor cibernético ao Exército Brasileiro, no âmbito das Forças Armadas.

Em seguida, em 2010, foi lançado o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (BRASIL, 2010a), elaborado e organizado por especialistas de 13 órgãos da APF, propondo como objetivos gerais:

a) levantar e avaliar as potenciais vulnerabilidades e riscos que possam vir a afetar a segurança das infraestruturas críticas, identificando e monitorando suas

[36] United States Cyber Command (USCYBERCOM) é um comando conjunto das forças armadas norte-americanas subordinado ao Comando Estratégico dos Estados Unidos da América. O comando está localizado em Fort Meade, Maryland, e centraliza as operações no ciberespaço, organiza os recursos cibernéticos existentes e sincroniza defesa de redes militares dos EUA.

interdependências;

b) propor, articular e acompanhar medidas necessárias das infraestruturas;

c) estudar, propor e acompanhar a implementação de um sistema de informações com dados atualizados das infraestruturas; e

d) pesquisar e propor um método de identificação de alertas e ameaças da segurança de infraestruturas críticas da informação.

Nesse caso, percebe-se novamente uma preocupação extremada com as infraestruturas críticas do país, colocando-as como uma ameaça existencial. Ainda em 2010, foi lançado o *Livro Verde*: Segurança Cibernética no Brasil (BRASIL, 2010b), o qual apresenta uma breve visão do país no que se refere às oportunidades e aos desafios em termos político-estratégicos, econômicos, sociais e ambientais, ciência, tecnologia e inovação, educação, legalidade, cooperação internacional, e segurança das infraestruturas críticas, tendo como foco central a segurança cibernética. Além do mais, contém diretrizes estratégicas para a formulação de uma possível futura Política Nacional de Segurança Cibernética para o país (BRASIL, 2010b, p. 17,33).

Mais tarde, em 2012, é elaborado o documento que pela primeira vez aloca publicamente recursos para o setor cibernético. O *Livro Branco de Defesa Nacional* (BRASIL, 2012a) – que, apesar de aprovado na Câmara dos Deputados e no Senado, mas ainda não sancionado, é documento disponível no site do governo brasileiro – trata a cibernética como um desafio, denominando-a com um tipo de "conflito do futuro" (BRASIL, 2012a, p.28), e coloca a defesa cibernética propriamente como um novo tema no plano internacional.

O livro também mira as infraestruturas do país como ameaça existencial ao afirmar que a "ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas [...] essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (BRASIL, 2012a, p. 69). O documento supracitado ainda defende que a proteção do espaço cibernético abrange variadas áreas, desde capacitação, inteligência, pesquisa científica, preparo e emprego operacional e gestão de pessoal até a proteção dos próprios ativos e capacidade de atuação em rede.

Outra publicação importante concernente ao tema em âmbito brasileiro foi a Política Cibernética de Defesa de 2012. A finalidade da Política é nortear "as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos" (Política Cibernética de Defesa. Portaria nº

3.389/MD, de 21 de dezembro de 2012).

Esse documento solidifica o entendimento acerca das possibilidades e dos limites da atuação cibernética brasileira, tendo em vista a sensibilidade que esse espaço e ferramenta de poder possui. Mais uma vez, para além da atuação do MD, a audiência pública é chamada para colaborar com processo de construção do setor cibernético:

> a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa; (Política Cibernética de Defesa. Portaria nº 3.389/MD, de 21 de dezembro de 2012).

O documento cita o Sistema Militar de Defesa Cibernética (SMDC), órgão militar com o intuito de prevenir ataques aos sistemas de informática de todo o Brasil, o qual é coordenado pelo Estado-Maior das Forças Armadas. Dessa forma, o país insere-se no modelo de gestão cibernética das grandes potências, ainda que apenas inicialmente.

Por fim, tem-se a Estratégia Nacional de Defesa de 2012, sendo uma atualização da END 2008. O último documento possui alguns pontos atualizados importantes que merecem ser citados. Primeiramente, nessa nova estratégia o setor cibernético adquire uma seção exclusiva para apontamento de prioridades. Uma delas é expandir o CDCiber, comandado pelo Exército, para um comando maior de atuação integrada das Forças Armadas, ao afirmar que se deve "fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas" (BRASIL, 2012c). Outra prioridade é conduzir o tema para o debate acadêmico ao propor a necessidade de "fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional" (BRASIL, 2012c). Inclusive, nesse ponto, propõe-se um estudo conjunto entre Ministros, Secretários e GSI/PR com vistas à "criação da Escola Nacional de Defesa Cibernética" (Estratégia Nacional de Defesa de 2012, 2012c).

A Estratégia de 2012 proclama a independência nacional de capacitação tecnológica autônoma, incluindo os setores espacial, cibernético e nuclear. Dessa forma, o país pretende desprender-se de tecnologia estrangeira.

Enfim, no campo da segurança cibernética, as ações ganharam maior investida a partir da criação do DSIC no GSI/PR, em 2006, e, no campo da defesa cibernética, destaque maior passou a ser dado através da elaboração da END. Os documentos aqui referidos,

acompanhados pela criação e atuação de órgãos estatais – no qual o GSI/PR[37] e o MD – possuem papel imprescindível pela atribuição de competências no que tange à segurança e defesa cibernéticas. Nesse caso, podem ser encarados como uma sistematização do processo de formação de ameaças existentes no setor cibernético.

Ponderando-se na mesma medida, os breves discursos apresentados podem ser vistos como uma forma de alcançar a legitimação da população e a aceitação pública em busca da securitização, haja vista que seu processo torna-se mais aceitável em virtude da associação entre possíveis ataques cibernéticos em âmbito nacional com os ocorridos diariamente como crime comum.

Sendo assim, conforme apontaram Buzan e Hansen (2012, p. 366), a segurança não é uma condição objetiva, mas sim um discurso que constitui identidades e ameaças. Nesse caso, parece claro o desenvolvimento, ainda que em prosseguimento, das identidades e ameaças cibernéticas, levando a uma securitização ainda incompleta do setor no país.

3.9 A QUESTÃO CIBERNÉTICA NO BRASIL: POLITIZAÇÃO *VERSUS* SECURITIZAÇÃO

Nesta etapa do trabalho, trataremos o espaço cibernético brasileiro com um enfoque voltado aos seus marcos legais e a evolução do tema pelo Estado onde nos questionamos se ele eleva o tema para um modelo securitizado.

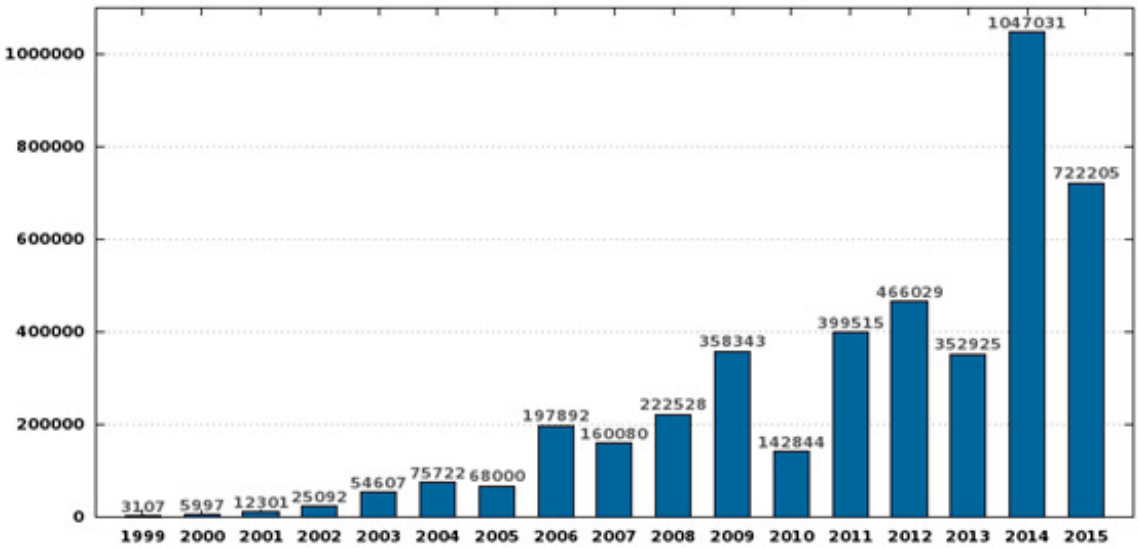
De acordo com o Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br), o Brasil possui o maior número de internautas da América Latina, cerca de 50 milhões. Em 2013, o CERT.br recebeu notificações de 352.925 tipos de ataques no país, número que chegou a alcançar 466.029 em 2012. Comparando-se com o relatório de 2002, quando se reportou pouco mais de 25.000 ataques, os incidentes cibernéticos tiveram um aumento superior a 1.800% em uma década.

Isso demonstra o crescimento vertiginoso não só de usuários de Internet no país, como também na quantidade e diversificação dos ataques virtuais, conforme constatado no Gráfico 1 a seguir. Ainda de acordo com as estatísticas de 2015, advindas no Gráfico 2, os incidentes reportados partiram majoritariamente de dentro do território nacional (54,02%), seguido por EUA (11,16%) e, depois, China (10,59%).

---

[37] O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) deu lugar à Casa Militar sob o Ministério da Casa Civil, conforme a Medida Provisória Nº 696 de 2 de Outubro de 2015.

Gráfico 1 – Total de incidentes reportado ao CERT.br por ano (1999 - 2015)

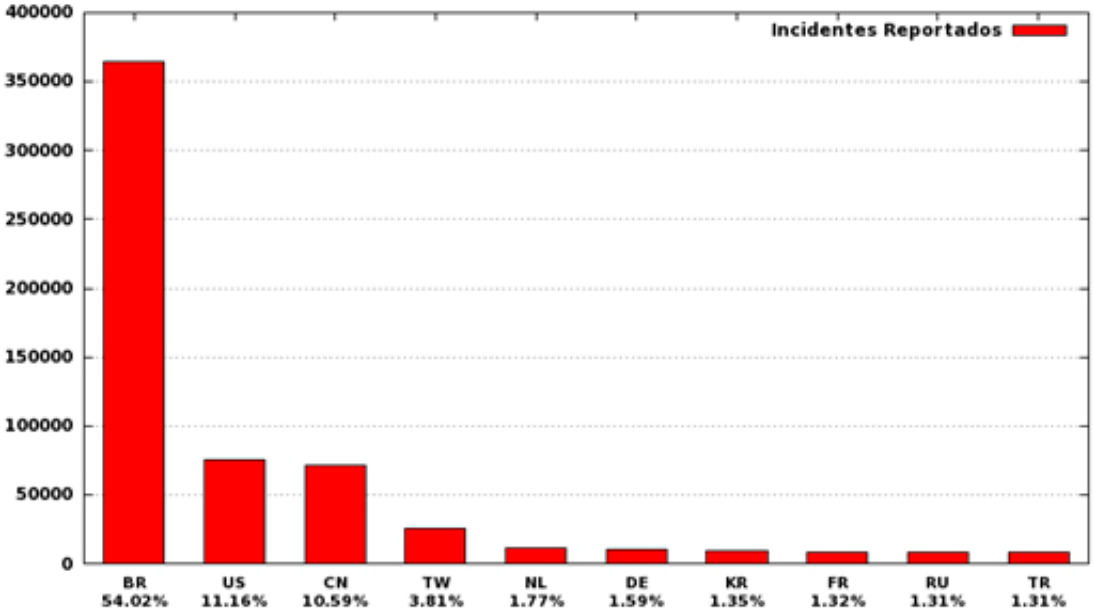


Fonte: http://www.cert.br/stats/incidentes/

Assim:

> a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos e ao número de usuários, observados, especialmente, ao longo dos últimos anos. (LIVRO VERDE, 2010, p. 31).

Gráfico 2 – Incidentes reportados ao CERT.br - Top 10 CCs origem de ataques



Fonte: http://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.png

Em 2011, os incidentes reportados pelo Centro tinham como alvo, preferencialmente, empresas privadas e bancos. Já nos anos seguintes, os ataques estenderam-se para sites e

sistemas governamentais, entre eles os sites da Presidência da República e da Receita Federal. Essa situação revela uma potencial preocupação com a fragilidade do sistema de segurança cibernética do governo brasileiro. Por exemplo, um ataque que paralisasse o site da Receita Federal às vésperas do prazo de entrega das declarações de imposto de renda do cidadão brasileiro poderia trazer grandes prejuízos tanto para o governo quanto para o cidadão.

Portanto, fazem-se necessárias uma categorização e tipificação das várias formas de conflito no ciberespaço, das possíveis vulnerabilidades, das ameaças e de suas fontes, "para que sejam alocadas responsabilidades aos cidadãos, ao Estado; sejam estabelecidas contramedidas e investigações criminais" (DUNN, 2010, p. 1, tradução nossa).

Ainda que não se comprove que o tema não tenha sido totalmente securitizado no Brasil, pode-se dizer que a cibernética é objeto de preocupação no âmbito da segurança e da defesa. Nesse caso, a securitização, de acordo com Hansen e Nissenbaum (2009), é um processo em construção no âmbito das práticas de segurança diárias (politização). Assim, a cibernética tornou-se um tema relevante para o governo brasileiro, conforme revelado pelo ex-ministro da Defesa, Celso Amorim:

> Ao contrário de cem anos atrás, tempo do Barão do Rio Branco, quando o Brasil comprava do exterior praticamente todos seus principais equipamentos de defesa sem a capacidade de nacionalizar sua produção, hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política. A Estratégia Nacional de Defesa, cuja segunda edição foi lançada no ano passado e agora acaba de ser apreciada pelo Congresso Nacional, define três áreas prioritárias desse esforço: a nuclear, **a cibernética** e a espacial. (2013, p. 308-309, grifo nosso).

No âmbito militar brasileiro, há uma clara preocupação com a segurança e defesa cibernética dos sistemas virtuais e de infraestrutura do país. A política adotada pelas Forças Armadas brasileiras é a de defesa-ativa[38], onde não se busca atacar outras nações seguindo a linha pacifista histórica de posicionamento e obediência direta ao texto constitucional em seu artigo 4^0 incisos I a VII, visando primordialmente proteger os próprios sistemas e neutralizar possíveis ataques e intrusões.

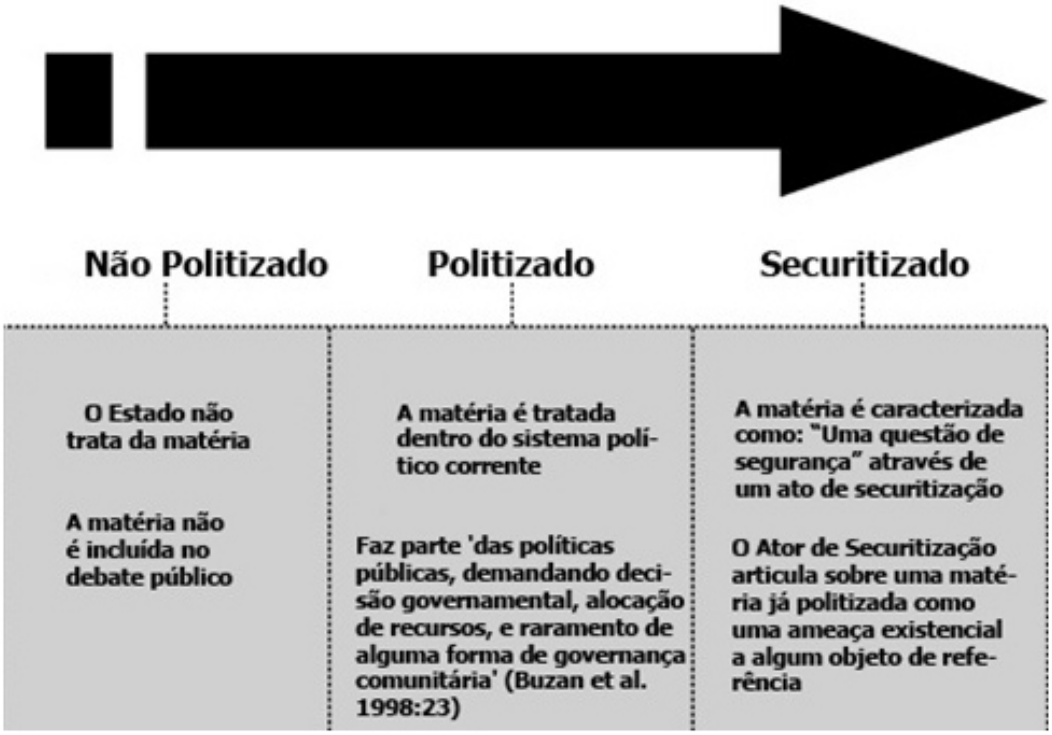
Levando-se em consideração a elaboração de Buzan et al. (1998) referente à categorização do tratamento de questões públicas, podemos dividir o tratamento da segurança cibernética pelo Brasil em três etapas: até os anos 2000 (não politizado); na primeira metade

[38] Defesa-ativa: capacidade de identificar o ataque cibernético e sua origem e na mesma medida, se oportuno for, retaliar o atacante e seus sistemas.
Disponível em: <https://gestao.consegi.serpro.gov.br/cobertura/noticias/a-favor-de-uma-defesa-ativa-contra-ataques-ciberneticos>. Acesso em: 16 ago. 2016.

dos anos 2000 (politizado); e a partir de 2008 (em processo de securitização).

Levando-se em consideração a elaboração de Buzan et al. (1998) referente à categorização do tratamento de questões públicas, podemos dividir o tratamento da segurança cibernética pelo Brasil em três etapas: até os anos 2000, não politizado; na primeira metade dos anos 2000, politizado; e, a partir de 2008, em processo de securitização, conforme se ilustra na Figura 6.

Figura 6 – Evolução no processo de securitização



Fonte: Contemporary Security Studies, p. 170[39].

Até o final dos anos 1990, não foram criados documentos relevantes concernentes ao tema nem debates ou preocupações quanto aos riscos e às vulnerabilidades foram notados, certamente pelo fato de a cibernética e seus elementos encontrarem-se em processo de formação e evolução, juntamente com as Tecnologias de Informação e Comunicação (TICs). A partir de então, conforme o Estado Brasileiro percebe a necessidade e a importância de tal tecnologia, há uma institucionalização da questão, designação de capacidades e demarcação de conceitos.

Então, no ano 2000, tem-se o marco inicial do processo de politização do tema com o *Livro Verde*: Sociedade da Informação no Brasil (BRASIL, 2010b), do Ministério da Ciência e

[39] COLLINS, Alan. *Contemporary Security Studies*. Oxford University Press, 12 jan. 2016.

Tecnologia. O livro representa uma visão mais ampla para estabelecer contornos e diretrizes de um programa de ações rumo à sociedade da informação no Brasil.

O programa versa sobre as oportunidades e os riscos de uma sociedade em rede e informatizada; sobre economia, trabalho e comércio eletrônico; sobre universalização dos serviços de Internet como forma de cidadania; sobre como a informatização auxilia a educação; sobre transparência governamental para colocar o "governo ao alcance de todos", além de abordar questões mais específicas de P&D e infraestrutura avançada. Basicamente, são definidos conceitos ligados à informática e são propostos projetos de disseminação da Internet pelo território nacional.

