MARINHA DO BRASIL

ESCOLA DE GUERRA NAVAL

MESTRADO PROFISSIONAL EM ESTUDOS MARÍTIMOS

SARA MARTINS IBRAHIM PAZ

CIÊNCIA, TECNOLOGIA E INOVAÇÃO NA GUERRA: REFLEXÕES PARA A DEFESA CIBERNÉTICA BRASILEIRA A PARTIR DO ESTUDO DE CASOS INTERNACIONAIS.

Rio de Janeiro

2019

SARA MARTINS IBRAHIM PAZ

CIÊNCIA, TECNOLOGIA E INOVAÇÃO NA GUERRA: REFLEXÕES PARA A DEFESA CIBERNÉTICA BRASILEIRA A PARTIR DO ESTUDO DE CASOS INTERNACIONAIS.

Dissertação apresentada ao curso de Mestrado Profissional em Estudos Marítimos da Escola de Guerra Naval, como requisito parcial à obtenção do grau de Mestre(a) em Estudos Marítimos.

Área de Concentração em Segurança, Defesa e Estratégia Marítima.

Orientador: Prof. Dr. Claudio Rodrigues Corrêa

Rio de Janeiro, 2019.

P348c Paz, Sara Martins Ibrahim
Ciência, tecnologia e inovação na guerra: reflexões para a defesa cibernética brasileira a partir do estudo de casos internacionais / Sara Martins Ibrahim Paz. __ Rio de Janeiro, 2019.
116 f.. : il.

Dissertação (Mestrado) - Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos (PPGEM), 2019.
Orientador: Claudio Rodrigues Corrêa.

Bibliografia: f. 100 - 107.

1. Defesa Nacional 2. Cibernética 3. Guerra cibernética - Ciência militar 4. Ciberespaço. I. Escola de Guerra Naval (BRASIL). II.Título.

CDD 355.0091

Ficha catalográfica elaborada pela bibliotecária
Marjourie A. Araujo Cruz Marques – CRB7/6818
Biblioteca da Escola de Guerra Naval

Sara Martins Ibrahim Paz

CIÊNCIA, TECNOLOGIA E INOVAÇÃO NA GUERRA: REFLEXÕES PARA A DEFESA CIBERNÉTICA BRASILEIRA A PARTIR DO ESTUDO DE CASOS INTERNACIONAIS.

Dissertação apresentada ao curso de Mestrado Profissional em Estudos Marítimos da Escola de Guerra Naval, como requisito parcial à obtenção do grau de Mestre(a) em Estudos Marítimos.
Área de Concentração em Segurança, Defesa e Estratégia Marítima.

Aprovada em 28 de agosto de 2019.

BANCA EXAMINADORA

_____

CMG (RM1 IM), Prof. Dr. Claudio Rodrigues Corrêa –
Orientador EGN

_____

Prof. Dr. Nival Nunes de Almeida
EGN

_____

Prof. Dr. Alan Oliveira de Sá
CIAW

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida terrena e vindoura, pela sua graça infinita e imerecida. Agradeço pelas dádivas recebidas, pelas pessoas e oportunidades que Ele coloca em meu caminho.

Papai e mamãe: muito obrigada pelas orações, orientação, abnegação e instrução. Nenhuma escola no mundo substitui o bom ensinamento no lar. Agradeço ao meu marido Thiago, que no primeiro ano de casamento esteve ao meu lado durante o turbilhão da minha jornada na empresa e no mestrado. Paulo, meu irmãozinho querido, obrigada pelas horas sem sono, gastas na revisão do trabalho. Tias, obrigada pelo amor dedicados desde o meu nascimento.

Agradeço ao meu orientador Cláudio Corrêa por não desistir de me orientar. Suas palavras de ânimo e ajuda durante todo o processo foram fundamentais para que eu conseguisse terminar o TCC. Muito obrigada pelo empenho e paciência demonstrados.

Agradeço ao corpo docente do PPGEM pelos ensinamentos valiosos durante todo o curso. Os senhores são excelentes e dedicados aos alunos. Obrigada Marisol e Valdir por atenderem sempre com esmero e simpatia. Valdir, agradeço especialmente por sempre fazer contato e me lembrar que faltava “pouco” para a conclusão de mais uma etapa.

Meu muito obrigada aos integrantes da banca Dr. Nival Nunes de Almeida e Dr. Alan Oliveira de Sá, que fizeram observações pertinentes e colaborativas durante o processo de elaboração do trabalho. Agradeço também ao CMG RM1 FN William Alves Rosa, especialista no assunto e professor na Escola de Guerra Naval, pelo tempo dispensado falando sobre guerra cibernética, pela leitura prévia das perguntas do questionário e até empréstimo de livro.

Aos meus queridos professores Gisela Madureira e Pablo Laignier: suas aulas deixaram saudades. O zelo e o prazer de vocês em ensinar de maneira tão maravilhosa me encorajaram a dar um passo além da graduação. Obrigada, mestres.

Ohara, agradeço pela cooperação durante a pós-graduação, por me informar sobre o mestrado da EGN e incentivar que eu tentasse uma vaga. Obrigada a todos os respondentes que dispuseram do tempo precioso para responder às perguntas do questionário.