Em termos de segurança cibernética (até então denominado segurança da informação), no mesmo ano, o governo publicou o Decreto nº. 3.505, de 13 de junho de 2000, instituindo a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal. A legislação federal instituiu o Comitê Gestor da Segurança da Informação (CGSI), o qual serve de assessor e é subordinado à Secretaria-Executiva do Conselho de Defesa Nacional, portanto, nota-se uma preocupação inicial com a segurança da informação do Estado.

Em seguida, através da Lei Federal nº 10.683, de 28 de maio de 2003, cria-se o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Assim sendo, até 2005, há um processo de politização do tema da segurança cibernética – inicialmente tecnicamente entendido como segurança da informação –, com a criação de órgãos, documentos oficiais, discussões, centros de estudos, determinação de recursos etc. Então, o tema ainda não havia escalado um grau de preocupação concernente a uma ameaça existencial propriamente dita, mas apenas um objeto de preocupação inicial e de debate político. Doravante, há um processo de entendimento da cibernética como uma ameaça, se não plenamente existencial ao menos potencialmente existente e, portanto, em construção da securitização.

Nesse sentido, a Política Nacional de Defesa (Decreto nº 5484, de 30 de junho de 2005) menciona brevemente o tema em duas seções. Dessa forma, temos as primeiras citações diretas referentes a um ataque cibernético:

> 6.19 Para minimizar os danos de possível ataque cibernético, 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. [...] XII - aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso permita seu pronto restabelecimento. (Política de Defesa Nacional. Ministério da Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 5484, de 30 de Junho de 2005).

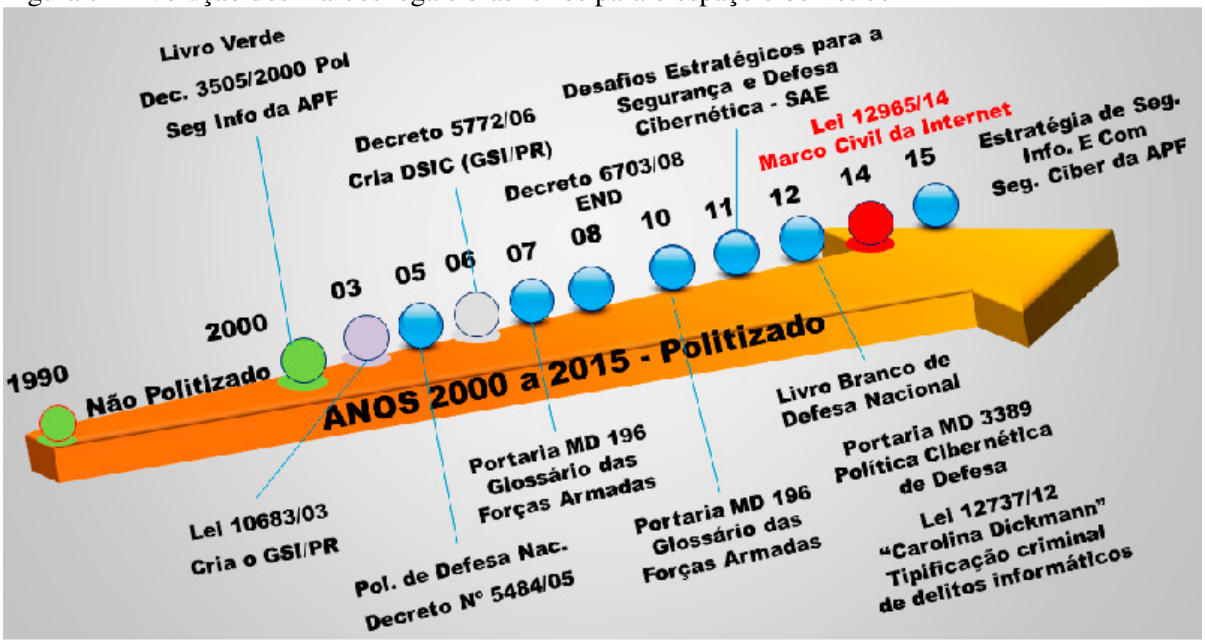
A partir dessa Política Nacional de Defesa (BRASIL, 2013), ampliam-se as produções de documentos legais brasileiros, os quais fomentam o debate público de Defesa Nacional, incluindo, então, a segurança cibernética; sendo eles o Glossário Militar das Forças Armadas (2015), a Estratégia Nacional de Defesa[40] (2008 e rev. 2012), o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (BRASIL, 2010), o *Livro Verde*: Segurança Cibernética no Brasil (BRASIL, 2010b), o relatório Desafios Estratégicos para a Segurança e Defesa Cibernética (2011), o *Livro Branco de Defesa Nacional* (BRASIL, 2012), a Política Cibernética de Defesa (BRASIL, 2012) e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (BRASIL, 2015).

A consequência é a percepção pelo Estado brasileiro da potencialidade e dos riscos de ataques cibernéticos às infraestruturas críticas e da segurança da informação no país, alocando publicamente espaços em documentos legais que promovem a discussão e o crescimento da importância do tema, tendo o Gabinete de Segurança Institucional da Presidência da República e o Exército Brasileiro como órgãos principais de atuação no setor cibernético.

Em resumo, a Administração Pública Federal esforçou-se por apresentar a evolução da questão da segurança cibernética pelo Estado Brasileiro com um direcionamento para uma possível securitização. Temática essa que outrora, nos anos 1990, ainda se encontrava não politizada e que em consequência da maior integração da sociedade brasileira com o Espaço Cibernético, somados a eventos de ordem internacional (Stuxnet – Irã, DDos – Estônia) elevaram o tom do debate, principalmente nas forças armadas brasileiras, e perceberam, de maneira ágil, a resposta estatal, conforme ilustração da Figura 7:

[40] A Estratégia Nacional de Defesa (END) foi aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, revisada em 2012 de acordo com o Decreto Legislativo nº 373, de 25 de setembro de 2013, implicando em alterações na Política Nacional de Defesa e no *Livro Branco da Defesa*.

Figura 7 – Evolução dos marcos legais brasileiros para o espaço cibernético[41]



Fonte: Elaborada pelo autor.

[41] Lei Nº 12.737, de 30 DE NOVEMBRO DE 2012: Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Lei Nº 12.965, de 23 DE ABRIL DE 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

4 SEGURANÇA E DEFESA DO ESPAÇO CIBERNÉTICO NA MARINHA DO BRASIL

A utilização cada vez mais acentuada de informações sendo transferidas e armazenadas digitalmente, assim como a evolução tecnológica dos sistemas envolvidos, acarreta na gradativa dependência da MB de suas estruturas de comunicações e de TI, as quais têm se apresentado num grau cada vez maior de complexidade e interconexão.

Observa-se daí a necessidade de a MB possuir instrumentos que contenham diretrizes voltadas a auxiliar as Organizações Militares (OM) no planejamento, definição e implantação de mecanismos de segurança (normas, procedimentos, padrões, equipamentos, dispositivos e controles) no trato da informação digital, orientando as atividades que visam garantir a autenticidade, a integridade, a disponibilidade e o sigilo das informações armazenadas e trafegadas por meio magnético, eletrônico ou digital.

O espaço cibernético da MB apresenta um potencial de exposição a ações ofensivas à medida que a complexidade de sistemas e elementos de rede avoluma-se em suas atividades cotidianas, tornando-se um alvo de grande valor.

A preocupação com uma nova ordem de ameaças vinculadas ao domínio cibernético encontra reflexos nos mais variados extratos da Administração Pública Federal, e, no caso da Marinha do Brasil, essas considerações são expostas em documentos como as Orientações do Comandante da Marinha 2008 e 2016 (ORCOM) e também no Plano Estratégico de Tecnologia da Informação da Marinha (2016-2019).

A possibilidade de vazamento do conhecimento de projetos e pesquisas em andamento na MB, tais como o Programa de Desenvolvimento de Submarinos (PROSUB)[42] e do Laboratório de Geração de Energia Nucleoelétrica (LABGENE)[43], devido a ações maliciosas

[42] Programa de Desenvolvimento de Submarinos (PROSUB): firmado um acordo de transferência de tecnologia entre Brasil e França. O programa viabilizará a produção de quatro submarinos convencionais, que se somarão à frota de cinco submarinos já existentes. E culminará na fabricação do primeiro submarino brasileiro com propulsão nuclear. O PROSUB vai dotar a indústria brasileira da defesa com tecnologia nuclear de ponta – ponto destacado na Estratégia Nacional de Defesa. A concretização do programa fortalece, ainda, setores da indústria nacional de importância estratégica para o desenvolvimento econômico do país. Priorizando a aquisição de componentes fabricados no Brasil para os submarinos, o PROSUB é um forte incentivo ao nosso parque industrial. Além dos cinco submarinos, o PROSUB contempla a construção de um complexo de infraestrutura industrial e de apoio à operação dos submarinos, que engloba os Estaleiros, a Base Naval e a Unidade de Fabricação de Estruturas Metálicas (UFEM), no Município de Itaguaí. Disponível em: <https://www1.mar.mil.br/prosub/institucional>. Acesso em: 20 nov. 2016.

[43] Laboratório de Geração Nucleoelétrica (LABGENE): para a operação do submarino nuclear, a Marinha do Brasil está construindo, no Centro Experimental Aramar, o Laboratório de Geração de Energia Nucleoelétrica (LABGENE), que será utilizado para validar as condições de projeto e ensaiar todas as condições de operação possíveis para uma planta de propulsão nuclear. Será composto por 11 prédios principais, entre eles o Prédio do

intencionais, merecem a atenção de sua classificação como problemas de segurança nacional, conforme previsto na Estratégia Nacional de Defesa (END), sujeitos à proteção permanente a qualquer custo. (SALMON, 2015).

Nesta etapa do trabalho, os esforços se voltam para compreensão da estrutura político-administrativa da Marinha do Brasil, seu arcabouço legal e suas adaptações à Questão de Segurança e Defesa do Espaço Cibernético institucional, o qual se estende por todo o território nacional, e representações em território estrangeiro (Comissões Navais, Adidâncias e militares em missão no exterior).

4.1 RETROSPECTO DA QUESTÃO CIBERNÉTICA NA MARINHA DO BRASIL

> Hoje, a realidade mundial é muito distinta, mas igualmente insegura! Aos tradicionais atores estatais, somam-se ameaças transnacionais materializadas pelo terrorismo catastrófico; pelo crime organizado na forma do narcotráfico, do tráfico humano e da pirataria; **pela guerra cibernética**; e pelas crescentes discussões jurídicas quanto aos níveis de soberania em espaços marítimos[44]. (Marinha do Brasil, Ordem do Dia 2/2016, grifo nosso).

O mundo globalizado testemunha grandes modificações comportamentais, notadamente no que tange às relações do emprego das TIC na vida das organizações. Sua permeabilidade em todos os níveis organizacionais estabeleceu um novo paradigma: o da necessidade de alinhamento da TIC com os objetivos estratégicos das corporações.

A MB, não alheia a essa conjuntura, conforme o Boletim de Ordens e Notícias (BONO) Especial nº 748[45], dá publicidade à determinação da Alta Administração Naval para a criação de um Grupo de Trabalho em Tecnologia da Informação (GT-TI) que conta com a participação de representantes de todos os Órgãos de Direção Setorial (ODS) para elaborar um Estudo de Estado-Maior (EEM) detalhado, no qual foi revisada a Estrutura de recursos TIC na MB.

Definiram-se as atribuições e responsabilidades dos diversos atores, de forma a adaptar essa estrutura, no que for pertinente, ao adequado alinhamento com os respectivos objetivos estratégicos.

Uma diversidade de questões foi analisada no âmbito do GT-TI, desde a capacitação

---

Reator e o Prédio das Turbinas. Disponível em: <https://www1.mar.mil.br/ctmsp/labgene>. Acesso em: 20 nov. 2016.

[44] Ordem do Dia No 2/2016 – Assunto: 151º Aniversário da Batalha Naval do Riachuelo – Data Magna da Marinha, disponível em: <http://www.mar.mil.br/hotsites/11jun2016/ordem_do_dia.html>. Acesso em: 20 nov. 2016.

[45] Armada, Estado-Maior da. BONO nº 748. Boletim de Ordens e Notícias Especial, 7 nov. 2007.

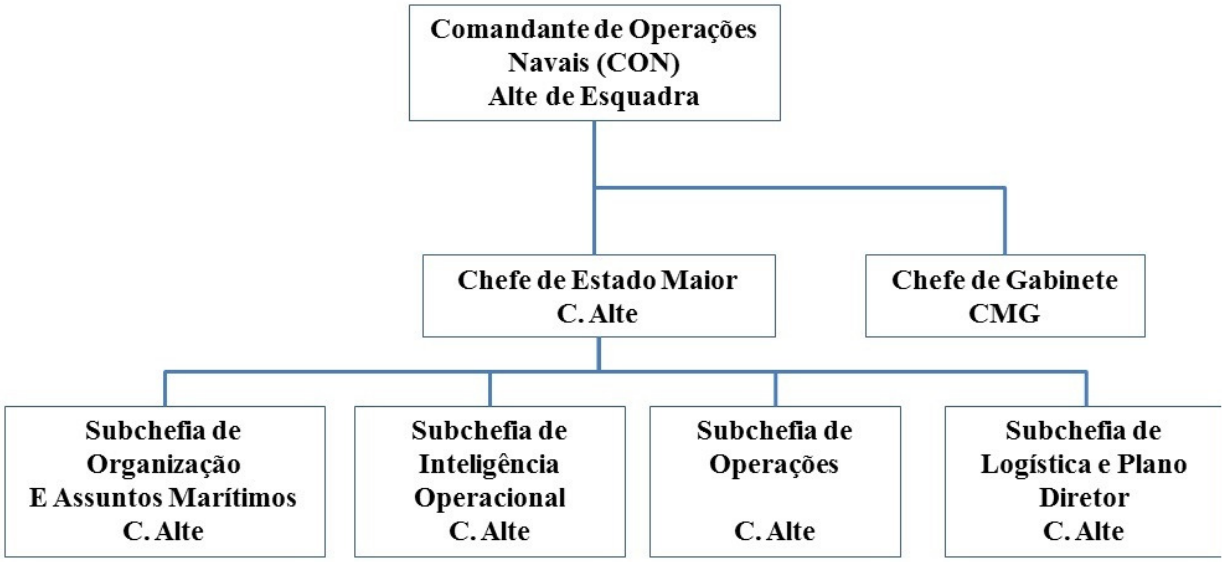
técnica de pessoal especialista até a revisão da relação de subordinação de órgãos responsáveis por atividades de TI.

Os principais pontos decorrentes do Estudo de Estado Maior resultantes do GT-TI seriam:

> Criação do COTIM, assessorado pela COTEC-TI. O COTIM é presidido pelo Chefe do Estado-Maior da Armada (CEMA - é o segundo na Cadeia de Comando na hierárquica da MB), que passa a ser a Autoridade de TI da MB, deliberando sobre os importantes temas relativos a TI, após parecer técnico elaborado pela COTEC-TI. Essa configuração é coerente com as melhores práticas de Governança de TI na atualidade, as quais são unânimes em evidenciar a necessidade de participação dos segmentos voltados para o "negócio" da empresa – no caso da MB, a manutenção do aprestamento do Poder Naval;
> Centralização das atividades de TI na futura DCTIM:
> [...]
> Normatização e estabelecimento de padrões técnicos para diversas atividades, tais como: processos de desenvolvimento e interoperabilidade de Sistemas Digitais (SD), guerra cibernética, auditoria de sistemas, bem como adesão a práticas consagradas de Governança de TI para as organizações.

Essas mudanças direcionaram a Marinha para uma nova mentalidade de uso da TIC no que diz respeito à questão de segurança e defesa cibernética, pois a primeira iniciativa do gênero foi oriunda do setor operativo (em 2006) com a criação da Seção de Guerra Cibernética no Comando de Operações Navais, que se encontrava subordinada à Subchefia de Inteligência (CON-20). (NUNES, 2010).

Figura 8 – Estrutura organizacional do ComOpNav



Fonte: Adaptado pelo autor a partir de www.comopnav.mar.mil.br.

O conhecimento que se detinha sobre o assunto era muito limitado, tanto em termos

técnicos como doutrinários, e restringia-se ao esforço de alguns poucos elementos que, por iniciativa própria, buscavam se atualizar. A cada movimentação de um desses militares, perdia-se um pouco da incipiente capacidade existente.

A partir de 2008, a Marinha do Brasil realiza uma forte guinada na maneira de tratar a questão de segurança e defesa cibernética, ao transferi-la do Setor Operativo ao Setor de Apoio, mais precisamente sob a estrutura da Diretoria-Geral de Material da Marinha (DGMM) (NUNES, 2010).

Compreende-se que a adoção de tal postura foi motivada, entre outros fatores, pela forte e natural relação que a TIC mantém com a questão de segurança e defesa cibernética, fazendo com que a competência natural para administrar a infraestrutura de dados do Poder Naval estabelecida pela IN01/DSIC/GSIPR fosse atribuída à Diretoria de Comunicações e Tecnologia da Informação da Marinha e em resposta direta aos itens b e f do EEM do GT-TI de 2007.

4.2 A DCTIM

Criada pela portaria n° 14, de 16 de janeiro de 2008, do Comandante da Marinha[46] e com sede na cidade do Rio de Janeiro, a Diretoria de Comunicação e Tecnologia da Informação da Marinha ampliou a missão da extinta DTM, para congregar em uma única Diretoria Especializada (DE) a orientação e supervisão funcional do Sistema de Comunicações da Marinha (SISCOM) e as atividades técnicas pertinentes às Telecomunicações, ambas antes exercidas pela extinta DTM, juntamente com a orientação da governança da Tecnologia da Informação na Marinha, atividades estas até então executadas concomitantemente pela DTM e pela Diretoria de Administração da Marinha (DadM).

A organização e as atividades da DCTIM foram estruturadas pelo Regulamento aprovado pela Portaria nº 98, de 16 de fevereiro de 2011, do Diretor-Geral do Material da Marinha responsável por elaborar normas, instruções técnicas e procedimentos padronizados para áreas de conhecimento concernentes ao emprego da Tecnologia da Informação na MB, incluindo a questão de Segurança e Defesa Cibernética.

Subordinada a essa Diretoria, o Centro de Tecnologia da Informação da Marinha (CTIM) foi designado como Órgão de Execução Operacional para a Guerra Cibernética (GC), sendo responsável por: operar os recursos tecnológicos para a GC; planejar os exercícios

[46] DOU de 23 de janeiro de 2008, Seção 1, p. 9.

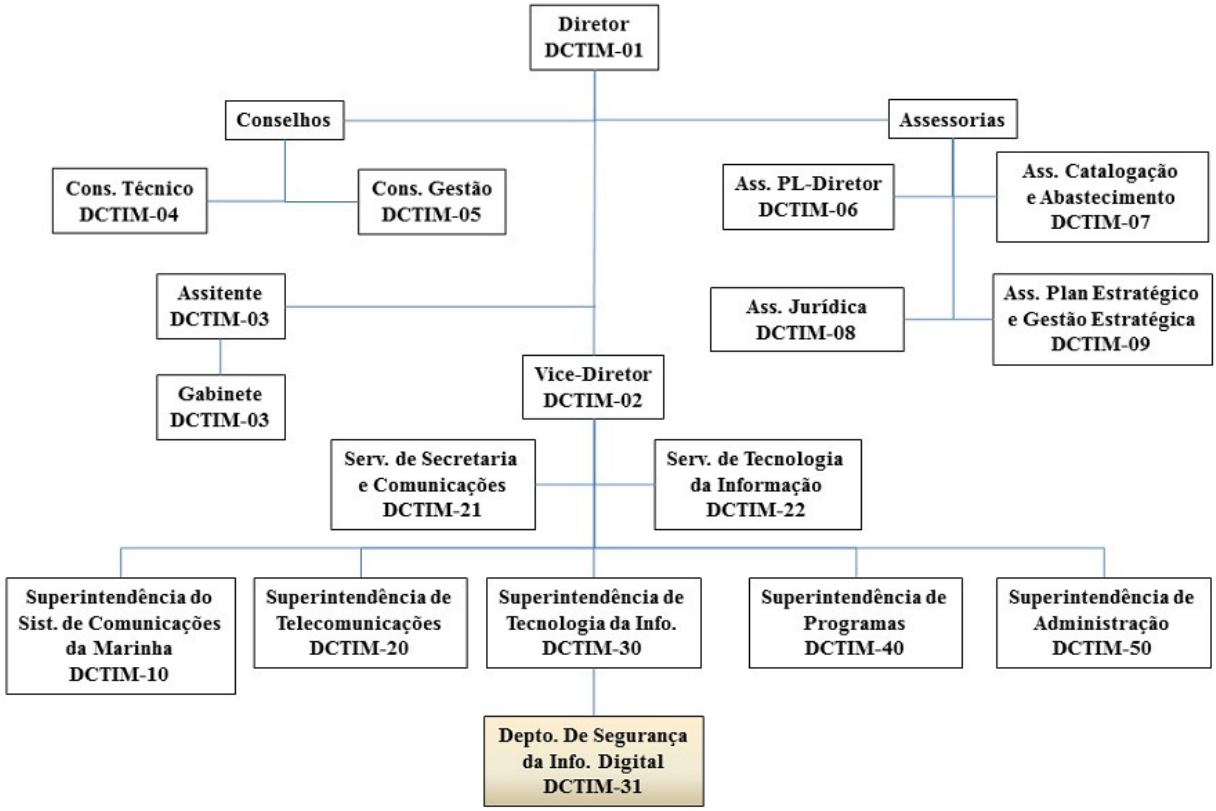
gerais de GC; subsidiar a DCTIM nos aspectos de capacitação técnica do pessoal envolvido com as atividades específicas de GC; e mobilizar pessoal qualificado, para o emprego em situações de conflito, de acordo com a doutrina estabelecida.

4.2.1 Estrutura organizacional da DCTIM

Em documento elaborado pelo Estado Maior da Armada denominado Doutrina de Tecnologia da Informação da MB (EMA-416: Doutrina de Tecnologia da Informação da Marinha, Volume I. 1ª rev. Brasília, DF: 2012), determinou-se à DCTIM:

> Elaborar normas, instruções técnicas e procedimentos padronizados para áreas de conhecimento concernentes ao emprego da Tecnologia da Informação na MB, notadamente: projetos de desenvolvimento e manutenção de sistemas digitais de informação, segurança de informação digital, auditoria computacional, criptologia, guerra cibernética, forense computacional e tecnologias de suporte à preservação digital e à gestão arquivística (MARINHA DO BRASIL, 2012, p. 3-4).

Figura 9 – Organograma da Diretoria de Comunicação e Tecnologia da Informação da Marinha



Fonte: Adaptada pelo autor a partir de www.dctim.mb/sites/dctim.br/files/Organograma.pdf

Dessa forma, apresenta-se um escopo amplo das funções dessa Diretoria Especializada (DE) no tratamento da Tecnologia da Informação na Marinha do Brasil, e em especial nos

aspectos em torno da questão cibernética.

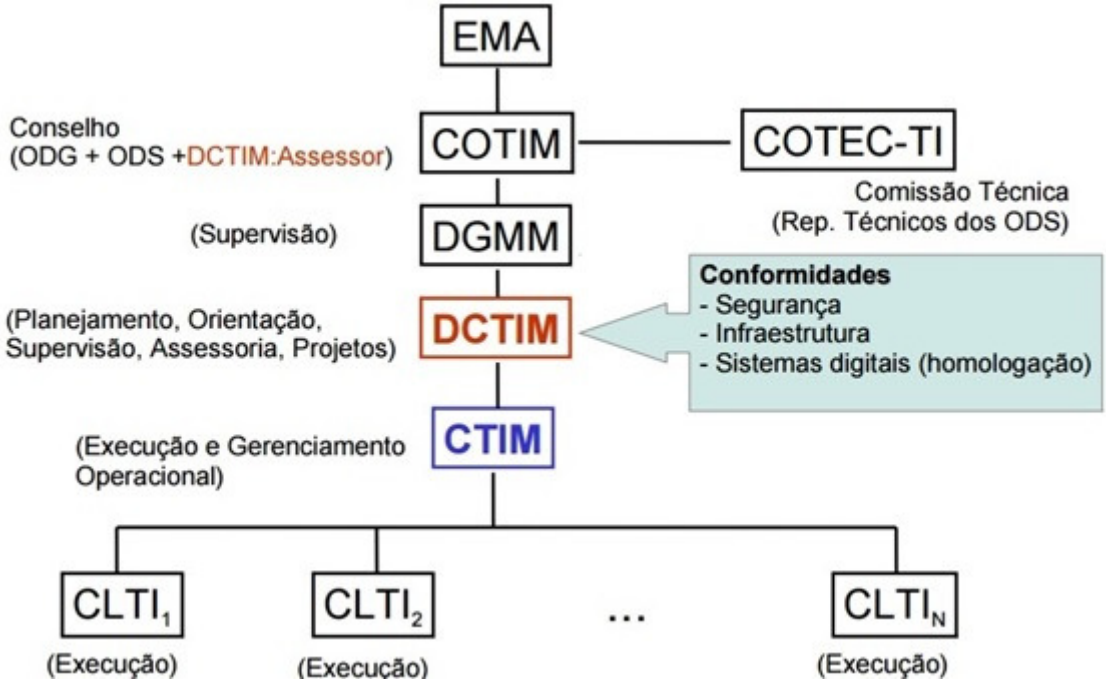
> A atividade Operacional de Guerra Cibernética na MB está a cargo do Centro de Tecnologia da Informação da MB (CTIM) e tem, como uma de suas tarefas, conduzir as atividades concernentes à Guerra Cibernética, auditoria de segurança e forense computacional[47], através do Departamento de Guerra Cibernética constante em seu organograma. Esse Departamento está subdividido em três Seções, quais sejam: Operações, Infraestrutura de Segurança da Informação Digital (SID) e Forense Computacional e Recursos Criptológicos. (NUNES, 2010).

Ainda de acordo com a supracitada publicação, coube ao Centro de Tecnoliga da Informação da MB, como Órgão de Execução Operacional, realizar diversas tarefas técnicas que visam **proteger a RECIM**, dentre elas: apoiar as OM, na sua área de jurisdição, e os CLTI, em 2º escalão; operar os recursos tecnológicos para a GC; mobilizar o pessoal qualificado, para o emprego em situações de conflito; implantar, gerenciar, operar e manter os sistemas de proteção da RECIM; apoiar as OM na implantação de sistemas de proteção nas suas redes locais; realizar as análises de vulnerabilidades, ameaças e riscos de segurança da informação; avaliar os dispositivos de segurança da informação para a RECIM, bem como a proposição de soluções de segurança que mitiguem os riscos detectados a níveis aceitáveis; e posicionar, manter e monitorar os sensores, dispositivos de alertas e concentradores de logs, mantendo seus registros e análises, de forma a possibilitar estudos e ativação, quando necessário, do Grupo de Resposta a Incidentes de Segurança da Informação Digital (GRISID) (MARINHA DO BRASIL, 2012, p. 3-4 a 3-7, grifo nosso).

Na Estrutura Organizacional dessa DE, observamos o destaque dado à questão de Segurança e Defesa com a estrutura da seção DCTIM-31, que cuida especificamente da matéria e coordena tecnicamente a elaboração de normativas afeitas à questão cibernética, bem como elabora exercícios de guerra cibernética e a capacita pessoal especializado.

[47] Forense computacional: é o emprego de técnicas e de procedimentos para aquisição, preservação, identificação, extração, restauração, análise e documentação de provas computacionais armazenadas em mídias eletrônicas, a fim de atender demandas administrativas, jurídicas ou judiciais. (*EMA-416 Doutrina de tecnologia da informação da Marinha*. 2012, Brasília).

Figura 10 – Governança de TI na MB



Fonte: http://portal.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/218[48].

Como último nível de capilaridade da estrutura organizacional, apresentam-se os Centros Locais de Tecnologia da Informação (CLTI), que possuem por objetivo otimizar o uso de recursos humanos e financeiros da área de TI por meio da concentração de serviços comuns às OM por eles apoiadas (BRASIL, 2012a, p.1), sendo classificados como elementos organizacionais de apoio e responsáveis, dentre outras tarefas, por auxiliar o CTIM na "resolução de problemas de maior complexidade e que requeiram ações de reparo interdisciplinares para restabelecimento dos sistemas da RECIM" (MARINHA DO BRASIL, 2012, p. 3-9) e "na resolução de todo e qualquer tipo de incidente relativo às redes, e/ou aos sistemas de TI, nos locais sob sua área de jurisdição que afetem o bom funcionamento da RECIM" (MARINHA DO BRASIL, 2011).

4.3 ESPAÇO CIBERNÉTICO NA MB

Faz-se conveniente, neste momento, que se comente um pouco sobre duas estruturas que compõem o domínio cibernético da MB, quais sejam: a sua rede interna que tem o nome de Rede de Comunicações Integradas da MB (RECIM) e a Internet[49] na MB, por serem

[48] A Defesa Cibernética na Visão da Marinha do Brasil – CF (A) Nilson Rocha Vianna, *Anais do XI Ciclo de Estudos Estratégicos*: Segurança e Defesa Cibernética, 2012.

[49] A Internet é um conglomerado de redes e não é propriedade de qualquer indivíduo ou grupo. Assegurar uma

"portas de entradas" de possíveis ameaças externas e internas.

4.3.1 RECIM

A RECIM tem como propósito a interconexão de dispositivos eletrônicos, possibilitando a comunicação entre usuários (voz, dados ou voz e dados), obedecendo aos seguintes itens: confiabilidade, rapidez nas respostas às solicitações, disponibilidade, eficiência e custo.

Ela pode ser definida como a infraestrutura para uma rede de grande área privada (WAN)[50], composta por redes metropolitanas Distritais, tendendo a ser independente das prestadoras de serviço de telecomunicações e fundamentada em suporte de comunicação de alta qualidade.

Utiliza-se de uma CETELMA (Central Telefônica da Marinha) e/ou equipamento de conectividade que dispõem de dispositivos com capacidade de manipulação de voz e dados, para efetuar a integração das redes que fazem parte de um Distrito, Comando ou Complexo Naval.

Pode ser estruturada em três áreas de atuação:

a) área restrita à OM: a primeira área de atuação restringe-se, basicamente, a uma OM. Cada OM pode ter ao menos uma rede de dados local que, em conjunto com ramais telefônicos ou centrais telefônicas ligadas a uma CETELMA, é integrada à RECIM. A responsabilidade administrativa e técnica de suas redes ficam a critério da própria OM;

b) área dos Distritos, Comandos ou Complexos Navais: a segunda área de atuação refere-se aos Distritos, Comandos ou Complexos Navais (exemplo: Complexo de Mocanguê). Cada um desses elementos constitui uma rede metropolitana integrada pelas redes locais das OM situadas em sua área de responsabilidade.

   A responsabilidade administrativa e técnica dessas redes fica a cargo dos respectivos Distritos, Comandos ou Complexos Navais;

---

comunicação eficaz através dessa infraestrutura diversificada requer a aplicação de tecnologias consistentes e comumente reconhecidas e normas, bem como a cooperação de muitas agências de administração de rede. Existem organizações que foram desenvolvidas com a finalidade de ajudar a manter a estrutura e a padronização de protocolos e processos da Internet. Essas organizações incluem a Internet Engineering Task Force (IETF), além de muitos outros. (Cisco Network Academy. *Network Basics Companion Guide*. 1st edition. San Francisco: Cisco Press, 2013).

[50] Wide-area network (WAN): Uma infraestrutura de rede que fornece acesso a outras redes em uma ampla área geográfica. (Cisco Network Academy. *Network Basics Companion Guide*. 1st edition. San Francisco: Cisco Press, 2013).

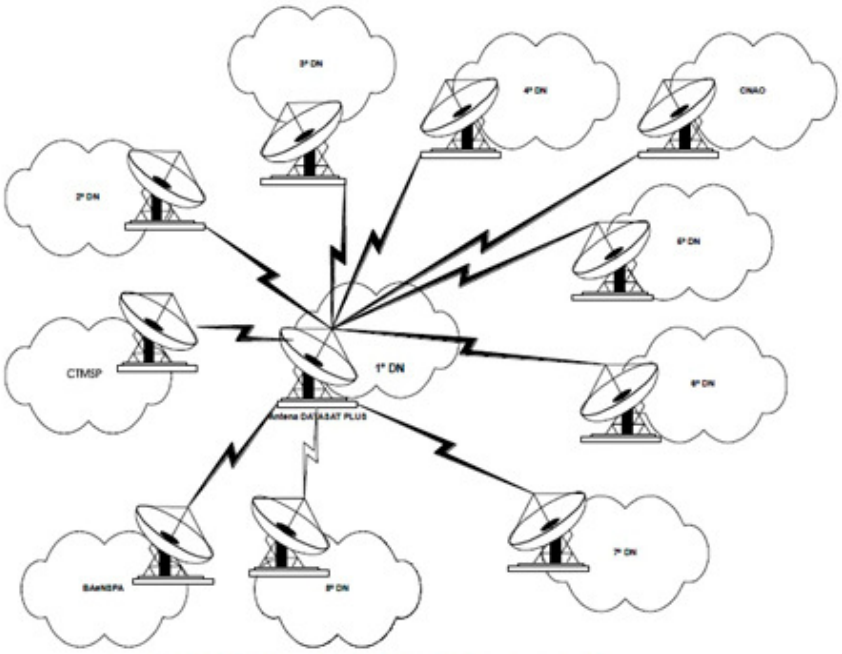
c) integração das redes metropolitanas: a terceira área de atuação abrange a integração de todas as redes metropolitanas, formando uma rede de grande área privada. Essa WAN (Wide Area Network) possibilitará a integração de todas as sub-redes da Marinha.

Caberá à DCTIM (Diretoria de Comunicações e Tecnologia da Informação da Marinha) a responsabilidade administrativa, bem como a responsabilidade técnica.

Em sua estrutura física, a RECIM é dividida em três grandes redes, estando, atualmente, seu gerenciamento diferenciado em REDE DE TELEFONIA – RETELMA (voz), REDE DE PACOTES (dados) e REDE DE INTEGRADORES (voz e dados).

A Figura 11 apresenta a configuração do *backbone* principal da RECIM, interligando todas as redes metropolitanas de todos os Distritos Navais (DN), Centro Tecnológico da Marinha em São Paulo (CTMSP) e a Base Aeronaval de São Pedro da Aldeia (BAeNSPA).

Figura 11 – Backbone principal da RECIM



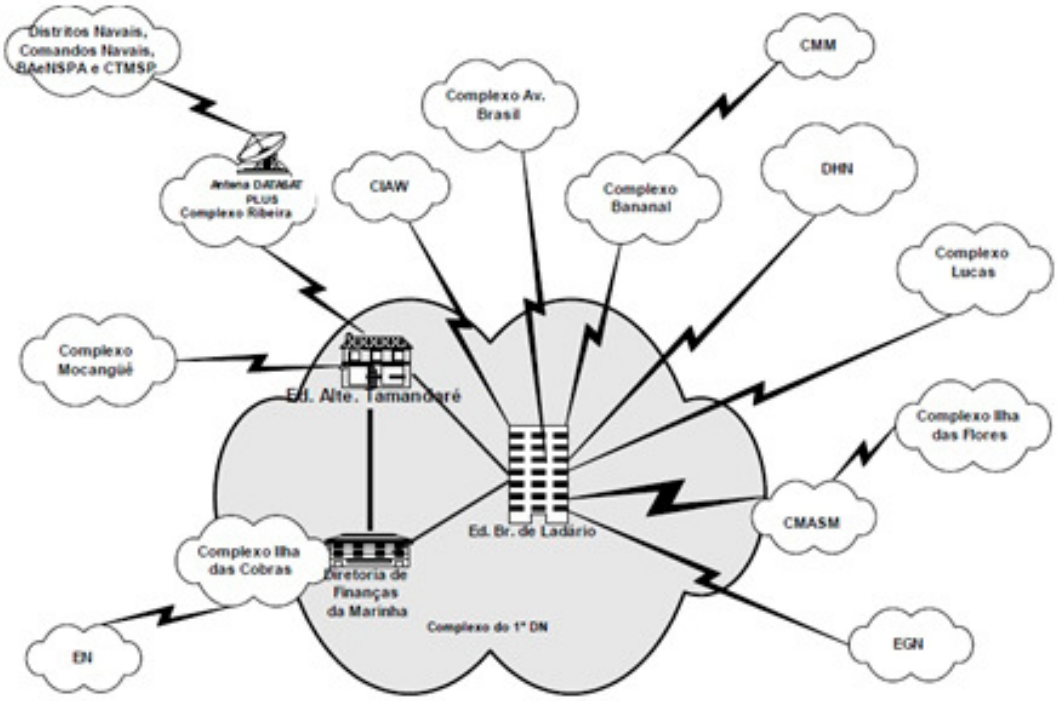
Fonte: VELOSO, 2008[51].

A Figura 12 reproduz uma representação simbólica da rede metropolitana (de Comunicações Integradas) do 1º DN. Nessa representação, estão simbolizadas as redes de voz

[51] VELOSO, Rubem Ribeiro. A*valiação de Conformidade a Modelos de Gestão de Segurança da Informação na Marinha do Brasil*. 2008. 72 f. Monografia (Curso de Especialização em Gestão de Segurança da Informação e Comunicações) – Universidade de Brasília, Brasília – DF, 2008.

e dados. As outras redes metropolitanas se assemelham, em menor escala e complexidade, à apresentada.