A maquinaria do Estado-nação, inventada e cultivada para garantir a soberania territorial e separar claramente os de dentro dos de fora, foi apanhada despreparada pelo “cabeamento” do planeta. Dia após dia, uma atrocidade terrorista após outra, as instituições de lei e ordem dirigidas pelo Estado aprendem sobre sua própria inépcia em lidar com os novos perigos que gritantemente atacam as categorias e distinções ortodoxas consagradas, aparentemente testadas e confiáveis. (ZYGMUNT BAUMAN: 2008)

Ainda há muito a ser inventado. Muita coisa ainda vai acontecer. Ninguém ainda faz ideia do impacto que a internet produzirá e de que em muitos aspectos estamos apenas no primeiro dia. (JEFF BEZOS)

RESUMO

Este estudo tem como objetivo pesquisar sobre a inovação da tecnologia, que possibilita uma nova forma de fazer guerra através do ciberespaço. A revisão de literatura usada como base para o estudo busca compreender os conceitos relacionados ao avanço da tecnologia ligados à Guerra Cibernética. O estudo é direcionado para identificação e descrição de conceitos relacionados à guerra cibernética e do arcabouço relativo à gestão da segurança e defesa cibernética no Brasil. Dada a natureza do estudo, a pesquisa aplica o método de estudo de caso envolvendo guerras cibernéticas já ocorridas. Os casos foram selecionados pela documentação acessível, impactos causados e repercussão internacional. Visando contribuir com reflexões passíveis de serem aplicadas à proteção cibernética brasileira, elaborou-se um questionário com perguntas abertas, enviado para especialistas na área. Quatorze profissionais contribuíram com sugestões para a melhoria da proteção cibernética do Brasil. Os resultados da pesquisa apontam que o avanço da tecnologia cria novas vulnerabilidades para os países, que podem não ter estrutura para combater uma possível guerra cibernética. Dentre as reflexões apreendidas ao longo da pesquisa, destaca-se a necessidade de fomentar o estudo acadêmico relacionado ao assunto; criação de planos de defesa cibernética e de contingenciamento em caso de ataque; estudo e melhoria constantes; continuação de boas práticas já adotadas, bem como a proteção de infraestruturas críticas. O presente estudo deixa patente a necessidade de investimento em Ciência, Tecnologia e Inovação para que o país esteja preparado para enfrentar as novas ameaças.

Palavras-chave: Guerra Cibernética. Defesa Nacional. Ataques Cibernéticos. Ciberespaço.

ABSTRACT

This research aims to study the innovation of technology, which enables a new way to make war through cyberspace. The literature review used as a basis for the study seeks to understand the concepts connected to technology advance linked to the Cyber War. The study identifies and describes concepts related to cyber warfare and the framework related to the management of cyber security and cyber defense in Brazil. By the nature of the study, the research applies the case study method involving cyber wars that have already occurred. The cases were selected by accessible documentation, impacts caused and international repercussions. Aiming to contribute lessons that could be applied to Brazilian cyber protection, a questionnaire with open questions was prepared and sent to experts in the field. Fourteen professionals provided suggestions for improving cyber protection in Brazil. Research results show that the advancement of technology creates new vulnerabilities for countries, which may lack the structure to combat cyber warfare. Among the lessons learned throughout the research, there is the need to foster society's awareness; increase academic study related to the subject; creation of cyber defense and contingency plans in case of attack; constant study and improvement; continuation of good practices already adopted, as well as the protection of critical infrastructures. This study shows the need for investment in science, technology and innovation so that the country is prepared to face the new threats.

Keywords: Cyber War. National Defense. Cyber Attacks. Cyberspace.

LISTA DE ILUSTRAÇÕES

Figura 1 - Ciberespaço 28
Figura 2 - Níveis de decisão no contexto do Ministério da Defesa, referentes às ações no Espaço Cibernético 31
Figura 3- Documentação brasileira relativa à cibernética, produzida entre 2007 e 2017 64
Figura 4 - Linha temporal dos ataques cibernéticos internacionais entre 1982 e 2015 83

LISTA DE ABREVIATURAS E SIGLAS

AOL – American On-line

CASNAV – Centro de Análise de Sistemas Navais

CDCiber – Centro de Defesa Cibernética

CGI.br – Comitê Gestor da Internet no Brasil

CT&I – Ciência, Tecnologia e Inovação

DARPA – *Defense Advanced Research Projects Agency*

DCA – *Defense Communication Agency*

DDoS – *Distributed Denial of Service*

DSIC – Departamento de Segurança da Informação e Comunicações

END – Estratégia Nacional de Defesa

EMA – Estado Maior da Armada

ENIAC – *Electrical Numerical Integrator and Calculator*

EUA – Estados Unidos da América

GC – Guerra Cibernética

GSI-PR – Gabinete de Segurança Institucional da Presidência da República

IGF – *Internet Governance Forum*

IoT – *Internet of Things*

IP – *Internet Protocol*

LBDN – Livro Branco de Defesa Nacional

LP – Linha de Pesquisa

MD – Ministério da Defesa

MJ – Ministério da Justiça

MRE – Ministério das Relações Exteriores

NSF – *National Science Foundation*

NSA – Agencia de Segurança Nacional Norte-Americana

PETIM – Plano Estratégico de Tecnologia da Informação da Marinha

PND – Política Nacional de Defesa

RBN – *Russian Business Network*

RFID – *Radio-Frequency Identification*

SCADA – *Supervisory Control and Data Acquisition*

TCP – *Transmission Control Protocol*

WWW – *World Wide Web*

SUMÁRIO

1. INTRODUÇÃO 12
1.1. Delimitação do tema 12
1.2. Objetivos 12
1.2.1. Objetivo Geral 12
1.2.2. Objetivos Específicos 12
1.3. Justificativa 12
1.4. Hipótese e variáveis 16
1.5. Metodologia 16
1.5.1. Método de abordagem 16
1.5.2. Fases da pesquisa 16