Figura 12 – Rede metropolitana do 1^0 DN

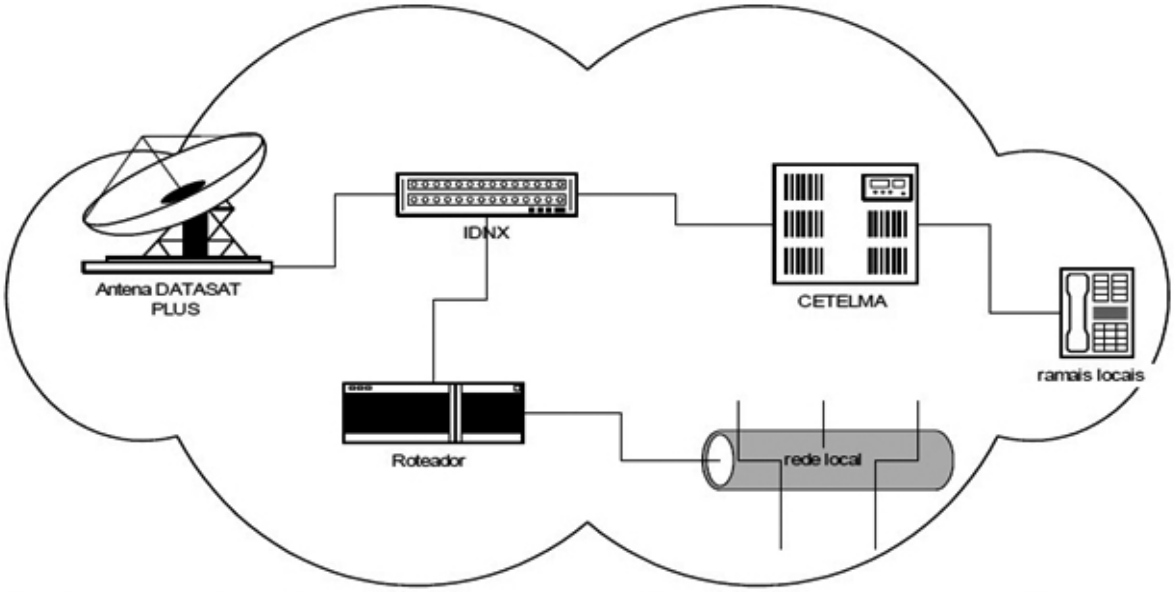


Fonte: VELOSO, 2008.

O gerenciamento integrado de voz e dados são efetuados de forma centralizada, na DCTIM, onde são monitorados todos os equipamentos multiplexadores-integradores distribuídos pelos Distritos, Comandos e Complexos Navais.

Em cada Distrito Naval, existe um conjunto de equipamentos que constituem o ponto de interligação entre os DN, em rede de grande área, por intermédio, principalmente, de Comunicações por Satélite (serviço DATASAT PLUS da EMBRATEL), conforme demonstra a figura seguinte:

Figura 13 – Conjunto de Equipamentos – Pontos de Interligação do 1^0 DN

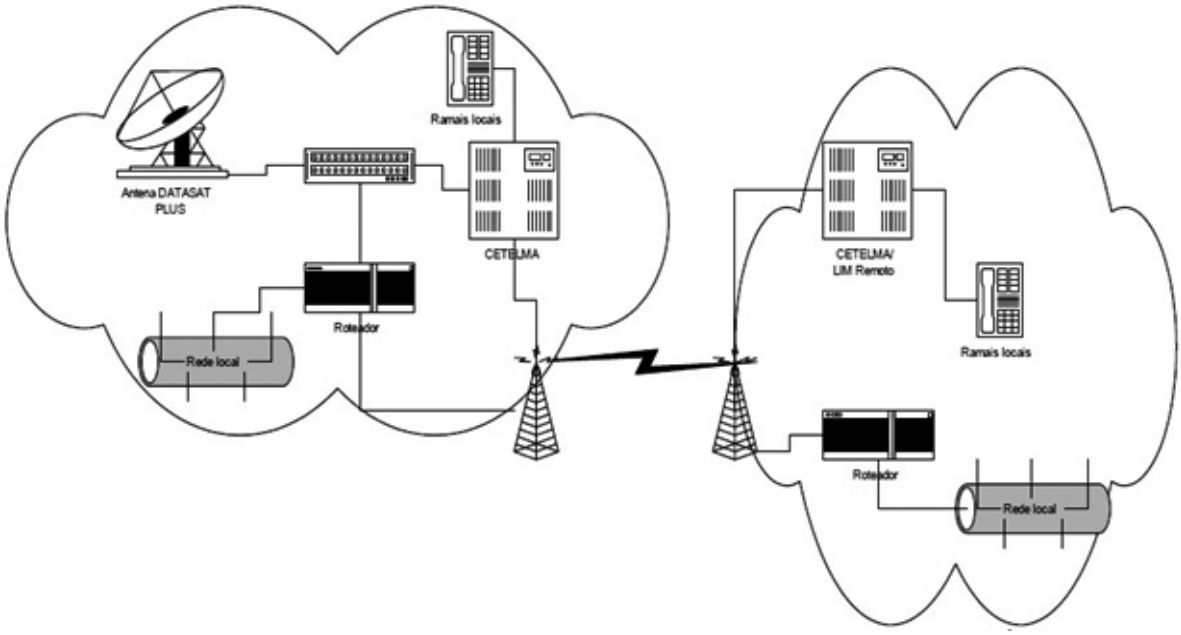


Fonte: VELOSO, 2008.

As redes metropolitanas são igualmente constituídas, obrigando assim na existência de um Supervisor Operacional de Área (SOA), surgindo o que convencionamos chamar de "complexos", ou seja, um local composto, normalmente, por uma quantidade razoável de OM, interligadas entre si por meios físicos (fibra óptica ou par metálico) e com um único ponto de interligação com o restante da RECIM. Isso pode ser bem visualizado na Figura 11, que apresenta a rede metropolitana do 1º DN e os vários complexos existentes.

A figura seguinte mostra, à semelhança do mostrado na rede de grande área, um conjunto de equipamentos por onde o complexo se interliga a outros dentro da área metropolitana.

Figura 14 – Conjunto de equipamentos complexo de interligação metropolitana



Fonte: VELOSO, 2008.

4.3.2 A internet na MB

Na MB, o acesso à Internet inicialmente possuía o objetivo predominantemente voltado às atividades relacionadas à pesquisa científica e de natureza acadêmica. Por esse motivo, houve uma seleção das OM, pela Comissão de Ciência e Tecnologia da Marinha (COMCITEM), que seriam contempladas com esse acesso.

Posteriormente, tendo a RECIM atingido dimensões nacionais e em decorrência da necessidade de tráfego de informações de naturezas diversas, foi realizado contrato junto à Embratel, para interligação da RECIM à Internet, através da rede de dados daquela empresa. Desse modo, todas as OM interligadas à RECIM têm condições técnicas de ter acesso à Internet, desde que sejam autorizadas a fazê-lo.

Todo o acesso à Internet, partindo de estações interligadas à rede de dados da RECIM, era realizado através dessa conexão, não sendo autorizada nenhuma outra interligação à Internet em qualquer ponto da RECIM. A consolidação da RECIM, no seu segmento de comunicação de dados, juntamente com a experiência adquirida com a Internet, permitiu a introdução na MB num segundo momento ao conceito de Intranet[52].

[52] Intranet é um termo frequentemente usado para se referir a uma conexão privada de LANs e WANs que pertencem a uma organização, sendo projetada para ser acessível apenas aos seus membros, funcionários ou outros que têm autorização. Possui aparência e funcionamento idênticos à Internet, sendo normalmente acessível dentro de uma organização. Seu uso é voltado a publicações de informações sobre: eventos internos,

A modernização da infraestrutura da RECIM e do acesso a Internet, conforme o BONO Especial nº 504/2008[53], a DCTIM, por meio de seus sistemas de gerenciamento, tem constatado um significativo aumento na demanda, de todas as OM, por serviços de TI (Tecnologia da Informação) disponibilizados na RECIM (Intranet) e na Internet. (VELOSO, 2008).

Em resumo, o domínio cibernético da MB é composto por um "framework" complexo denominado RECIM sobre o qual repousa uma camada de dados denominada Internet, em que efetivamente ocorre a integração de sistemas e a comutação dos dados necessários.

4.4 CONJUNTURA NORMATIVA DE SEGURANÇA E DEFESA CIBERNÉTICA NA MARINHA DO BRASIL

Elenca-se o grupo subsidiário de normas ao conjunto legislativo da Administração Pública Federal os quais representam o esforço da Marinha do Brasil em coordenar seu espaço cibernético. No que diz respeito à questão de segurança e defesa cibernética na Marinha do Brasil, sua expressão dá-se em diferentes níveis documentais quer sejam:

a) político;

b) normativo; e

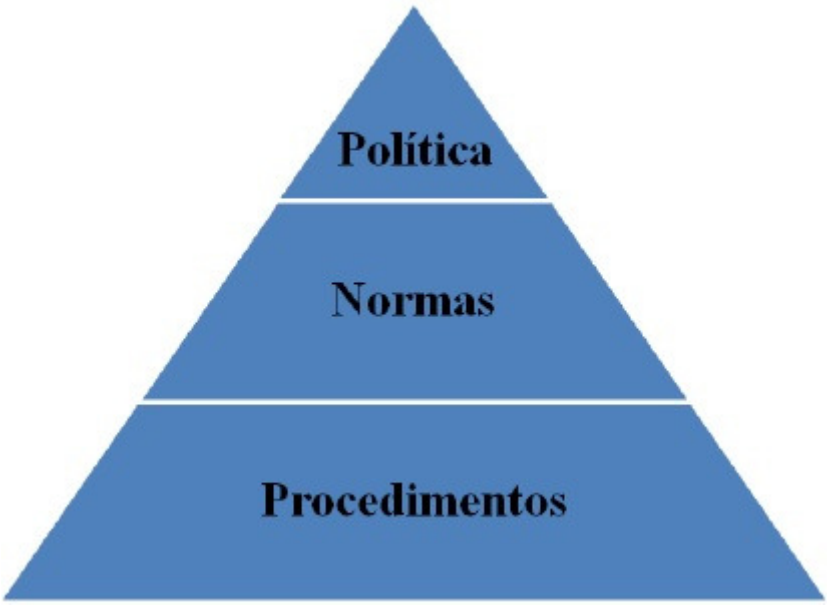
c) procedimental.

---

políticas, boletins informativos, diretórios telefônicos, ajudando a eliminar a burocracia e acelerando fluxos de trabalho. (Cisco Network Academy. *Network Basics Companion Guide*. 1st edition. San Francisco: Cisco Press, 2013).

[53] Marinha, Diretoria de Comunicações e Tecnologia da Informação da. BONO nº 504. *Boletim de Ordens e Notícias Especial*, 23 de junho de 2008.

Figura 15 – Níveis documentais



Fonte: Elaborada pelo autor.

Os documentos de cunho político possuem em sua autoria oficiais generais que buscam divulgar para toda a força uma visão de alto nível dos rumos do poder naval. Dentre os mais significativos, podemos apontar as próprias Orientações do Comandante da Marinha (ORCOM).

No que diz respeito à questão de segurança e defesa cibernética, o assunto manifesta-se de forma bem clara na ORCOM 2008 e ORCOM 2016.

> A-6. Tecnologia da Informação (TI) na Marinha.
> O EMA deverá avaliar a implementação da Doutrina de TI na MB e a execução das ações do Programa de Trabalho da Comissão Técnica de TI (COTEC-TI), bem como as deliberações do Conselho de TI da Marinha (COTIM), apresentando relatório consolidado ao CM, com o concurso dos ODS, até 30ABR, 31AGO e 15DEZ2008. (ORCOM, 2008)

O supracitado segmento faz referência ao que viria a ser a Doutrina da TI na MB, a qual em sua 2ª parte trata exclusivamente sobre a Guerra Cibernética.

Em 2016, o atual Comandante da Marinha volta ao assunto Segurança e Defesa cibernética, manifestando sua preocupação correspondente ao tema:

> A Marinha que almejamos legar às futuras gerações deverá ser uma Força moderna, equilibrada e balanceada, dispondo de meios navais, aeronavais e de fuzileiros navais compatíveis com a inserção político-estratégica do nosso País no cenário internacional e, em sintonia com os anseios da sociedade brasileira, deverá estar permanentemente pronta para atuar não só em águas azuis, litorâneas e interiores, como também sob a égide de organismos internacionais e em suporte à política externa do País, visando a contribuir para a defesa da Pátria e para a salvaguarda dos interesses nacionais, em consonância com as diretrizes constantes da Estratégia

> Nacional de Defesa (END). São as seguintes as minhas orientações de caráter geral, de aplicação a toda a Marinha:
> [...]
> e) Dar prosseguimento ao incremento da Defesa Cibernética e da Segurança da Informação Digital na MB;
> [...]
> 3.3 INTELIGÊNCIA
> I-1. Defesa Cibernética e Segurança da Informação Digital (SID) na Marinha
> Criar o Centro de Ações de Guerra Cibernética do ComOpNav, com o propósito de prover a infraestrutura necessária para coordenar os recursos e ações de Guerra Cibernética da MB. (ORCOM, 2016).

Dentre os esforços político-organizacionais, ainda no nível político, tem-se o Plano Estratégico da Marinha (PEM) aprovado em 13 de março de 2008, na sua 2ª revisão. Em seu capítulo 6, são definidos os objetivos da MB. Um desses objetivos aborda a necessidade de manter a segurança de nossos sistemas digitais de tecnologia da informação (TI) e de comunicações no Estado da Arte, a fim de se evitar ataques cibernéticos.

No capítulo 11 do supracitado planejamento, em suas Diretrizes para o Planejamento Naval (DIPNAV), no setor de Ciência e Tecnologia e TI, diz-se: "estabelecer ações para garantia do uso da informação de interesse da MB e negar a sua utilização de forma contrária". Nessa DIPNAV, encontra-se a necessidade de manter a segurança de nossos sistemas para garantir o uso da informação pela MB.

Nessa órbita de representatividade documental normativa, a Diretoria-Geral do Material da Marinha (DGMM) possui um conjunto de publicações que tratam de segurança de sistemas digitais, segurança criptológica e de comunicações na MB, e nelas se encontram orientações de escopo funcional expressando a implantação de uma vontade política. São elas:

a) DGMM-0500 – Manual de Comunicações da Marinha (2006);
b) DGMM-0510 – Normas para Criptologia da Marinha (2000);
c) DGMM-0520 – Normas para a Gestão de Segurança das Informações Digitais em Redes Locais (2004);
d) DGMM-0540 – Normas de Tecnologia da Informação da Marinha. 1ª rev. Rio de Janeiro, RJ, 2010.

O setor operativo também emana documentação afeita ao assunto de segurança e defesa cibernética, são eles:

a) EMA-416: Doutrina de Tecnologia da Informação da Marinha, Volume I. 1ª rev. Brasília, DF, 2007;
b) *EMA-416 Vol. II: Manual de Guerra Cibernética*.

Nesse último, constam vários conceitos e definições, como: Forense Computacional,

Governança de TI, Guerra Centrada em Redes (GCR), segurança da informação e segurança da informação digital (SID).

Também são definidos:

> Guerra Cibernética: conjunto de ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores. (EMA-416 2ª revisão, 2013, p.1-3).
> e Segurança Cibernética: é a segurança do espaço cibernético, ou seja, a segurança das redes de computadores e de seus equipamentos de conectividade correlatos. (EMA-416, 2013, p 1-4).

Por fim, os documentos de caráter operacional, procedimento são amplamente publicados sob a maestria da DCTIM e do CTIM, já que representam em sua maioria instruções de trabalho cotidiano e possuem aplicabilidade pontual.

a) DCTIMARINST nº 30-08A – Uso Institucional e não Institucional de mídias e redes sociais extra-MB pelo pessoal da MB 2015;
b) DCTIMARINST nº 30-12 – Gerenciamento dos registros de eventos computacionais relevantes (logs) 2014;
c) DCTIMARINST nº 31-03 – Gestão de Riscos em Segurança da Informação e Comunicações 2011;
d) DCTIMARINST nº 31-02A – Forense Computacional e Registros de Acesso à Internet 2014.

O significativo conjunto regulatório, ora manifesto pelas mais altas autoridades navais, ora conduzindo uma atividade cotidiana no segmento de SI, em soma com todo arcabouço regulatório da Administração Pública Federal, revela a significância que a matéria representa ao Poder Naval.

5 SIMULAÇÃO DE CENÁRIO: PLANEJAMENTO DE UM ATAQUE CIBERNÉTICO AO SISTEMA DE CONTROLE DE TRÁFEGO MARÍTIMO

A Marinha do Brasil, como detentora de um espaço cibernético próprio, encontra-se exposta a toda ordem de ameaças pertinentes a esta arena tecnológica. Não obstante, a gestão desse domínio onde repousam um sem número de sistemas tanto operativos quanto de apoio administrativo cabe à DCTIM.

Na seara da segurança e defesa cibernética, é fundamental o entendimento que um ataque cibernético não é mais a manifestação da curiosidade de um aficionado pelas TIC (hacker), e sim o resultado final de uma ação elaborada que, por sua vez, possui motivação, planejamento e financiamento.

O capítulo três desta pesquisa revelou uma série de fatores motivadores, sejam eles políticos, econômicos ou, no caso dos Estados, pela disputa do poder. A Marinha do Brasil, como órgão da Administração Pública Federal, está exposta a todo esse conjunto de motivadores.

Um exemplo de exposição a uma ação do cyber-ativismo seria por uma questão de motivação pela causa ecológica,

> **Marinha deve suspender exercícios de tiro em Alcatrazes.**
> Após ter chegado a um consenso com o Ministério do Meio Ambiente, o Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA) e o Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), a Marinha do Brasil deverá alterar o posicionamento da raia onde são realizados os exercícios de tiro, de forma a utilizar apenas a Ilha da Sapata, uma ilha menor, situada a nordeste da Ilha de Alcatrazes, no litoral de São Paulo.
> Tal reposicionamento contribuirá para a redução do impacto ambiental decorrente da atividade, que é considerada imprescindível pela Marinha. A mudança ainda está em estudos, mas tem a simpatia da Marinha do Brasil.
> Dessa forma, a Marinha apoia a criação do Parque Nacional Marinho de Alcatrazes, mas quer que a Ilha da Sapata seja mantida fora dos limites do futuro parque e sob a jurisdição da Marinha, a fim de que se possa dar continuidade aos exercícios. "A presença da Marinha do Brasil no Arquipélago de Alcatrazes tem ainda como objetivo dissuadir a presença e a atuação de depredadores ou de qualquer utilização indevida da ilha". (REVISTA ALMANÁUTICA[54], 17 jun. 2013).

O motivador econômico, muitas vezes, consiste em vazamentos de informações que podem prejudicar as relações comerciais, a exemplo:

> **Vazam dados de submarino francês comprado pelo Brasil.**
> A Marinha do Brasil ressalta que 'os S-Br foram projetados atendendo

[54] Edição on-line da revista *Almanáutica*. Disponível em: <http://almanautica.com.br/2013/06/17/marinha-deve-suspender-exercicios-de-tiro-em-alcatrazes-litoral-de-sp/>. Acesso em: 1 fev. 2017.