CAPÍTULO 2: PANORAMA SOBRE A GESTÃO DA SEGURANÇA E DA DEFESA CIBERNÉTICA 17
2.1. Definição dos termos 18
2.1.1. Guerra 19
2.1.2. Guerra Cibernética 19
2.1.3. Guerra Cinética 22
2.1.4. Guerra Centrada em Redes 23
2.1.5. Tecnologia 24
2.1.6 Internet/ Ciberespaço 25
2.1.7. Defesa/ Defesa Cibernética 29
2.1.8. Segurança/ Segurança Cibernética 31
2.1.9. Ataque Cibernético 32
2.1.10. Crime Cibernético/Cibercrime 33
2.2. Da ARPANET à Internet das Coisas 34
2.3. Novos desafios no Ciberespaço 42
2.4. Guia de Defesa Cibernética na América do Sul 47
2.5. Políticas brasileiras para a Segurança e Defesa Cibernética.....48
2.5.1. Livro Verde: Segurança Cibernética no Brasil 49
2.5.2. Política Nacional de Defesa (PND) 51
2.5.3. Estratégia Nacional de Defesa (END) 52

2.5.4. Livro Branco de Defesa Nacional (LBDN) 53
2.6. Lei Nº 12.737/2012, a “Lei Carolina Dieckmann” 55
2.7. Lei Nº 12.965/2014, o Marco Civil da Internet 58
2.8. Marinha do Brasil e a cibernética 61
2.9. Pontos tratados no capítulo 2 usados para análise dos casos internacionais 65

CAPÍTULO 3: ATAQUES CIBERNÉTICOS INTERNACIONAIS 66
3.1. 1982: Ataque contra a União Soviética 67
3.2. 2007: Ataque contra a Estônia 69
3.3. 2007: Ataque contra a Síria 72
3.4. 2008: Ataque contra a Geórgia 75
3.5. 2009: Ataque contra o Irã 77
3.6. 2015: Ataque contra setores público e privado norte-americanos 82

CAPÍTULO 4: ANÁLISE DAS RESPOSTAS 83
4.1. Análise da resposta à questão 1 86
4.2. Análise da resposta à questão 2.....87
4.3. Análise da resposta à questão 3 91
4.4. Análise da resposta à questão 4 92
4.5. Análise da resposta à questão 5 93
4.6. Análise da resposta à questão 6 94
4.7. Análise da resposta à questão 7 95

5. REFLEXÕES A PARTIR DOS CASOS INTERNACIONAIS 96
6. CONCLUSÃO 98
REFERÊNCIAS 100
ANEXO A 108
ANEXO B 111

1. INTRODUÇÃO

1.1. DELIMITAÇÃO DO TEMA

A pesquisa busca compreender o impacto dos avanços ligados à tecnologia computacional no que concerne à defesa nacional. O período teórico do estudo se inicia em 1969, com a criação da ARPANET. Serão estudados os conceitos ligados à Guerra Cibernética. Haverá a posterior exemplificação de ataques virtuais ocorridos em sistemas cibernéticos, com o fito de roubo de dados, destruição de informações ou ataques de negação de serviço.

1.2 OBJETIVOS

1.2.1 GERAL

Identificar possíveis reflexões para a proteção cibernética brasileira a partir do exame de casos de ataques cibernéticos internacionais.

1.2.2 ESPECÍFICOS

1.2.1. Analisar o avanço da tecnologia da Internet desde a sua criação.

1.2.2. Conceituar termos relacionados à Guerra Cibernética.

1.2.3. Examinar seis casos de ataques cibernéticos internacionais, que envolveram ações de uma nação-estado executando o ataque.

1.2.4. Examinar a regulamentação do setor cibernético para defesa do Brasil.

1.2.5. Analisar potenciais aprendizados para a defesa cibernética brasileira a partir desses casos.

1.3. JUSTIFICATIVA

O tema proposto tem aderência à linha de pesquisa LP III- Ciência, Tecnologia, Inovação e Poder Marítimo, do Programa de Pós-Graduação em Estudos Marítimos. O estudo da LP III é baseado no desenvolvimento da Ciência, Tecnologia e Inovação (CT&I). Através da história da CT&I é possível observar as mudanças sociais provocadas e apresentar perspectivas para o devir[1].

[1] ESCOLA DE GUERRA NAVAL. PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS MARÍTIMOS. Área de Concentração e Linhas de Pesquisa. Disponível em <https://tinyurl.com/y6qbnp64>. Acesso em 20 set. 2019.

As tecnologias computacionais promovem novas possibilidades de interação, sociabilidade, produção de conhecimento e difusão de ideias. Além de suscitar ameaças para os que estão conectados, existe a possibilidade de ataque a computadores que não estão conectados à internet, nem fazem conexão com nenhum outro sistema conectado à rede mundial. É o chamado "*air gap*". É possível atacar tais computadores e/ou dispositivos pelos meios eletromagnético, acústico, térmico e óptico (NOHE: 2018).

A Estratégia Nacional de Defesa (END) foi estabelecida pelo Decreto Nº 6.703, de 18 de dezembro de 2008. O Decreto preconiza que Estratégia nacional de defesa é indissociável de estratégia nacional de desenvolvimento. (BRASIL, 2008). A END prevê que a independência nacional é "alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento." (BRASIL, 2008, p. 44). A pesquisa proposta visa contribuir para apresentar e exemplificar as novas ameaças tecnológicas no campo cibernético.

A soberania de um Estado Nacional também pode sofrer ataques através da conexão cibernética. No primeiro semestre de 2017, pessoas e organizações em mais de 150 países foram atacadas pelo *malware* WannaCry (BAIG, 2018). O *software* malicioso bloqueou o acesso de sistemas e arquivos de computadores infectados. Para a liberação do acesso, os *hackers*[2] cobraram pagamento de resgate. De acordo com uma das maiores empresas de segurança no mundo, a AVAST, o Brasil foi um dos principais alvos do ataque (AVAST: 2018). Órgãos do governo, universidades, empresas ferroviárias e hospitais foram atingidos com o ataque. O ataque é um alerta sobre o quão vulnerável são os dados que circulam na Internet. As novas tecnologias da informática ratificam a necessidade de atentar para a questão de defesa e segurança cibernética.