> especificações e há diferenças entre os submarinos nacionais e os outros'
> Segredos técnicos e informações sigilosas contidas em 24.500 páginas do projeto original dos submarinos de ataque Scorpène, de tecnologia francesa — quatro dos quais estão sendo construídos no Brasil pela Odebrecht Defesa e Tecnologia para reequipar a Marinha — correm risco. Detalhes dos planos foram revelados há pouco mais de uma semana na Austrália, depois de o governo local ter anunciado a escolha do mesmo submarino para renovar sua força naval. A operação envolve 12 embarcações, ao custo de 38,5 bilhões de reais. (REVISTA VEJA, Edição on-line, 5 set. 2016).

Um exemplo de sobreposição de poder como uma motivação geopolítica:

> **Brasil foi alvo de mesma manobra naval dos EUA que irritou China**
> O Brasil foi alvo da mesma operação da Marinha americana que irritou autoridades chinesas nesta semana, quando o navio USS Lassen navegou a menos de 12 milhas marítimas das ilhas artificiais do arquipélago Spratly, mostram documentos americanos.
> [...]
> No caso da operação no Brasil, foi desafiada a exigência de que as Marinhas estrangeiras peçam permissão para realizar manobras militares na Zona Econômica Exclusiva brasileira (ZEE).
> O Brasil, que ratificou a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), entende que as disposições do tratado não autorizam outros países a realizar na ZEE exercícios ou manobras militares, em particular as que impliquem o uso de armas ou explosivos, sem aval do Estado costeiro.
> [...]
> A porta-voz do Departamento de Defesa americano, porém, afirma que os Estados Unidos "não notificam os Estados costeiros quando conduzem manobras militares nas suas ZEE, porque a lei internacional não o requer. (FOLHA DE S. PAULO[55], 30 out. 2015).

O planejamento de um ataque cibernético consiste num estudo elaborado pelo atacante, em que se procura o maior potencial de dano possível, seja esse dano por constrangimento, financeiro ou operacional.

Por último, advém o financiamento das ações, visto que, para o sucesso, ou não, da empreitada, demandam-se técnicos experientes, equipamentos, desenvolvimento de softwares, e, mesmo que tudo isso seja uma iniciativa solitária, ainda sim esses custos estarão presentes.

5.1 O QUE ATACAR EM QUEM TE DEFENDE?

Existe uma metodologia para se proceder a um ataque cibernético, pois, como dito anteriormente, esse é o resultado de um processo motivado, planejado e financiado. Sendo assim, faz-se necessário saber quais são as etapas de um ataque:

---

[55] CAVALCANTI, Fernando, em colaboração ao Jornal *Folha de S. Paulo*, Edição on-line, 30 out. 2005. Disponível em: <http://www1.folha.uol.com.br/mundo/2015/10/1700336-brasil-foi-alvo-de-ato-naval-semelhante-ao-que-os-eua-realizaram-na-china.shtml>. Acesso em: 1 fev. 2017.

5.2 ETAPAS DE UM ATAQUE CIBERNÉTICO[56]

a) reconhecimento: antes de lançar um ataque, um alvo vulnerável é escolhido, podendo ser uma organização, um executivo ou um administrador de rede;
b) varreduras: uma vez escolhido o alvo, a próxima etapa é identificar um ponto fraco que permitirá acesso aos atacantes;
c) acesso e elevação de privilégio: identificadas as fragilidades, o próximo passo no ataque cibernético é ganhar acesso e, em seguida, obter privilégios administrativos;
d) extração: com a liberdade para se deslocar na rede, agora é possível acessar sistemas com dados mais sensíveis de uma organização e extraí-los à vontade;
e) manutenção de acesso: secretamente programas maliciosos como root-kits são instalados para que seja possível retornar sempre que possível;
f) assalto: felizmente, essa etapa não é realizada em todos os ataques cibernéticos, pois visa alterar a funcionalidade de hardware da vítima ou desativar o hardware inteiramente;
g) cobrindo rastros: normalmente, os rastros são removidos, mas isso não é universal para todos os casos, especialmente se a intenção do atacante é deixar um "cartão de visita" para se gabar de suas façanhas.

Este trabalho concentra sua atenção nas duas primeiras etapas de um ataque com o intuito acadêmico de mostrar a complexidade de uma ação cibernética.

Dentre os possíveis cenários de ataque cibernético ao Poder Naval brasileiro, aqueles que concentram sua atenção em sistemas operativos possuem um potencial de dano significativo, pois atingem a imagem institucional, bem como dirimem o moral de seus operadores.

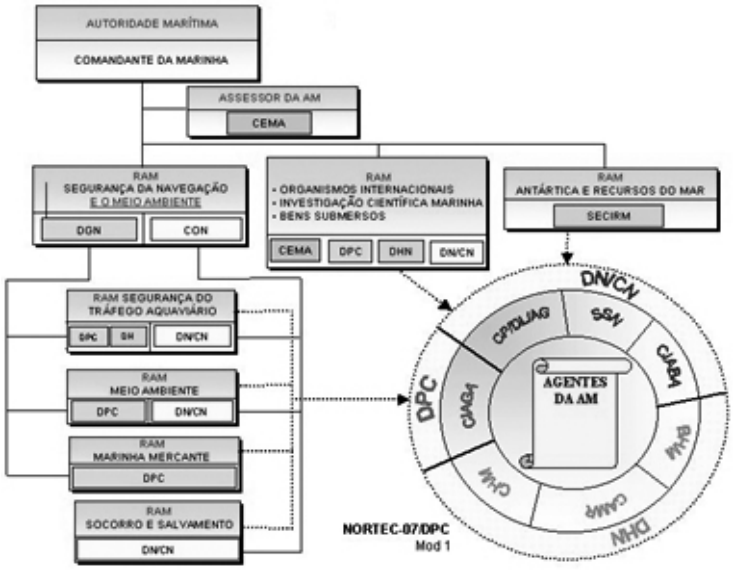
5.2.1 Reconhecimento

Vale lembrar que, dentre as missões da Marinha do Brasil, jaz a de Autoridade Marítima Brasileira, e, com esse legado, o Poder Naval compromete-se perante o Estado brasileiro e a Comunidade Internacional em regulamentar o tráfego marítimo, garantir a

[56] Fonte: Infosecinstitute.com. Disponível em: <http://resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack/#gref>. Acesso em: 31 jan. 2017. Tradução nossa.

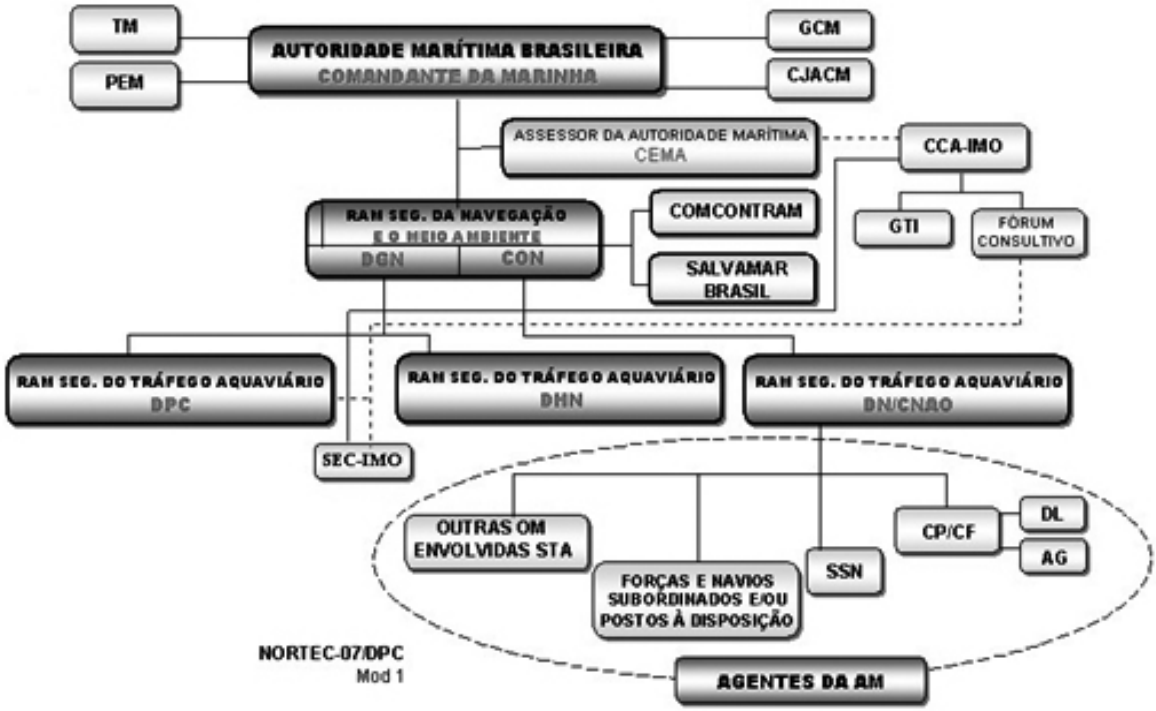
salvaguarda da vida no mar e monitorar o trânsito de embarcações comerciais não só em águas territoriais, como também em uma significativa área do Atlântico Sul.

Figura 16 – Organograma da estrutura da autoridade marítima



Fonte: https://www.mar.mil.br/cprs/cprs/adm/automaritima.htm

Figura 17 – Sistema de Segurança do Tráfego Aquaviário



Fonte: https://www.mar.mil.br/cprs/cprs/adm/automaritima.htm

O levantamento realizado por esta pesquisa observa que, dentre os sistemas operativos atualmente em uso pela Marinha do Brasil, encontra-se destaque na relação a seguir:

Quadro 5 – Sistemas operativos da esquadra

SIMMAP	Sistema de Monitoramento Marítimo de Apoio às Atividades de Petróleo
PREPS	Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite
GMDSS	*Global Maritime Distress and Safety System*
INMARSAT	Sistema que emprega satélites geoestacionários
V-RMTC	*Virtual - Regional Maritime Traffic Centre*

Fonte: https://www.mar.mil.br/salvamarbrasil/sistemas.html

O conjunto de sistemas operativos acima visa o cumprimento da missão de serviços essenciais à Marinha do Brasil, dentre eles os prestados pelas OM:

a) Comando do Controle Naval do Tráfego Marítimo (COMCONTRAM);

b) Centro de Comando do Teatro de Operações Marítimas (CCTOM);

c) Centro de Operações da Esquadra (COE);

d) Salvamar Brasil.

Isso nos leva a considerar que havendo uma plataforma comum, seja pelo uso, seja pela integração dos sistemas, essa seria considerada o alvo ideal.

Assim sendo, pelo uso:

Quadro 6 – Correlação de uso dos sistemas

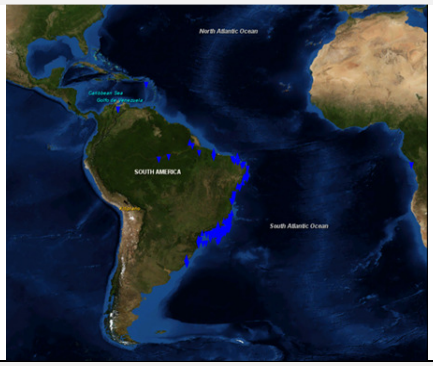
OM	**SISTEMAS**						
	SISTRAM	**LRIT**	**SINMAP**	**PREPS**	**GDMSS**	**INMARSAT**	**V-RMTC**
COMCONTRAM	X	X	X	X	X	X	X
CCTOM	X	X	X	X	X	X	X
COE	X	X	X	X	X	X	X
SALVAMAR BR	X	X	X	X	X	X	-

Fonte: Elaborado pelo autor.
Legenda: X indica a utilização do sistema.

Em levantamento realizado na página oficial do COMCONTRAM e do SALVAMAR Brasil, constatou-se que o SISTRAM é utilizado como plataforma consolidadora dos dados obtidos pelos demais sistemas, conforme a Figura 18 nos revela:

Figura 18 – Saída dos sistemas operativos no SISTRAM

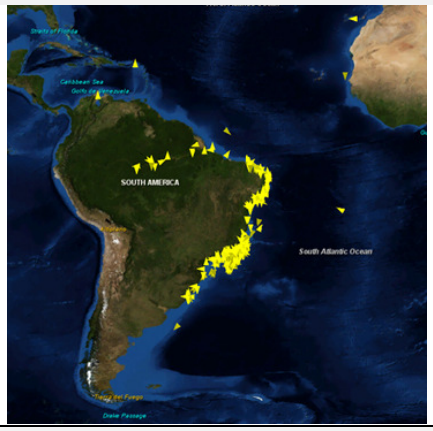
LRIT no SISTRAM



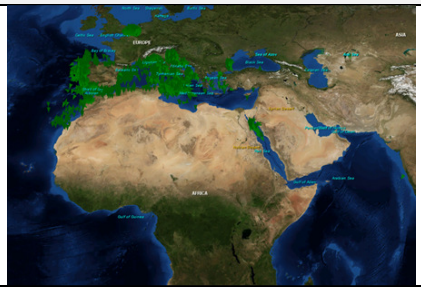
MSIS no SISTRAM

PREPS no SISTRAM

SINMAP no SISTRAM



V-RMTC no SISTRAM

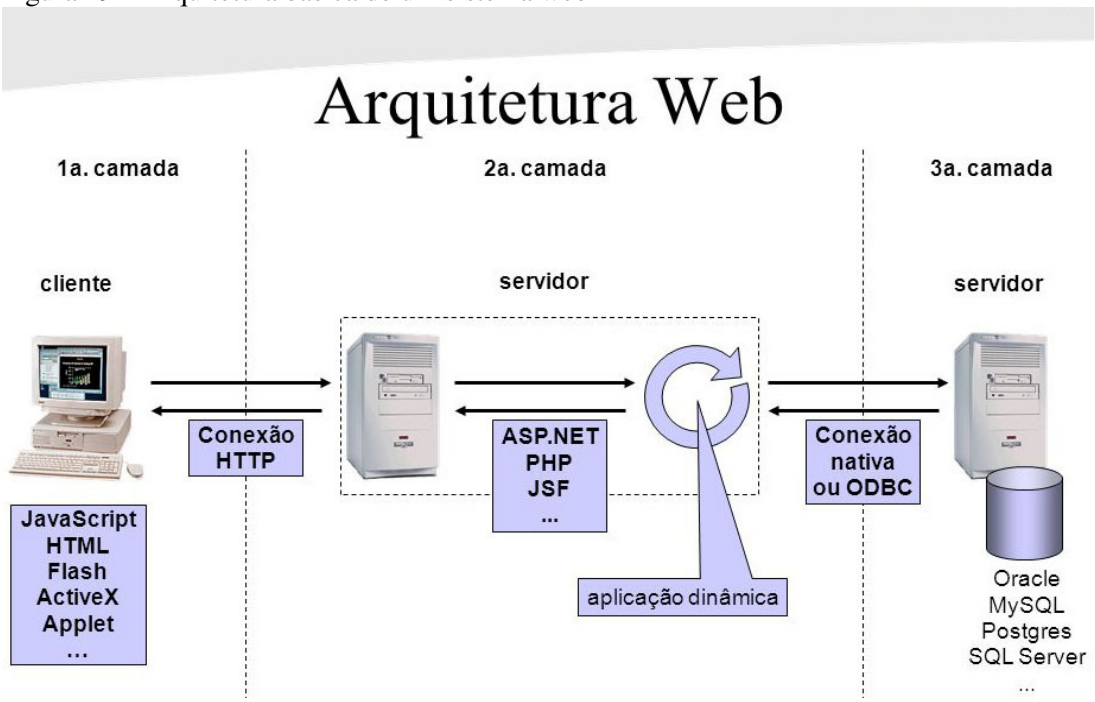


Fonte: https://www1.mar.mil.br/comcontram/

Esse ponto do reconhecimento revelou que o alvo de ataque com maior potencial de dano dentre os sistemas operativos recai sobre o SISTRAM.

O SISTRAM é um sistema baseado em arquitetura web, ou seja, uma modalidade de aplicação que apresenta sua interface ao usuário final em sua estação de trabalho local, mas que utiliza a estrutura da Internet para conectar com a infraestrutura de TIC que realiza o processamento e armazenamento das informações, conforme nos mostra a figura a seguir:

Figura 19 – Arquitetura básica de um sistema web



Fonte: Elaborada pelo autor.

5.2.2 Varredura

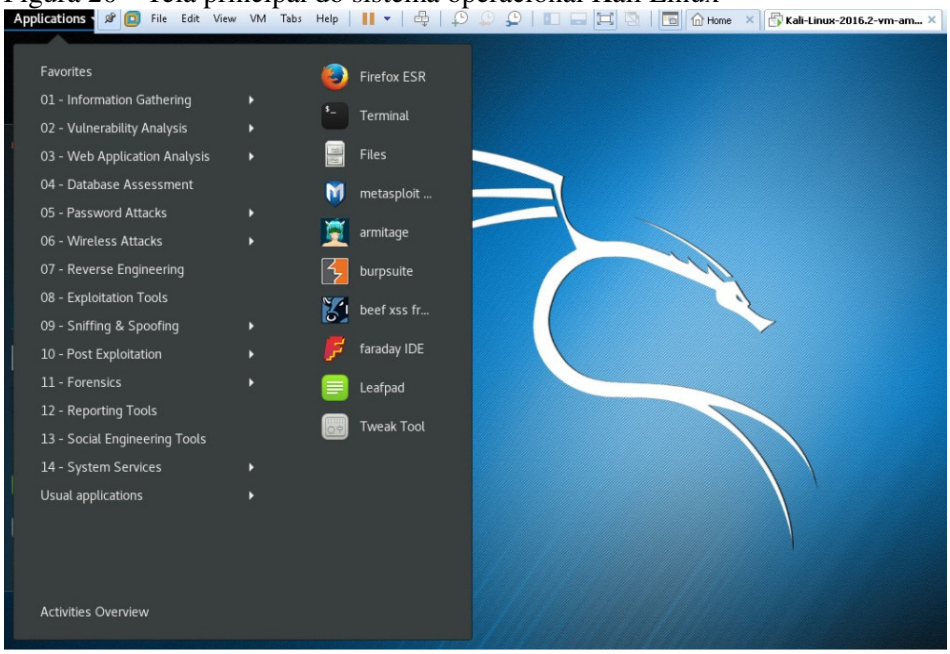
Reconhecido o sistema vulnerável, procede-se com a obtenção de informações de ordem técnica para que se tenha um entendimento global do objeto do ataque, bem como que tipo de ataque terá chance de lograr êxito.

Nesse momento, faz-se uso, se possível de engenharia social[57], e de ferramentas computacionais diversas. Uma forma de reuni-las é através de uma distribuição de sistema operacional voltado para o emprego de Pentest[58]. A mais utilizada no mercado é a distribuição Kali Linux.

[57] O termo engenharia social ficou mais conhecido em 1990, através de um famoso hacker chamado Kevin Mitnick. Esse termo designa práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las. Pode-se também definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações. (SILVA, 2008).