O Ministério da Defesa, órgão federal criado em 1999, tem como uma de suas tarefas fundamentais o estabelecimento de políticas de Defesa e Segurança no país. Em setembro de 2018, o Ministério da Defesa sofreu uma invasão que acarretou na exposição de dados pessoais do General da reserva do Exército Hamilton Mourão e do General Eduardo Villas Bôas. Na época do ataque, Mourão era candidato à vice-presidência do país e Villas Bôas era o

[2] JUSBRASIL. Hackers, Crackers e o Direito Penal. De origem na língua inglesa, o termo hacker surgiu por volta de 1990 com a popularização da internet, e significa aquele que se dedica a conhecer e modificar aspectos internos de aplicativos, programas e redes de computadores. Muitos hackers são contratados por grandes empresas para testar seus dispositivos de segurança informática. Já o cracker é aquele que explora as atividades dos sistemas e da tecnologia da informação para a prática de delitos, é o hacker mal-intencionado. Disponível em < https://tinyurl.com/y2ynq6n8>. Acesso em: 20 out. 2018.

Comandante do Exército Brasileiro. Na invasão, além de acessarem o banco de dados do Ministério, os *hackers* também divulgaram "informações como endereço, nomes, documentos oficiais e tabelas com informações como dados bancários de ambos os generais" (WAKKA: 2018).

Em junho de 2019, *hackers* invadiram o celular do atual Ministro da Justiça e Pública do Brasil, Sérgio Moro. Além da invasão, houve o vazamento de conversas entre o então ministro da justiça Sérgio Moro (na época em que atuava como juiz federal na operação Lava Jato) e o procurador Deltan Dallagnol, procurador da República (BOMFIM: 2019). O ministro percebeu que havia algo errado quando recebeu uma ligação do próprio número de celular. O ministro da justiça Sérgio Moro trocou o número da linha e não soube a princípio que sua conta no Telegram[3] fora invadida. A Polícia Federal iniciou investigações sobre o ocorrido.

Tanto os responsáveis pelo serviço Telegram quanto o Ministro Sérgio Moro usaram suas contas no Twitter[4] para comentar sobre o assunto. O Ministro Sérgio Moro, que usa o perfil @SF_Moro, disse em 11 de junho de 2019 que "além de juízes e procuradores, jornalistas também tiveram celulares hackeados pelo mesmo grupo criminoso" e anexou uma reportagem de O Globo com o título "Jornalista do GLOBO teve conta em aplicativo de mensagens hackeada" (https://twitter.com/SF_Moro). Os Responsáveis pelo Telegram informaram que não haviam evidências que comprovassem que o aplicativo em si havia sido *hackeado* (LOPES, 2019). Usando a conta do Twitter @telegram, a empresa informou também em 11 de junho de 2019 que "Na verdade, não há evidências de qualquer invasão. Provavelmente, houve *malware* ou alguém que não está usando uma senha de verificação em duas etapas." (https://twitter.com/telegram) (tradução nossa).

Adicionalmente, o Telegram incluiu um link (https://telegra.ph/Keeping-your-chats-secure-06-10) que ensina aos usuários como manter a conta segura, como configurar a verificação de senha em duas etapas e como usar bate-papos secretos (onde é possível ativar um temporizador para apagar as mensagens depois de um tempo programado pelo usuário). Em

[3] Telegram é um aplicativo para troca de mensagens de texto, imagens, áudios e vídeos. O Telegram existe desde 2013 e ganhou popularidade no Brasil após os bloqueios do WhatsApp pela justiça em 2015 e 2016. G1. WhatsApp bloqueado: Relembre todos os casos de suspensão do app. Disponível em <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html>. Acesso em 12 jun. 2019.

[4] O Twitter é uma ferramenta de micromensagens. O usuário tem a limitação de 280 caracteres por mensagem. Essas mensagens são chamadas de tweet, que significa "pio". O logotipo da empresa é um pássaro azul, que remete a esse som. Na versão em português, o Twitter pergunta para os usuários cadastrados "O que está acontecendo?" Significados. Significado de Twitter. Disponível em <https://www.significados.com.br/twitter/>. Acesso em 12 jun. 2019.

12 de junho de 2019, também através do Twitter, o Telegram informou que sofreu ataques DDoS (Distributed Denial of Service, ou, em português, ataque distribuído de negação de serviço): "No momento, estamos enfrentando um poderoso ataque DDoS, usuários de telegrama nas Américas e alguns usuários de outros países podem ter problemas de conexão." (https://twitter.com/telegram, tradução nossa).

Supostos trechos das mensagens trocadas entre os senhores Sérgio Moro e Deltan Dallagnol foram publicados pelo *site* The Intercept Brasil em 9 de junho de 2019. O *site* criou diversos conteúdos relacionados para, além de divulgar o conteúdo teoricamente obtido pelos *hackers*, também comentar sobre as decisões da Lava Jato e os diálogos vazados[5]. Além de comprometer diretamente o ministro Moro e o procurador Dallagnol, desde o vazamento das mensagens, as ações já tomadas na operação são questionadas, assim como a idoneidade dos envolvidos.

No dia 14 de junho, em uma palestra em Porto Alegre para empresários em evento do Lide-RS (Grupo de Líderes Empresariais), o atual vice-presidente da República general Hamilton Mourão afirmou: "a guerra cibernética atingiu em cheio o nosso governo" (Bemfica: 2019). A declaração foi feita após o vice-presidente comentar que a Rússia interfere nas comunicações e na Internet, apoiando o regime de Bashar al-Assad na Síria e o governo de Nicolás Maduro na Venezuela. A frase sobre o ataque cibernético contra o governo fez menção ao vazamento das informações das mensagens trocadas entre o ministro Sérgio Moro e o procurador Deltan Dallagnol.

No dia 20 de junho de 2019 aconteceu outro episódio que pode ser enquadrado como guerra cibernética, conforme definição apresentada no segundo capítulo. No dia 17 de junho de 2019, o Irã derrubou um drone de vigilância dos Estados Unidos. O Irã alegou que seu espaço aéreo foi invadido. Os Estados Unidos alegaram que o drone sobrevoava águas internacionais. Em resposta à destruição do equipamento, os Estados Unidos provocaram um ataque cibernético que desabilitou os sistemas iranianos de computadores que fazem o controle de lançadores de mísseis e foguetes. Inicialmente, o presidente norte-americano, Donald Trump publicou no Twitter que o Irã seria bombardeado em três pontos diferentes. Em seguida, Trump disse que desistiu desse tipo de retaliação, pois pelo menos 150 pessoas iriam morrer e essa seria uma resposta desproporcional à destruição do drone (BBC: 2019; G1: 2019).

[5] Um dos três fundadores do site é Glenn Greenwald, que junto com Edward Snowden, publicou informações sobre a vigilância global pela NSA, dos EUA. THE INTERCEPT BRASIL. Disponível em < https://tinyurl.com/y5zzg2vf>. Acesso em 12 jun. 2019.

Diante de tais fatos, entende-se a necessidade de estudar conceitos relativos à guerra cibernética, pesquisar sobre ataques já realizados e buscar reflexões para proteção cibernética do Brasil.

1.4. HIPÓTESE E VARIÁVEIS

Conforme Marconi e Lakatos, "toda hipótese é o enunciado geral de relações entre, pelo menos duas variáveis" (MARCONI; LAKATOS: 2012, p. 108). A pesquisa proposta tem caráter exploratório, focada em buscar familiaridade com o objeto do tema. Tendo em vista que ele é recente e não conta com bibliografia brasileira extensa que permita comparação, a pesquisa não está baseada numa hipótese nem na relação entre variáveis.

1.5. METODOLOGIA

1.5.1. MÉTODO DE ABORDAGEM

Foi usado o Método Dedutivo, que parte de uma cadeia de raciocínio descendente, da análise geral para a particular, até a conclusão. O método dedutivo parte "de teorias e leis, na maioria das vezes prediz a ocorrência dos fenômenos particulares (conexão descendente)" (MARCONI; LAKATOS: 2012, p. 110).

1.5.2. FASES DA PESQUISA

- Documentação indireta. Pesquisa bibliográfica feita a partir de material já publicado (livros, artigos, periódicos, *sites* da Internet).

- Os documentos para descrição de ataques cibernéticos internacionais selecionados são os que tratam dos seguintes episódios: União Soviética (1982), Estônia (2007), Síria (2007), Geórgia (2008) e Irã (2009/10), empresas e entidades americanas (2015). Esses casos foram selecionados pelo impacto causado, repercussão internacional e documentação acessível.

- A partir da revisão de bibliografia, foram levantadas perguntas de pesquisa pertinentes ao tema, que são a base das questões feitas aos especialistas.

- Questionário aberto, produzido com perguntas que foram respondidas por escrito pelos entrevistados especialistas, sem a presença do entrevistador (MARCONI; LAKATOS: 2012, p. 111).

- Para que o conteúdo das respostas dos questionários seja abalizado e contribua com o estudo, a seleção dos entrevistados foi baseada em profissionais que tenham afinidade com o tema, como profissionais que tenham atuado em setores de defesa cibernética e em órgãos governamentais que atuam e estudam sobre conteúdos relacionados à defesa cibernética. A escolha e posterior convite aos respondentes do questionário foi feita visando a contribuição de suas respostas às perguntas propostas.

- A seleção foi feita com aval e ajuda do orientador, que, através de contatos prévios em congressos e afins, estabeleceu relação com os respondentes. Os potenciais respondentes foram convidados pelo orientador e também foram instados a indicar outros potenciais respondentes. A partir dessas respostas, foram selecionados e convidados um total de 27 especialistas, sendo 25 militares. O convite para participação com as respostas para o questionário se deu através de contatos via telefone e e-mail. Desses 27 especialistas aos quais foram enviados os questionários, 14 responderam dentro do tempo necessário para o andamento da pesquisa.

- A abordagem dos possíveis respondentes do questionário foi feita por meio de e-mails, a fim de maximizar o tempo dos entrevistados e uniformizar as perguntas, evitando desvios que poderiam acontecer em entrevistas presenciais.

- A análise dos dados foi feita com a leitura de todas as respostas para o questionário, buscando pontos de similaridade e de dissonância entre o que foi informado por cada entrevistado. Como o questionário foi constituído de perguntas abertas, não foi possível fazer uma análise estatística sobre as respostas. As respostas não estão integralmente transcritas, conforme previamente combinado com respondentes, a fim de evitar possível supressão de informações, tidas como sensíveis pelos respondentes.

CAPÍTULO 2: PANORAMA SOBRE A GESTÃO DA SEGURANÇA E DA DEFESA CIBERNÉTICA

O segundo capítulo apresenta a definição de termos que serão usados ao longo do trabalho e necessitam de conceituação para nortear o estudo: Guerra; Guerra Cibernética; Guerra Cinética; Guerra Centrada em Redes; Tecnologia; Internet/Ciberespaço; Defesa/Defesa Cibernética; Segurança/Segurança Cibernética; Ataque Cibernético; Crime

Cibernético/Cibercrime. O presente capítulo trata sobre o desenvolvimento da Internet, desde a ARPANET, até a Internet das Coisas. Após o histórico da Internet, serão observados o novo paradigma que abarca novos desafios no Ciberespaço. No capítulo também são apresentadas as Políticas Brasileiras para a Defesa Nacional, como o Livro Verde: Segurança Cibernética no Brasil, a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END), o Livro Branco de Defesa Nacional (LBDN). As Leis Nº 12.737/2012 "Lei Carolina Dieckmann" e Lei Nº 12.965/2014 "Marco Civil da Internet" também são estudadas, juntamente com a relação entre a Marinha do Brasil e a cibernética.