[58] O teste de invasão (Pentest) é uma série de atividades realizadas para identificar e explorar vulnerabilidades de segurança, ajudando a confirmar a eficácia ou não das medidas de segurança que foram implantadas. (BACUDIO, Aileen G. et al., 2011, tradução nossa).

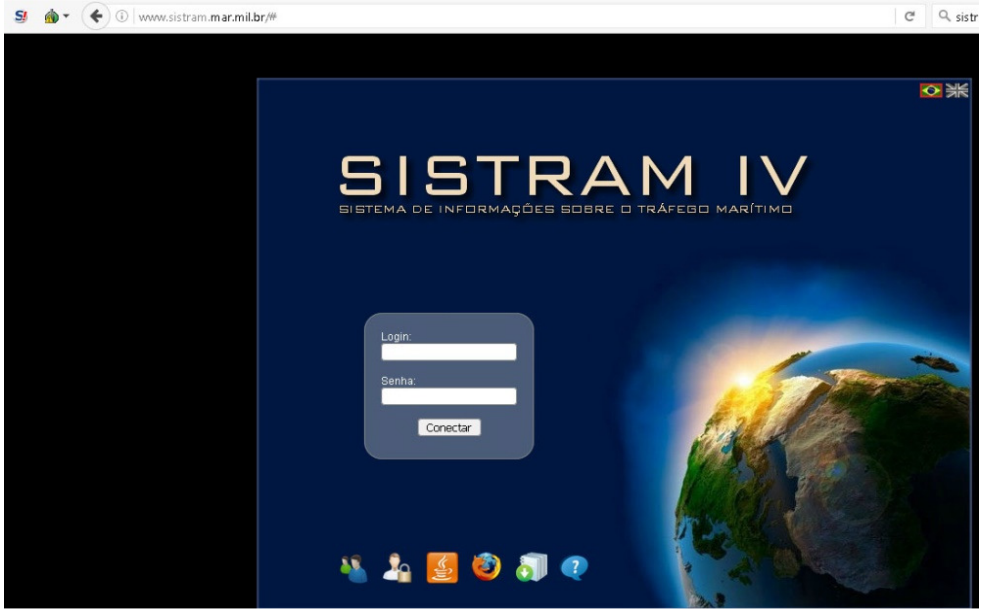
Figura 20 – Tela principal do sistema operacional Kali Linux



Fonte: Elaborada pelo autor.

A primeira ação na etapa de varredura é simplesmente realizar uma visita ao alvo:

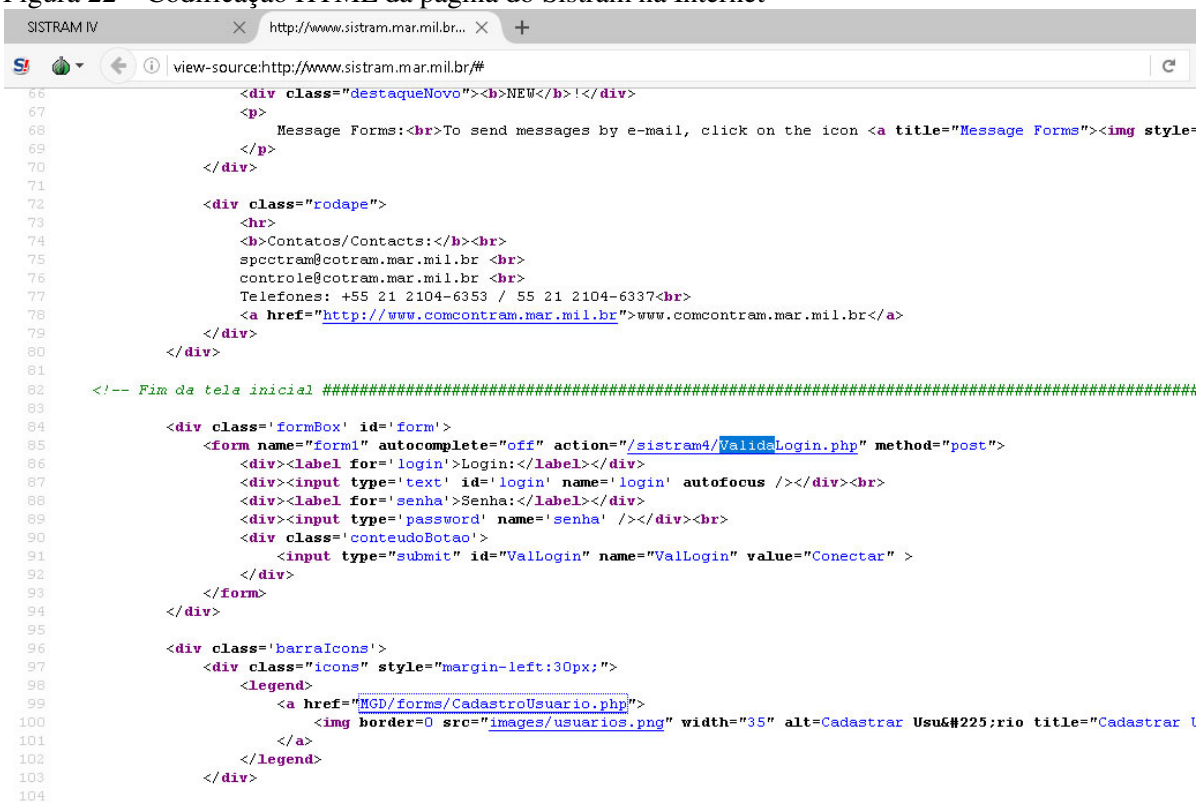
Figura 21 – Página de acesso ao Sistram na Internet



Fonte: www.sistram.mar.mil.br

A visita inocente segue-se com uma leitura da codificação da página, em que por sorte se possa obter alguma informação relevante.

Figura 22 – Codificação HTML da página do Sistram na Internet



Fonte: www.sistram.mar.mil.br

O resultado dessa varredura na codificação resulta na identificação do tipo de tecnologia utilizada no servidor web e em alguns segmentos de código identificamos o nome de alguns membros da equipe de desenvolvimento:

Figura 23 – Identificação de programadores do SISTRAM

```
//[redacted] - FunÃ§Ã£o que calcula altura e redimensiona um id
//[redacted] - adicionando apendices para controle de altura dinamica;
function setHeight(id1, id2)
{
    //em geral esses sÃ£o o menu e o conteÃºdo
    var el = document.getElementById(id1);
    var el2 = document.getElementById(id2);

//---------------------------------------------------------------------
//Biblioteca JS escrita por [redacted]
//---------------------------------------------------------------------
```

Fonte: view-source:http://www.sistram.mar.mil.br/sistram4/MGD/js/cctramJSlib.js

A obtenção dos nomes dos desenvolvedores proporcionará uso para o emprego de engenharia social e construção de um dicionário de logins e senhas conhecidos como *rainbow table* aplicado em ataques que recorrem a “força-bruta”.

A engenharia social reduziu a amostra de sistemas gerenciadores de banco de dados utilizados pelo sistema:

Quadro 7 – Curriculum vitae dos programadores identificados no SISTRAM

Programador 01
Desenvolvedora Front-end e Back-end Desenvolvimento de um sistema utilizado pelas Marinhas do Brasil, Argentina, Uruguai e Paraguai para visualização e inserção de dados georreferenciados em um mapa mundi 2D. Interface para inserção de dados também por meio de formulários, além de consumo e fornecimento de dados via web service e leitura de arquivos txt. Tecnologias front-end utilizadas: HTML5, CSS, Javascript, jQuery, JSON, OpenLayers, Google Maps API. Tecnologias back-end utilizadas: PHP, **PostgreSQL**, PostGIS, Mapscript, REST.
Programador 02
Desenvolvimento de sistemas online em Java EE / PHP / **MySQL / PostgreSQL** / PostGIS. Instalação e uso do MapServer e GeoServer. Criação de softwares que utilizam georreferenciamento. Modelagem de Simulações com HLA/RTI. Instalação e configuração do Ubuntu Server. Webservices e aplicativos para Android.
Programador 03
Software Architect Java Web for information systems development at Naval Systems Analysis Center (CASNAV) – Brazilian Navy. Systems development for IT department of Brazilian Navy. IT Project´s Technical responsible and Scrum Master. Team leadership, training and mentoring. Decision making. Configuration management. Requirements validation and supporting. Data modeling through UML design, using Domain Driven Design. Main technologies used: Java, UML, Tomcat, JPA, Spring, Maven, JUnit, Bootstrap, JavaScript, Ajax, **Oracle, PostgreSQL**, Jasper Reports, Subversion, Jenkins and Sonar. ISO 9001-2008, MPS.BR F.

Fonte: https://www.linkedin.com

Os três programadores identificam em seu currículo que, ao trabalharem no desenvolvimento do SISTRAM, necessitavam da qualificação nas seguintes soluções de SGBD: MySQL, Oracle e PostgreSQL, sendo esse último comum aos três.

Dada a adesão da Marinha do Brasil ao programa de Software Livre da Administração Pública Federal, a probabilidade recai para MySQL e PostgreSQL, como somente esse último, desde suas versões mais antigas, possui suporte ao plataformas georreferenciadas e é de conhecimento comum aos três profissionais, infere-se que a solução adotada seja o PostgreSQL.

Através de pesquisa na Internet, obtém-se uma informação valiosa quanto à escolha dos sistemas operacionais de produção adotados pela MB:

DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO
AVISO DE LICITAÇÃO
PREGÃO Nº 5/2015 - UASG 749000

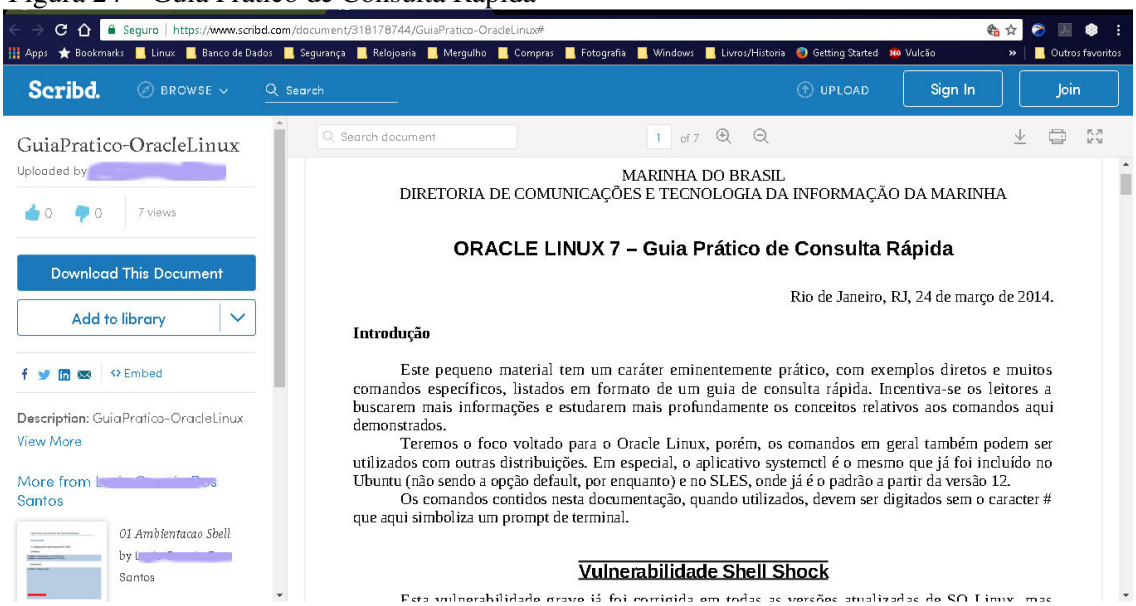
Nº Processo: 63394001234201501 . Objeto: Pregão Eletrônico -Eventual contratação de empresa especializada no fornecimento de licenças de uso definitivo de software na plataforma Oracle para Marinha do Brasil (MB), acrescidas do direito

> à atualização de versões e suporte por 12 (doze) meses e serviço de suporte à plataforma ***Oracle Linux***. Total de Itens Licitados: 00011. Edital: 22/10/2015 de 09h00 às 10h30 e de 13h às 16h00. Endereço: Rua Primeiro de Março Nr 118 - Centro Centro - RIO DE JANEIRO - RJ. Entrega das Propostas: a partir de 22/10/2015 às 09h00 no site www.comprasnet.gov.br.. Abertura das Propostas: 05/11/2015 às 09h00 site www.comprasnet.gov.br".(DOU, 22 out. 2015, Seção 3, p. 21)

Agora se sabe qual versão de sistema operacional a MB utiliza em seus servidores de produção. Melhor ainda seria descobrir qual a versão?

Mais uma vez, a engenharia social revela que o Ser Humano é o elo mais fraco na corrente da segurança.

Figura 24 – Guia Prático de Consulta Rápida

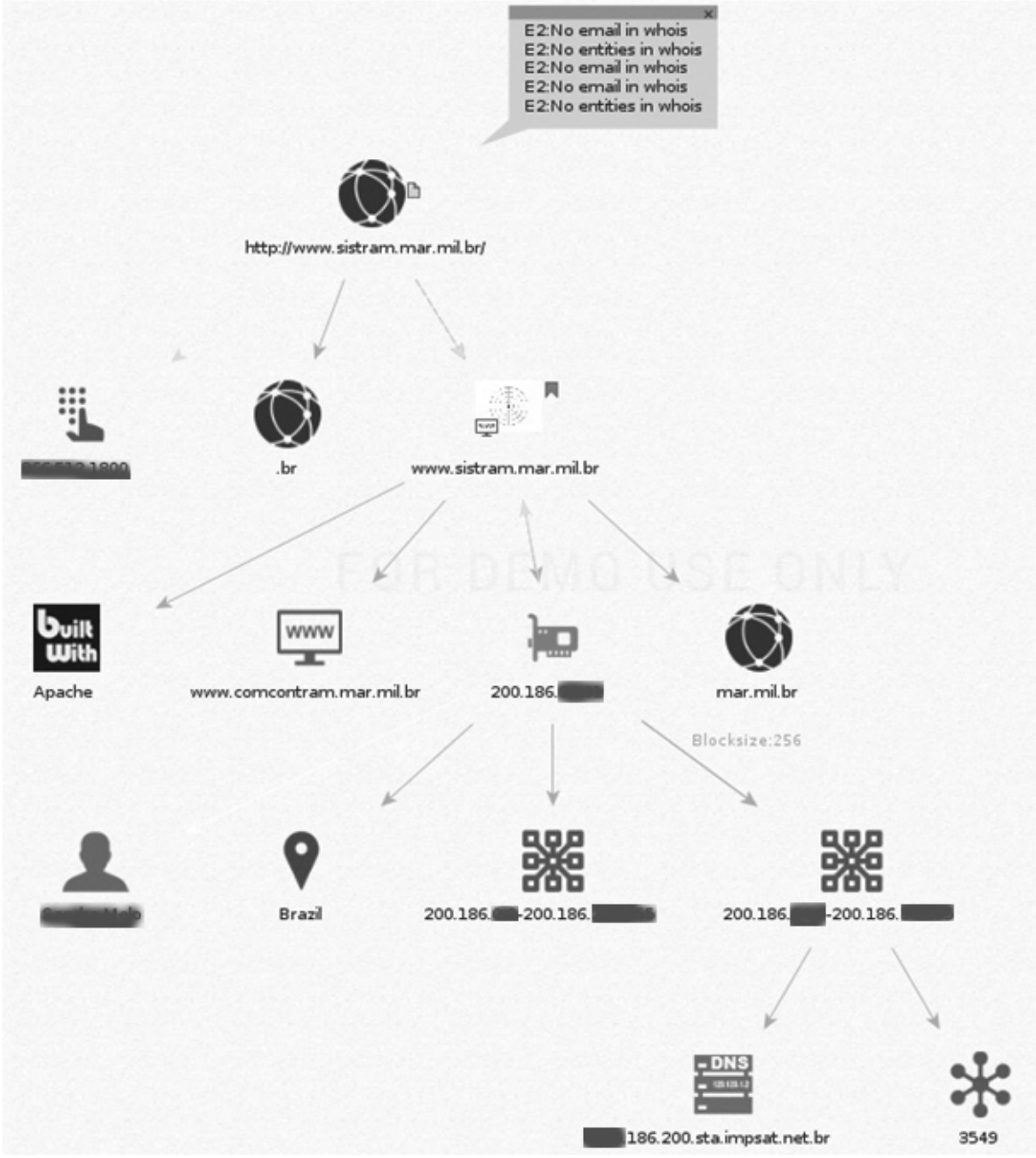


Fonte: https://www.scribd.com/document/318178744/GuiaPratico-OracleLinux

Infere-se, até o momento que, a infraestrutura de web service do Sistram IV é composta por um servidor com sistema operacional Oracle Linux 7.x executando um serviço web Apache (nativo do Linux) com um servidor de aplicação Ajax e um SGBD PostgreSQL.

A utilização de ferramentas automatizadas do Kali Linux ajuda a consolidar esse cenário.

Figura 25 – Tela de resultado de varredura do Maltego 4



Fonte: Maltego 4 CE for Kali Linux

A ferramenta proporciona a confirmação da arquitetura usada no Sistram e ainda nos traz algumas informações valiosas, como a faixa de endereços IP em que esse servidor se encontra a identificação de um possível gestor da rede (muitas vezes, as organizações utilizam nomes falsos para evitar engenharia social).

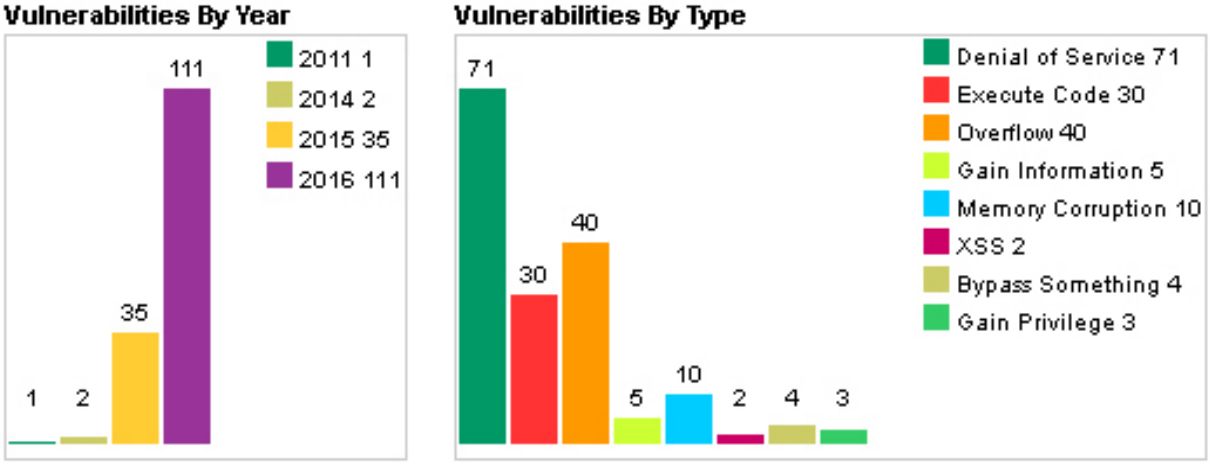
Agora, precisa-se escolher a modalidade de ataque e, para isso, pesquisa-se se os elementos dessa arquitetura possuem vulnerabilidades conhecidas que possibilitem sua utilização.

Oracle Linux:

Figura 26 – Common Vulnerabilities and Exposures (CVE) Oracle Linux

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2011	1														
2014	2	1	1	1							1				
2015	35	21	2	6											
2016	111	49	27	33	10		2			4	4	3			
Total	149	71	30	40	10		2			4	5	3			
% Of All		47.7	20.1	26.8	6.7	0.0	1.3	0.0	0.0	2.7	3.4	2.0	0.0	0.0	



Fonte: http://www.cvedetails.com/product/21375/Oracle-Linux.html?vendor_id=93

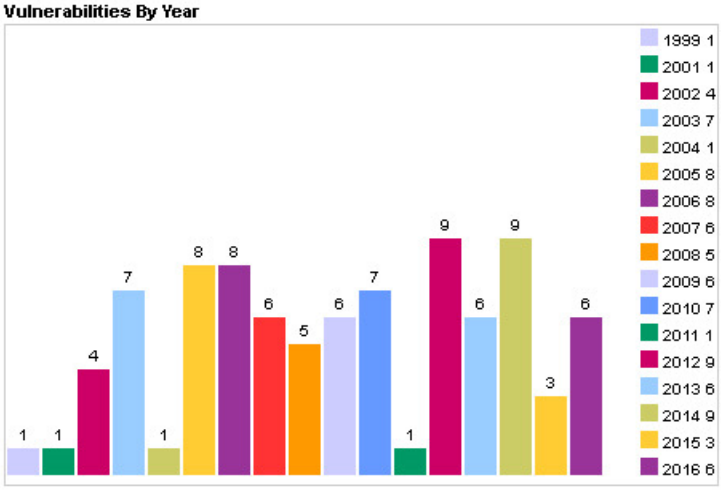
As estatísticas do CVE – Common Vulnerabilities and Exposures (CVE) reduzem as opções de ataque com maior probabilidade de sucesso para o Oracle Linux a: 1 - Denial Of Service; 2 - Execute Code.

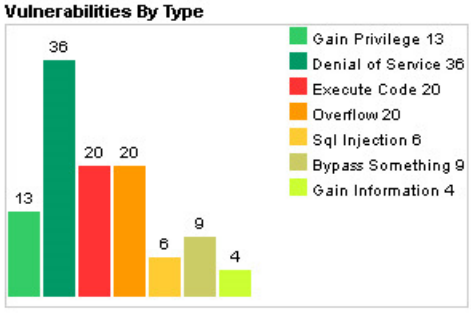
PostgreSQL:

Figura 27 – Common Vulnerabilities and Exposures (CVE) PostgreSQL

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	1											1			
2001	1											1			
2002	4	2	1	1		1									
2003	7	4	6	6											
2004	1	1		1											
2005	8	2	4	2						1					
2006	8	5				2				2		1			
2007	6	2										1			
2008	5	3										2			
2009	6	2								2		2			
2010	7	2	4	2						1		1			
2011	1	1	1	1											
2012	9	2	1	1		2					1				
2013	6	2	1			1				1					
2014	9	2	1	4								2			
2015	3	3		1							1				
2016	6	3	1	1						2	2	2			
Total	88	36	20	20		6				9	4	13			
% Of All		40.9	22.7	22.7	0.0	6.8	0.0	0.0	0.0	10.2	4.5	14.8	0.0	0.0	





Fonte: http://www.cvedetails.com/product/575/?q=Postgresql

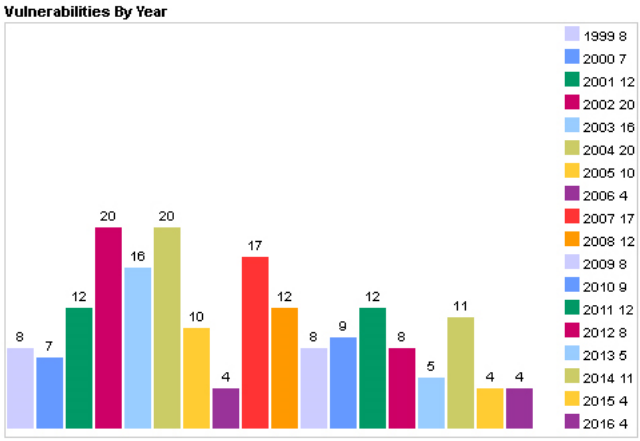
No caso do PostgreSQL, o CVE aponta como as duas melhores opções de ataque o Denial of Service e o Execute Code. O item que aparece em primeiro lugar não é um ataque, é uma falha própria a SGBD que está ligada ao ganho de privilégios.

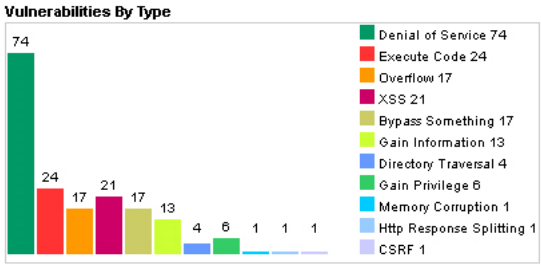
Apache (Http Server):

Figura 28 – Common Vulnerabilities and Exposures (CVE) Apache HTTP Server

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	8	3	2	1											
2000	7		1				1								
2001	12	1								5	1				
2002	20	6	5	3			2	1			2				
2003	16	9	3	1							1				
2004	20	8	2	4				1		3	1	1			
2005	10	5	2	3			3			2					
2006	4	1	2				1			1					
2007	17	5	3				4	2		1	2	1			2
2008	12	2			1		6		1			1	1		
2009	8	5								1		1			1
2010	9	3	2	1			1				3				1
2011	12	8		1								1			2
2012	8	4		1			1				2	1			
2013	5	1	1				2								
2014	11	9	1	2						2	1				1
2015	4	2								1					
2016	4	2								1					
Total	187	74	24	17	1		21	4	1	17	13	6	1		7
% Of All		39.6	12.8	9.1	0.5	0.0	11.2	2.1	0.5	9.1	7.0	3.2	0.5	0.0	





Fonte: https://www.cvedetails.com/product/66/Apache-Http-Server.html?vendor_id=45

Em servidores Http o Denial o Service e o Execute Code também aparecem em primeiro lugar.

AJAX

Sendo o acrônimo em língua inglesa de Asynchronous Javascript and XML, no português "Javascript e XML Assíncrono" caracteriza-se por ser uma combinação de tecnologias como Javascript e XML, providas por navegadores, para tornar páginas web mais interativas com o usuário, utilizando-se de solicitações assíncronas de informações.

Foi inicialmente desenvolvida pelo estudioso Jessé James Garret e mais tarde por diversas associações. Apesar do nome, a utilização de XML não é obrigatória e as solicitações também não necessitam ser assíncronas.

Portanto, o levantamento de vulnerabilidades do AJAX encontra-se intimamente ligado ao conjunto de vulnerabilidades do servidor HTTP.

Em resumo, pode-se concluir que a maior possibilidade de sucesso para um possível ataque cibernético, a plataforma de monitoração do tráfego marítimo utilizada pela Marinha do Brasil, seria advinda de um ataque do tipo ***Denial Of Service***.

Esse tipo de ataque, conforme explanado no capítulo 3 desta pesquisa, é um ataque duro (veja J. NYE 2012, p. 166), ou seja, propõe a indisponibilidade do serviço, geralmente de forma destrutiva (corrupção dos dados do SGBD), sobrecarga de requisições no servidor de acesso, as possibilidades são muitas para enumerá-las.

Sendo uma categoria de ataque de alto poder destrutivo, as etapas: 4 – Extração; 5 – Manutenção de acesso; e 6 – Assalto, nem sempre se concretizam. A etapa 7 – Cobrindo rastros, quando em se tratando de Banco de Dados e Sistemas Operacionais, é a celebração do sucesso do atacante.

O que se pretendeu demostrar neste capítulo foi a complexidade da elaboração de um ataque cibernético, reforçando a ideia de que ele necessita da tríade: motivação, planejamento e financiamento.

6 CONSIDERAÇÕES FINAIS

A pesquisa realizou um estudo exploratório na questão de segurança e defesa do espaço cibernético sob o ordenamento político-administrativo da Marinha do Brasil em seu entorno e confrontou com uma base científica, sob a óptica construtivista das Relações Internacionais.

Observou-se, no transcorrer do trabalho, que a concepção do que é segurança está inicialmente baseada em questionamentos de ordem epistemológica, ontológica e metodológica na Teoria das Relações Internacionais. Lembrando ainda que o conceito de segurança possui uma relação íntima com os desenvolvimentos históricos que têm lugar no sistema internacional com interação dos atores que o compõem.

O estudo da evolução do conceito de segurança nos mostrou como a ideia inicialmente ligada ao indivíduo afasta-se de sua origem até o ponto em que a coletividade (Estado) tornar-se-ia a garantidora dela perante o indivíduo e, numa perspectiva final de seu processo evolutivo, a segurança, agora coletiva, seria o motivador de disputas entre os Estados onde a conquista do poder numa arena internacional anárquica seria o garantidor dessa segurança.

As concepções a respeito do conceito de segurança possuíam a ortodoxia do vínculo com o pensamento realista nas RI. Suas variações ao longo do tempo (clássico, neorrealismo, realismo estrutural e outros) prevaleceram sobre as demais escolas de pensamento até o final do período de Guerra Fria quando acadêmicos do Copenhagen Peace and Research Institute (COPRI) propuseram a ampliação da agenda de segurança internacional.

As reformulações teóricas da agenda dos estudos de segurança, bem como as características de um potencial conflito com o uso da cibernética, estão fortemente baseadas numa concepção pós-acidente nuclear[59], na qual a reposta militar à resolução de conflitos deixa de ser prioritária, com fundamentos na linha de pensamento construtivista em especial aos estudos de Buzan e Weaver e a sua Teoria da Securitização.

O modelo securitizador proposto pela Escola de Copenhagen expande os tipos de ameaça para cinco setores (Militar, Ambiental, Social, Econômico e Político) e estende a qualidade de objeto de referência para indivíduos, sociedades, e atores não estatais, possibilitando que, no presente trabalho, fossem identificados num processo interno da Marinha do Brasil: o objeto a ser securitizado o espaço cibernético da MB, as ameaças identificadas como as oriundas desse novo ambiente, o agente securitizador o EMA, o

[59] Détente Nuclear – vide: ROSECRANCE, Richard. Détente or entente. *Foreign Aff*, v. 53, p. 464, 1974.

discurso securitizador materializado no relatório de Estudos de Estado Maior elaborado pelo GT-TI de 2007, e dentre as medidas de securitização a que culmina com a criação da DCTIM.

No que tange ao espaço cibernético, e a forma como ocorreu o seu "*empoderamento*", ainda se demandam inúmeras discussões, seja acerca de suas possibilidades e capacidades, seja no sentido de estabelecer seus limites.

Ainda que seja verdade que os domínios tradicionais (terrestre, marítimo, aéreo e espacial) gozem de uma maior capacidade de controle, no ciberespaço, essa capacidade de controle e de monitoramento ainda representa um desafio para muitos Estados, até mesmo pela própria natureza e finalidade de origem desse espaço: o de proporcionar rotas alternativas para a continuidade do fluxo da informação.

De forma similar ao domínio cósmico, o espaço cibernético é considerado de uso comum (*global common*) a todos os integrantes do sistema internacional e, uma vez que não possua normatização consistente, o objeto que circula por esse meio – a informação – possui um ator que tem interesse em mantê-la, não só íntegra como também disponível o seu real destinatário. Logo, ainda que trafegue por um ambiente de "domínio público", a informação carrega em si interesses de seus formuladores, transmissores e receptores.

Sabendo-se que em todo espaço onde há ação humana existe um exercício de poder, não se torna viável tratar o espaço cibernético sem a conotação do seu uso para fins políticos e o "domínio sobre esse novo domínio" significa, entre outros, a obtenção e a retenção do poder.

No âmbito da Administração Pública Federal desde o início dos anos 2000, constatou-se uma preocupação do Estado brasileiro no que diz respeito ao tema e de forma gradativa registra-se que a matéria passou de não politizada à politizada e persegue-se uma securitização, a qual é claramente percebida no seio das Forças Armadas motivadas principalmente pelo reconhecimento da questão cibernética, na Estratégia Nacional de Defesa, como um item relevante a segurança nacional.

A transversalidade do espaço cibernético pelos demais domínios, bem como a complexidade de sua composição, a qual envolve infraestruturas transnacionais, nacionais, públicas, privadas, civis e militares, contribui para a sobreposição de atuação de distintos agentes, onde a existência de zonas cinzentas, dificulta o estabelecimento de limites entre o que cabe à segurança e o que se designa à defesa.

Contribuindo para a complexidade no entendimento das ameaças provenientes do espaço cibernético, encontra-se a manifestação do exercício do poder não só por entes do

Estado, como também por uma ordem de organizações que, por interesses diversos, fazem uso deste novo domínio, revelando uma característica intrínseca desta nova realidade dada pela assimetria dos conflitos.

Os resultados observados, com os estudos contidos neste trabalho, bem como a utilização de uma simulação de cenário, mostraram que o espaço cibernético da Marinha do Brasil é depositário de uma diversidade de sistemas que não só facilitam o cotidiano de atividades administrativas, mas também são instrumentos para o exercício de responsabilidade da Autoridade Marítima Brasileira junto à comunidade internacional na garantia da regulação do tráfego marítimo, além da salvaguarda da vida no mar. Sistemas esses críticos e sujeitos a profanações provenientes advindas de um novo domínio de segurança e defesa.

Sendo a Marinha do Brasil pioneira no uso da Tecnologia da Informação e Comunicação no âmbito da Administração Pública Federal, a questão de segurança e defesa do espaço cibernético provocou um rearranjo não só institucional como também normativo e procedimental.

A percepção de uma nova forma de ameaça crescente no cenário internacional resultando num modelo de conflito assimétrico, anônimo e com alto grau de sofisticação tecnológica trouxe como resultado a criação de uma Diretoria Especializada em resposta a um processo securitizador não só da gestão de TIC, como também da defesa cibernética.

A corroboração do processo securitizador dá-se pela sua característica contínua e evolutiva necessitando de ações permanentes no zelo pelo espaço cibernético.

Na Marinha do Brasil, a materialização desta melhoria do processo securitizador dar-se-á com a ativação permanente do Centro de Tratamento de Incidentes de Redes (CTIR), contribuindo assim com aumento da consciência situacional do Poder Naval mediante aos possíveis atos de agressão ao seu entorno cibernético.

REFERÊNCIAS

AMARANTE, José Carlos A. do. A Batalha Automatizada: Um sonho Exequível? *Cadernos de Estudos Estratégicos*. Centro de Estudos Estratégicos da Escola Superior de Guerra, Rio de Janeiro, n. 9, p. 3-18, jul. 2010.

AMERICAN SOCIETY FOR CIBERNETICS FOUNDATIONS. Defining Cibernetic. 2008. Disponível em: <http://www.asc-cybernetics.org/foundations/definitions.htm>. Acesso em: 20 dez. 2015.

AMORIM, Celso. Aspectos da Defesa Cibernética. In: *Seminário de Defesa Cibernética*, 3., 2012, Brasília. Palavras do Ministro da Defesa. Brasília: MD, 2012. Disponível em: <https://www.defesa.gov.br/arquivos/2012/Pronunciamentos/Ministro_defesa/discurso_seminario_defesa_cibernetica_out_2012.pdf>. Acesso em: 20 nov. 2015.

AXELROD, Robert; KEOHANE, Robert O. Achieving Cooperation under Anarchy: Strategies and Institutions. *World Politics*, v. 38, p. 226-254, 1985. [Também disponível em: Cooperation Under Anarchy. OYE, Kenneth (Org.). Princeton: Princeton University Press, 1986].

BARBOSA, Alexandre de Freitas. *O mundo globalizado* – política, sociedade e economia. Contexto, São Paulo, SP, 2001.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília: Assembleia Nacional Constituinte, 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em 03 mai. 2015.

_____. *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Cel Cav Otávio Santana de Rêgo Barros e TC Inf Ulisses de Mesquita Gomes (Orgs.). Presidência da República. Secretaria de Assuntos Estratégicos, 2011. Disponível em: <http://www.sae.gov.br/site/wpcontent/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em 16 dez. 2014.

_____. *Discurso da Presidente, Dilma Rousseff, na abertura do Debate Geral da 68ª AGNU*. Nova Iorque/EUA, 2013. Disponível em: <http://www2.planalto.gov.br/acompanhe-oplanalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-naabertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua>. Acesso em 15 jan. 2015.

_____. *Doutrina Militar de Defesa Cibernética*. Brasília, DF, 2014. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.> Acesso em: 15 jan. 2015.

_____. *Lei 10683/83, Dispõe sobre a Organização da Presidência da República e dos Ministérios, e dá Outras Providências*. Brasília: Congresso Nacional, 2003. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2003/l10.683.htm>. Acesso em: 20 jun. 2016.

_____. *Estratégia Nacional de Defesa. Decreto nº 6.703, De 18 de Dezembro de 2008*.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 12 dez. 2015.

_____. *Estratégia Nacional de Defesa de 2012*. 2012c. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/end.pdf>. Acesso em 11 jan. 2015.

_____. *Glossário das Forças Armadas*. Ministério da Defesa. PORTARIA NORMATIVA nº 9/GAP/MD, de 13 de janeiro de 2016, MD35-G-01 (5ª Edição/2015). Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35_g_01_glossario_ffaa_5_ed_2015.pdf>. Acesso em: 16 ago. 2016.

_____. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*, v. 1. Brasília. Gabinete de Segurança Institucional da Presidência da República, 2010a. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 13 jan. 2015.

_____. *Livro Branco de Defesa Nacional*, 2012a. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 20 jan. 2015.

_____. *Livro Verde*: segurança cibernética no Brasil. Claudia Canongia e Raphael Mandarino Junior (Orgs.). Brasília: GSIPR/SE/DSIC, 2010b. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 2 dez. 2015.

_____. Política Cibernética de Defesa. "Portaria Nº 3.389/MD, de 21 de dezembro de 2012." Edição: Ministério da Defesa. *Diário Oficial [da] República Federativa do Brasil* (Poder Executivo), p. 11-12, 2012b. Disponível em: <http://www.jusbrasil.com.br/diarios/44578940/dou-secao-1-27-12-2012-pg-11>. Acesso em 10 mai. 2015.

_____. *Política Nacional de Defesa. Ministério da Casa Civil*. Subchefia para Assuntos Jurídicos. Decreto Legislativo 818/13, de 12 de setembro de 2013. Brasília. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em: 10 jun. 2015.

_____. Sociedade da Informação no Brasil. In: TAKAHASHI, Tadao (Org.). *Livro Verde*. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: <http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf>. Acesso em: 3 maio 2015.