2.1. DEFINIÇÃO DOS TERMOS

Ao longo do tempo, palavras e expressões sofrem alteração de conceito. O advento da Internet e dos mecanismos de armazenamento alteraram algumas expressões e criaram outras. "Baixar" era um verbo que indicava descer algo, passar da parte superior para a inferior. Atualmente, essa palavra tem um correspondente polissêmico vinculado à Internet. A transferência de arquivos feita de forma virtual também é chamada de "download". Ou, em português: "baixar", que é usada como sinônimo de descarregar um arquivo, transferir dados da Internet para a própria máquina ou para e-mails e outras formas de armazenamento. Outro termo que ganhou nova acepção é "nuvem". Nuvens eram associadas às formas brancas naturais, que aparecem no céu. Tecnicamente, são: "manifestações visíveis da condensação e deposição de vapor d'água na atmosfera. Podem ser definidas como conjuntos visíveis de minúsculas gotículas de água ou cristais de gelo, ou uma mistura de ambos" (DEPARTAMENTO DE FÍSICA, 2017). No tempo hodierno, a palavra "nuvem" está associada a serviços de armazenamento na Internet, como o Dropbox, Google Drive e OneDrive. "Nestas páginas, é possível enviar arquivos do seu computador ou fazer backup para que estes fiquem acessíveis em qualquer lugar do mundo através de uma conexão da Internet." (TECH TUDO, 2014).

O Google é o maior buscador de termos na Internet "de tão icônico, é usado como substantivo e verbo" (VAIDHYANATHAN: 2011, p. 16). Se a palavra "nuvem" for pesquisada no *site*, todos os resultados da primeira página são ligados a serviços de armazenamento (GOOGLE, 2017). A própria criação do Google, que só existe graças à Internet e aos resultados fornecidos por ele, mostram as mudanças que a tecnologia provocou. Inclusive em palavras e expressões.

E qual seria a função de definir um conceito? O historiador Reinhart Koselleck trata sobre o poder peculiar das palavras, que abarcam conceitos em si. Há uma relação entre a linguagem e o mundo. Essa relação atinge as premissas teóricas, que devem ser focadas sob a ótica da prática de pesquisa. Para analisar historicamente os conceitos, é necessário usar como auxílio a história da língua e a história social, uma vez que a semântica não fica restrita à dimensão linguística.

A história dos conceitos tem exigências metodológicas que definem um campo particular de estudos. O rigor metodológico da história dos conceitos advém da possibilidade de juntar tempo e espaço, sob a perspectiva concomitante de análise. Assim, é possível fazer a "tradução" de significados léxicos usados no passado para o entendimento atual. Com esse processo, há a fixação dos conceitos e da história dos termos através da perspectiva contemporânea. O processo da história dos conceitos é metodológico, enquanto a análise sincrônica do passado é diacrônica (KOSELLECK: 2016).

A seguir, serão apresentados os seguintes conceitos: Guerra; Guerra Cibernética e Guerra Cinética, Guerra Centrada em Redes; Tecnologia; Internet/ Ciberespaço; Defesa e Defesa Cibernética; Segurança e Segurança Cibernética; Ataque Cibernético e Crime Cibernético.

2.1.1. GUERRA

O conceito de guerra balizador do trabalho é o proposto pelo estrategista militar e teórico Carl von Clausewitz (1780-1831). Clausewitz é considerado um dos principais teóricos do período de formação do pensamento militar moderno. Ele refletiu sobre a guerra como um instrumento da política de Estado. Guerra é "um ato de força para compelir o inimigo a fazer a nossa vontade" (CLAUSEWITZ: 1989, p. 75). A Doutrina militar de Defesa MD51-M-04 define guerra como "(...) conflito no seu grau máximo de violência. Em função da magnitude do conflito, pode implicar a mobilização de todo o Poder Nacional, com predominância da expressão militar, para impor a vontade de um ator ao outro" (BRASIL: 2007, p. 15).

2.1.2. GUERRA CIBERNÉTICA

O conceito de Guerra Cibernética deriva do uso de novas tecnologias. Segundo Richard Clarke e Robert Knake guerras Cibernéticas são "(...) ações de um estado-nação para invadir

computadores ou redes de outra nação com a intenção de causar danos ou transtornos" (CLARKE; KNAKE: 2015, posição 335). A Guerra Cibernética não é um sucedâneo para os combates bélicos tradicionais. Conforme conceituação de Clarke e Knake, ao invés de ser uma "alternativa para a guerra convencional, a guerra cibernética, na verdade, pode até mesmo aumentar a chance de que um combate mais tradicional aconteça, com explosivos, balas e mísseis" (CLARKE; KNAKE: 2015, posição 229).

A Doutrina Militar de Defesa Cibernética MD31-M-07informa que a guerra cibernética "corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C^2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar"[6] (BRASIL: 2014, p. 19).

No livro *Cyber Warfare: a "Nuclear Option"?* Krepinevich, que já integrou o Exército dos Estados Unidos e trabalha com consultoria na área de defesa, define a guerra cibernética da seguinte maneira:

> ações por Estados-nação e atores não estatais que empregam ciber armas para penetrar computadores ou redes com o propósito de inserir, corromper e / ou falsificar dados; interromper ou danificar um computador ou dispositivo de rede; ou infligindo danos e / ou perturbações para sistemas de controle de computador. A guerra cibernética pode envolver a prática de espionagem, atividades criminais e guerra econômica. Também pode incluir ações destinadas a apoiar operações militares nos níveis tático e operacional de guerra, bem como operações independentes destinadas a atingir estratégias efeitos estratégicos (KREPINEVICH: 2012, p. 8, tradução nossa).