BUZAN, Barry. *People, States and Fear*. Brighton: Harvester Wheatsheaf, 1983.

_____. *People, states & fear*: an agenda for international security studies in the post-cold war era. 2. ed. Boulder-CO: Lynne Rienner Publishers, 1991.

_____. Rethinking Security after the Cold War. *Cooperation and Conflict*, v. 32, n. 1, p. 5-28, 1997.

_____; WAEVER, Ole; DE WILDE, Jaap. *Security*: a new framework for analysis. Boulder: Lynne Rienner, 1998.

_____; WAEVER, Ole. *Regions and Powers*: The structure of International Security. Cambridge: Cambridge University Press, 2003.

CANONGIA, Claudia. Segurança Cibernética: o desafio da nova sociedade da informação. *Revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos*, v. 14, n. 29, p. 98, 2009.

CARR, Edward Hallett. *Vinte anos de crise*: 1919-1939. Brasília, DF: UnB, 1981.

CARVALHO, Paulo Sergio Melo de. O Setor Cibernético nas Forças Armadas Brasileiras. In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Orgs.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011. p. 13-34.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CLAUDE, Innis. *Power and International Relations*. Nova York: Random House, 1984.

CLARKE, Richard; KNAKE, Robert. *Cyber War*: The Next Threat to National Security and What to Do About It. New York: CCCO, 2010.

CORRÊA, Alexandre José. Operações de Informação: um antigo conceito sob um novo paradigma. *Coleção Meira Mattos*, Rio de Janeiro, v. 3, n. 27, 2012. Disponível em: <http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/14/showToc>. Acesso em: 13 jan. 2016.

DEIBERT, Ron. *Distributed Security as Cyber Strategy*: Outlining a Comprehensive Approach for Canada in Cyberspace. Calgary: Canadian Defense & Foreign Affairs Institute, August, 2012. Disponível em: <http://ebookbrowse.com/distributed-security-as-cyber-strategy-pdf-d380969236>. Acesso em: 10 dez. 2015.

DIZARD, Wilson P. *The coming information age*. New York : Longman, 1982.

DUNN, Myriam. Cyberwar: concepts, status quo, and limitations. *CSS Analysis in Security Police*. ETH Zurich, p. 1-3, 2010. Disponível em: <http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf>. Acesso em: 11 jul. 2016.

EISSA, Sergio G. et. al. El ciberespacio y sus implicancias em la defensa nacional. Aproximaciones al caso argentino. In: *Congresso de Relaciones Internacionales da Universidad Nacional de La Plata*, 6., 2012, La Plata. Disponível em: <http://www.iri.edu.ar/VI_congreso/ponencias/EISSA_GASTALDI_POCZYNOK_ZACARIAS_DI%20TULLIO_el%20ciberesoacio%20y%20sus%20implicancias%20en%20la%20defensa%20nacional.pdf>. Acesso em: 27 nov. 2015.

EPSTEIN, Isaac. *Cibernética*. São Paulo: Ática, 1986.

ESTADOS UNIDOS DA AMÉRICA. Joint Publication 3-13, de 20 de novembro de 2014. Describes techniques for assessing information related capabilities (IRC) and techniques for assessing the integration of the IRCs in support of the joint force commander's objectives. Legislação Federal.

ERIKSSON, Johan ‘Revisiting Copenhagen Observers or Advocates? On the Political Role of Security Analysts’, *Cooperation and Conflict*, n. 3, 311-313, 1999.

FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão dos conflitos do século XXI, p. 53-69, 2012. Disponível em: <http://www.scielo.mec.pt/pdf/ri/n33/n33a05.pdf>. Acesso em: 20 nov. 2016.

FERREIRA, Kelly de Souza. *China e a Ásia Central*: petróleo, segurança e os Estados Unidos. 2012. 99 f. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual de Campinas, Campinas, 2012.

FERREIRA NETO, Walfredo Bento. Política de Fronteiras: elemento aglutinador do Estado-Sociedade, da Defesa-Desenvolvimento (1999-2011). In: *Seminário sobre o Livro Branco de Defesa*, 6., 2011, São Paulo. Disponível em: <http://www.defesa.gov.br/projetosweb/livrobranco/arquivos/apresentacao-trabalhos/artigo-walfredo-bento-neto.pdf>. Acesso em: 20 out. 2015.

_____. *Por uma geopolítica Cibernética*: Apontamentos da Grande Estratégia Brasileira para uma Nova Dimensão da Guerra. 2013. 212 f. Dissertação (Mestrado em Ciências Políticas) – UFF, Niterói, 2013.

FONTENELE, Marcelo Paiva. *Análise e Proposta de Articulação de Esforços no Contexto da Defesa Cibernética da Administração Pública Federal*. 2008. 65 f. Monografia (Especialização em Gestão de Segurança da Informação e Comunicações) – Universidade de Brasília, Brasília, 2008.

GELLNER, Ernest. *Nações e nacionalismo*. Lisboa: Gradiva, 1993.

GIDDENS, Anthony. *O Estado-nação e a Violência*. São Paulo: Edusp, 2001.

HAFTENDORN, Helga. The security puzzle: theory-building and disciplinebuilding in International Relations. *International Studies Quarterly*, v. 35, n. 1, 1990.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly*, n. 53, p. 1155-1175. 2009. Disponível em: <http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>. Acesso em: 05 jan. 2015.

HERZ, John. Idealist Internationalism and the Security Dilemma. *World Politics*, v. 2, n. 2, p. 157-180, 1950.

HUYSMANS, Jef. Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe. *European Journal of International Relations*, v. 4, n. 4, p. 479-505, 1998.

JERVIS, Robert. Cooperation under the Security Dilemma. *World Politics*, v. 30, n. 2, p. 167-214, 1978.

KELSTRUP, Morten. Globalization and societal insecurity: the securitization of terrorism and

competing strategies for global governance. In: GUZZINI, Stefano; JUNG, Dietrich. *Contemporary security analysis and Copenhagen peace research*. Londres: Routledge, 2004.

KEOHANE, Robert. *After hegemony*: cooperation and discord in the world political economy. Princeton: Princeton University, 1984.

KLIMBURG, Alexander. Mobilishing Cyber Power. *Survival*. An IISS (International Institute for Strategic Studies) publication, v. 53. p. 41-60, 2011. Disponível em: http://web.clas.ufl.edu/users/zselden/coursereading2011/Klimcyber.pdf. Acesso em 07 mai. 2015.

LÉVY, Pierre. *Cibercultura*. São Paulo: Ed. 34, 1999.

MACHADO, CARLOS. Guerra Anônima. *Revista Info Exame*, São Paulo, ed. 306, p. 52, ago. 2011.

MANDARINO JR, Raphael. Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético. 2009, 156p. Monografia (Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações) – Universidade de Brasília, Brasília, 2009. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf >. Acesso em: 3 mai. 2016.

MARINHA DO BRASIL. Comando de Operações Navais. *COMOPNAVINST-2301a*: Listas de Verificação de Segurança Orgânica. Rio de Janeiro, RJ: 2013. Disponível em: <http://www.comopnav.mb/secretaria/doc_conf.htm>. Acesso em: 10 jun. 2015.

_____. Diretoria de Comunicações e Tecnologia da Informação da Marinha. *DCTIMARINST 31-02A* 2014: Forense Computacional e Registros de Acesso à Internet. Rio de Janeiro, RJ: 2014. Disponível em: <http://www.dctim.mb/sites/dctim.br/files/DCTIMARINST%2031-02A.pdf>. Acesso em: 10 jun. 2015.

_____. Diretoria de Comunicações e Tecnologia da Informação da Marinha. *DCTIMARINST 31-03* 2011: Gestão de Riscos em Segurança da Informação e Comunicações. Rio de Janeiro, RJ: 2011. Disponível em: <http://www.dctim.mb/sites/dctim.br/files/DCTIMARINST%2031-03.pdf>. Acesso em: 10 jun. 2015.

_____. Diretoria de Comunicações e Tecnologia da Informação da Marinha. *DCTIMARINST 31-04*: Utilização de Recursos Criptológicos na Marinha. Rio de Janeiro, RJ: 2012a. Disponível em: <http://www.dctim.mb/sites/dctim.br/files/DCTIMARINST%2030-09A.pdf>. Acesso em: 10 jun. 2015.

_____. Diretoria de Comunicações e Tecnologia da Informação da Marinha. *DCTIMBOTEC-31/002/2013*: Requisitos de SID para Homologação de SD. Rio de Janeiro, RJ: 2013. Disponível em: <http://www.dctim.mb/sites/dctim.br/files/DCTIMBOTEC%2031-002-2013%20-%20Requisitos%20de%20SID%20para%20Homologacao%20de%20SD.pdf>. Acesso em: 10 jun. 2015.

_____. Diretoria de Comunicações e Tecnologia da Informação da Marinha. *DCTIMBOTEC-31/005/2014*: Configuração para Conexão Remota segura a Servidores. Rio de Janeiro, RJ:

2014. Disponível em: <http://www.dctim.mb/sites/dctim.br/files/DCTIMBOTEC%2031-005%20-%20ConfiguracaoSSH.pdf>. Acesso em: 10 jun. 2015.

_____. Estado Maior da Armada. *EMA-414 REV1*: Normas para a Salvaguarda de Materiais Controlados, Dados, Informações, Documentos e Materiais Sigilosos na Marinha (Rev.1). Rio de Janeiro, RJ: 2012. Disponível em: <http://www.ema.mb/docs/publicacoes/EMA-414.zip>. Acesso em: 10 jun. 2015.

_____. Estado Maior da Armada. *EMA-416 REV1*: Doutrina de Tecnologia da Informação da Marinha. Rio de Janeiro, RJ: 2012. Disponível em: <http://www.ema.mb/docs/publicacoes/EMA-416Rev1.zip>. Acesso em: 10 jun. 2015.

_____. Estado Maior da Armada. *EMA-416 REV1 Vol. 2*: Doutrina de Tecnologia da Informação da Marinha (Manual de Guerra Cibernética Volume II). Rio de Janeiro, RJ: 2013. Disponível em: <http://www.ema.mb/docs/publicacoes/EMA-416Rev1.zip>. Acesso em: 10 jun. 2015.

MATHEWS, Jessica T. Redefining Security. *Foreign Affairs*, v. 68, n. 2, p. 162-177, 1989.

MCSWEENEY, Bill. *Security, Identity and Interests*: a Sociology of International Relations. Cambridge: Cambridge University Press, 1999.

MEARSHEIMER, John J. Back to the Future: Instability in Europe After the Cold War. *International Security*, v. 15, p. 5-56, 1990.

MORAN, Daniel. Geography and Strategy. In: BAYLIS, J.; WIRTZ, J. J.; GRAY, C. S. *Strategy in the Contemporary World*: An Introduction to Strategic Studies. 3. ed. New York: Oxford University Press, 2010. p. 124-140.

MOREIRA, Marcílio Marques. Karl Deutsch, a Política e a Cibernética. In: *Deutsch na UNB*: conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980. Brasília: Editora da UNB, 1980.

MORGENTHAU, Hans Joachim. *A política entre as nações*: a luta pelo poder e pela paz. São Paulo: Imprensa Oficial do Estado de São Paulo; Brasília: Ed. UnB: IPRI, 2003 [1948].

NUNES, Luiz Artur Rodrigues. *Guerra Cibernética*: Está a MB preparada para enfrentá-la. Monografia do Curso de Política e Estratégia Marítimas. Rio de Janeiro, Escola de Guerra Naval, 2010. Disponível em: <https://www.egn.mar.mil.br/arquivos/biblioteca/monografias/cpem/2010/CMG(FN)%20RODRIGUES%20-%20OSTENSIVO.pdf>. Acesso em: 15 maio 2015.

NYE, Joseph S. *O Futuro do Poder*. São Paulo: Benvirá, 2012.

NYE JR, Joseph. Cyber Power. Harvard Kennedy School, Belfer Center for Science and International Affairs. 2010. Disponível em: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. Acesso em: 19 out. 2016.

_____. Guerra e paz no ciberespaço. *Estado de São Paulo*, 2012. Disponível em: <http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no-ciberespaco-,861242,0.htm>.

Acesso em: 15 out. 2016.

OBAMA, Barack. *State of Union Speech*, Washington, DC, 12 fev. 2013. Disponível em: <https://www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address-prepared-delivery>. Acesso em: 1 ago. 2016.

OLIVEIRA, João Roberto de. Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional. In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011. p. 105-128.

PERES, João Roberto. A vez da governança corporativa. *Revista Abinee*, n. 43, p. 25, out. 2007. Disponível em: <http://www.abinee.org.br/informac/revista/43j.pdf>. Acesso em: 16 ago. 2016.

POSEN, Barry R. Command of the Commons: The Military Foundation of U.S. Hegemony. *International Security*, v. 28, n. 1, p. 5-46, summer, 2003. Disponível em: <http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf>. Acesso em: 20 set. 2015.
WAEVER, Ole. Aberystwyth, Paris, Copenhagen - New 'Schools' in Security Theory and their Origins between Core and Periphery. Paper presented at the Hotel, Montreal, Quebec, Canada, Mar 17, 2004. Disponível em: <www.isanet.org> ou <http://www.allacademic.com/meta/p74461_index.html>. Acesso em: 21 maio 2016.

_____. Discourse Analysis as Foreign Policy Theory: The case of Germany and Europe. In: *Center for German and European Studies*. University of California at Berkley: Working Papers (Unpublished). Disponível em: <http://www.ciaonet.org/wps/wao01/>. Acesso em: 11 set. 2016.

_____. Peace and Security: two concepts and their relationship. In: GUZZINI, Stefano; JUNG, Dietrich. *Contemporary security analysis and Copenhagen peace research*. Londres: Routledge, 2004.

_____. Securitisation and Desecuritisation. In: LIPSCHUTZ, Ronnie D. *On Security*. New York: Columbia University Press, 1995.

_____. Security, the Speech Act: Analyzing the Politics of a Word. *Working Paper*. Copenhagen: Center for Peace and Conflict Research, 1989.

WIENER, Norbert. *Cibernética e Sociedade*: o uso humano de seres humanos. 4. ed. São Paulo: Cultrix, 1973.

RAFFESTIN, Claude. *Por uma Geografia do Poder*. São Paulo: Ática, 1993.

REVERON, Derek S. *Cyberspace and National Security*: Threats, Opportunities and Power in a Virtual World. Washington D. C.: Georgetown University Press, 2012.

RODRIGUES, Alexandre Reis. Portugal e o espaço estratégico de interesse. In: *Jornal de Defesa e Relações Internacionais*. Revista Segurança e Defesa, Loures: Diário de Bordo Editores, 2012. Disponível em:

<http://database.jornaldefesa.pt/politicas_de_defesa/portugal/JDRI%20009%20221112%20Portugal%20e%20o%20espa%C3%A7o%20interesse.pdf>. Acesso em: 27 nov. 2015

ROTHSCHILD, Emma. What is security? The Quest for World Order. *Daedalus*: Journal of the American Academy of Arts and Sciences, v. 124, n. 3, p. 53-98, 1995.

ROSECRANCE, Richard. Détente or entente. *Foreign Aff*., v. 53, p. 464, 1974

SALES, João Rufino de. *Guerra Cibernética*. Palestra proferida no II Congresso sobre Crimes Virtuais e Formas de Proteção. Federação do Comércio de São Paulo, São Paulo, em 28 set. 2010. Disponível em:<http://www.ebah.com.br/content/ABAAABQZQAG/guerra-cibernetica-joao-rufino>. Acesso em: 22 jun. 2016.

SAQUET, Marcos Aurelio. *Abordagens e concepções sobre território*. São Paulo: Expressão Popular, 2007.

SANTOS, General José Carlos: "Podemos recrutar hackers". [Brasília]. *Revista Época*, 15 jul. 2011. Entrevista concedida a Leandro Loyola. Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.htm> . Acesso em: 20 jul. 2016.

SHAKARIAN, Paul. Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008. *Military Review*, p. 67-74, nov./dez. 2011.

SHEEHAN, Michael. *International security*: an analytical survey. Boulder, Colo: Lynne Rienner, 2005.

SILVEIRA, Fernando Malburg da. "Cyberwarfare: a nova dimensão da guerra". *Revista do Clube Naval*, ano 119, n. 360, out./nov./dez. 2011.

SOUZA, Eduardo André A; NUNES, Nival de Almeida. A Questão da Segurança e Defesa do Espaço Cibernético brasileiro, e o Esforço Político-administrativo do Estado. *Revista da Escola de Guerra Naval*, Rio de Janeiro, v. 22, n 2, mai/ago. 2016.

TANNO, Grace. A Contribuição da Escola de Copenhague aos Estudos de Segurança Internacional. *Contexto Internacional*, v. 25, n. 1, p. 47-80, jan./jul. 2003.

THEOPHILO, Roque. A História da Cibernética. Disponível em <http://www.psicologia.org.br/internacional/ap10.htm>. Acesso em: 3 out. 2015.

TOFFLER, Alvin; TOFFLER, Heidi. *Guerra e Antiguerra*: sobrevivência na aurora do terceiro milênio. Rio de Janeiro: Biblioteca do Exército, 1995.

TOURÉ, Hamadoun. ONU organiza primeira simulação contra ataques cibernéticos. Organização das Nações Unidas no Brasil, 2 dez. 2011. Disponível em: <http://www.onu.org.br/onu-organiza-primeira-simulacao-contra-ataques-ciberneticos/>. Acesso em: 12 maio 2016.

ULLMAN, Richard. *Redefining Security. International Security*, v. 8, p. 129-153, 1983.

VENTRE, Daniel. Ciberguerra. In: *Seguridad Global y Potencias Emergentes em un Mundo Multipolar, XIX Curso Internacional de Defensa*, 2011. Zaragoza: Imprenta Ministerio de Defensa, 2012. p. 32-45.

VELOSO, Rubem Ribeiro. *Avaliação de Conformidade a Modelos de Gestão de Segurança da Informação na Marinha do Brasil*. 2008. Monografia (Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações) – Universidade de Brasília, Brasília, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf >. Acesso em: 10 maio 2016.

VIZENTINI, Paulo Fagundes. *Guerra do Vietnã*. 3. ed. Porto Alegre: Editora: UFRGS, 2006. 120p.

WAEVER, Ole. Aberystwyth, Paris, Copenhagen – New 'Schools' in Security Theory and their Origins between Core and Periphery. Paper presented at the Hotel, Montreal, Quebec, Canada, Mar 17, 2004. Disponível em: <http://www.isanet.org>. Acesso em: 21 maio 2015.

_____. Security, the Speech Act: Analyzing the Politics of a Word. *Working Paper* Copenhagen: Center for Peace and Conflict Research, 1989.

WALT, Stephen. The Renaissance of Security Studies. *International Studies Quarterly*. v. 35, p. 211-239, 1991.

WALTZ, Kenneth. *Theory of International Politics*. Reading, Mass: Addison-Wesley, 1979.

WIENER, Norbert. *Cibernética e Sociedade*: o uso humano de seres humanos. 4. ed. São Paulo: Cultrix, 1973.