Para Friedman e Singer, o termo "cyberwar" (guerra cibernética) tem sido usado tanto para conceituar uma situação envolvendo duas nações, como o caso entre a Rússia e a Estônia (LIBICKI: 2009; CLARKE; KNAKE: 2015), como também para tratar de fraudes com cartões de crédito, até estado o real de guerra, envolvendo os meios cibernéticos (FRIEDMAN; SINGER, 2010, p. 120). Contudo, para os autores, os elementos-chave da guerra no ciberespaço têm seus paralelos e conexões com a guerra em outros domínios: "seja guerra na terra, no mar ou no ar, ou agora no ciberespaço, a guerra sempre tem um objetivo e modo político (que a distingue do crime) e sempre tem um elemento de violência" (FRIEDMAN; SINGER, 2010, p. 121, tradução nossa).

A Doutrina Básica da Marinha EMA-305 também conceitua a guerra cibernética:

> Ações de Guerra Cibernética (GC), que envolvem ferramentas disponíveis nos campos da Tecnologia da Informação e Comunicações (TIC), também

[6] C^2: Comando e Controle.

> Conhecidas como “ciberguerra”, relacionam-se à modalidade de guerra onde o conflito não ocorre em terra, no mar ou no ar ou no espaço, mas sim no espaço cibernético (ECiber). São ações de defesa, exploração e ataque a informações e sistemas de informação, empreendidas de forma ofensiva e defensiva para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de Computadores (BRASIL: 2014, p. 3-24).

No artigo *Principles of Cyber-warfare*, Parks e Duggan definem Guerra cibernética como: “(…) uma combinação de ataque e defesa de redes de computadores e operações técnicas especiais” (PARKS; DUGGAN, 2011, p. 30, tradução nossa). Os autores também definem oito princípios específicos da Guerra cibernética:

1. A distância não é um limitador: as limitações físicas de distância e espaço não se aplicam ao mundo cibernético. Tais fatores não são um obstáculo para a realização de ataques. O atacante pode estar próximo do atacado ou não.
2. Efeito cinético: apesar de ser executada no ambiente cibernético, a guerra cibernética deve ter efeitos cinéticos. Ataques cibernéticos podem afetar objetos no mundo físico. Abertura de comporta de barragem ou desligamento de uma subestação elétrica, por exemplo. Também pode, de forma sutil, afetar a maneira como os tomadores de decisão pensam, provendo o decisor de informações que levam a decisões erradas. Conforme De Sá, Machado e Almeida: “podemos dizer que a energia dispendida por guerreiros cibernéticos em combate só resulta em trabalho quando os resultados afetam – direta ou indiretamente – o mundo físico” (DE SÁ; MACHADO; ALMEIDA: 2019, p. 90).
3. Furtividade: é possível tomar medidas para esconder “o rastro” no mundo cibernético. Porém, tudo o que é feito é visível, caso alguém esteja olhando. As ações executadas requerem a manipulação de dados. O protagonista da guerra cibernética deve tentar esconder as evidências dentro dos fluxos de dados existentes, similar à camuflagem na guerra cinética. Quem procura se proteger deve fazer a distinção entre o uso esperado do sistema e a presença do invasor.
4. Mutabilidade e inconsistência: no mundo físico, caso as condições sejam as mesmas, as ações e reações de determinada ação podem ser previstas. No mundo cibernético a imprevisibilidade e mutabilidade são constantes. Ataques nem sempre funcionam da mesma maneira devido à essa característica mutável do ambiente cibernético. Fatores que não mudam no mundo cibernético são os que dependem de mudanças no mundo físico (exemplo: aumento da capacidade de um processador).

5. Identidade e privilégios: o objetivo de um invasor de sistema é assumir a identidade de alguém com autoridade no mundo cibernético. A maioria das etapas de qualquer ataque na guerra cibernética é destinada a assumir a identidade de quem pode executar a ação desejada.
6. Duplo uso das "ferramentas": ao contrário das ferramentas cinéticas usadas na guerra, com uso único (arma ataca, escudo defende, por exemplo), as ferramentas cibernéticas têm uso duplo. Elas são usadas tanto por quem ataca como por quem defende.
7. Controle de infraestrutura: defensor e atacante controlam uma parte muito pequena do ciberespaço usado por ambos. E, quem consegue controlar uma parte do ciberespaço do oponente, controla o oponente. Uma maneira de se precaver, é fazer testes para ataque à própria rede. Tanto atacante quando defensor são vulneráveis aos ataques.
8. Informação como ambiente operacional: na guerra cibernética, as conexões de comunicação, rede de computadores, listas de pessoal, *sites*, links, e-mails, postagens, e os outros aspectos do alvo já são informações no ciberespaço. Não é necessário converter a informação para uso no ambiente, pois a informação faz parte do ambiente (PARKS; DUGGAN, 2011, p. 32 - 34).

Conforme as definições apresentadas, pode-se dizer que a guerra cibernética envolve o uso do ambiente cibernético para provocar danos virtuais e/ou físicos em um adversário. A guerra cibernética não é um paliativo ou substituto para a guerra "convencional". Ela pode ser uma aliada aos combates bélicos, envolvendo Estados que desejam minar a capacidade ofensiva do adversário, danificar estruturas, obter segredos através da espionagem e provocar efeitos cinéticos usando a capacidade cibernética.

2.1.3. GUERRA CINÉTICA

Richard Clarke e Robert Knake informam que o Exército dos Estados Unidos usa o termo "ataque cinético" para nomear os ataques "convencionais" (CLARKE; KNAKE: 2015, posição 414), ou seja: os que não acontecem no espaço cibernético. Parks e Duggan definem guerra cinética como "(…) praticada nos domínios terrestre, marítimo, aéreo e espacial. Todos os tanques, navios, aviões e soldados das forças armadas atuais são os protagonistas da guerra cinética" (PARKS; DUGGAN, 2011, p. 30, tradução nossa). Ou seja: a guerra cinética envolve artefatos tangíveis e seres humanos. Os autores consideram os seguintes princípios cinéticos da guerra, em comparação à guerra cibernética: direcionar todas as operações militares para uma direção claramente definida, decisiva, e objetivo atingível. De Sá, Machado e Almeida fazem uma observação importante sobre a conceituação de Parks e Duggan:

> Note que, a definição de guerra cinética apresentada por (Parks; Duggan, (2011) não permite uma caracterização clara do domínio deste tipo de guerra, visto que ações de guerra cibernética e eletrônica também podem ser praticadas em terra, mar, ar e espaço. Por esse motivo, para caracterizar o domínio da guerra cinética, recorremos ao significado de cinética. Considerando que a cinética é a parte da física que estuda as mudanças de movimento produzidas pela força, podemos estabelecer que o domínio da guerra cinética reside no mundo real – isto é não virtual – sujeito a mudanças mediante a aplicação de forças. (DE SÁ; MACHADO; ALMEIDA: 2019, p. 102)

O princípio cinético da ofensiva é apreender, reter e explorar a iniciativa. Na guerra cinética, a inércia das forças opostas significa que tomar a iniciativa é difícil. Comparativamente, para Parks e Duggan, na guerra cibernética a inércia é quase inexistente, pois "mover bits é muito mais fácil do que mover tanques, navios e aeronaves" (PARKS; DUGGAN, 2011, p. 31, tradução nossa). O princípio cinético também envolve concentrar os efeitos de poder de combate em determinado local e tempo, a fim de se alcançar resultados decisivos. Tal concentração não é essencial na guerra cibernética (exceto em ataques de negação de serviço).

2.1.4. GUERRA CENTRADA EM REDES

No documento *The Implementation of Network-Centric Warfare*, Alberts diz que a Network Centric Warfare (Guerra Centrada em Rede) é uma teoria que surge na Era da Informação. O conceito de Guerra Centrada em Rede descreve de maneira ampla a combinação de estratégias, táticas emergentes, técnicas, procedimentos e organizações que de forma total ou parcial podem ser usadas para se obter uma vantagem decisiva no combate (ALBERTS: 2003, p. 3).

O Glossário das Forças Armadas Brasileiras MD35-G-01 define a Guerra Centrada em Redes da seguinte maneira:

> 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. (BRASIL: 2015, p. 134)

2.1.5. TECNOLOGIA

Conforme Longo e Moreira: “ao longo da história, as demandas de segurança e defesa, individual ou coletiva, foram molas impulsoras de avanços tecnológicos de produtos, processos e serviços.” (LONGO; MOREIRA: 2013, p. 278). As demandas fazem com que o homem produza novas tecnologias e se aproprie dela, através do uso. Para Longo, tecnologia é “o conjunto organizado de todos os conhecimentos científicos, empíricos ou intuitivos empregados na produção e comercialização de bens e serviços” (LONGO: 2000, p. 1). Longo ainda informa que “alguns autores consideram a tecnologia como sendo apenas ciência aplicada. Na realidade esta definição pode não ser sempre verdadeira, embora no mundo atual, a tecnologia dependa cada vez mais dos conhecimentos científicos”. (LONGO: 2000, p. 1).

“Uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível” (CASTELLS: 2007, p.67). Castells cita como tecnologias da informação: tecnologias em microeletrônica, computação (*software* e *hardware*), telecomunicações/ radiodifusão e optoeletrônica (CASTELLS: Idem). Para Friedman e Singer, “essa questão de saber se uma nova tecnologia favorece o ataque ou a defesa é crítica para a cibersegurança, pois pode moldar tudo, desde a probabilidade de guerra até a forma como os governos e até as empresas devem se organizar” (FRIEDMAN; SINGER, 2010, p. 154, tradução nossa).

Para Everett M. Rogers, que trata sobre tecnologia no livro *Difusion of Inovations*, a tecnologia é “um projeto de ação instrumental que reduz a incerteza nas relações de causa-efeito envolvidas na obtenção de um resultado desejado”. (ROGERS: 1983, p. 12, tradução nossa). O autor apresenta a ideia de que, em geral, a tecnologia é vista como composta de dois aspectos: hardware (parte física) e software (base de informações). O autor exemplifica os aspectos evocando a estrutura de um computador composto de partes físicas (*hardware*) e os comandos, códigos, que são a base para o funcionamento (*software*). Tal junção forma o computador, que permite a expansão dos recursos que as pessoas podem ter para ampliar a solução de problemas. O computador é a ferramenta, passível de ser usada para resolver questões. Com o exemplo, Rogers demonstra que normalmente a tecnologia é caracterizada como hardware, uma parte física, sendo máquina ou equipamento que auxilia as pessoas. Contudo, salienta que a tecnologia não é somente um aparelho, maquinário, somente hardware. Para Rogers, uma tecnologia não precisa necessariamente ser atrelada ao maquinário. Pelo contrário, a tecnologia pode ser “quase inteiramente composta de informações; exemplos são uma filosofia política conservadora, uma ideia religiosa como a Meditação Transcendental, um evento de notícias,

um boato, produção em linha de montagem e gerenciamento por objetivo". (ROGERS: 1983, p. 12, tradução nossa). Tal conceito demonstra que não somente os aparatos, máquinas, equipamentos e quaisquer outras nomenclaturas usadas para denominar *hardwares* criados podem ser considerados como "tecnologia".

No livro Os meios de comunicação como extensões do homem, Marshall MCluhan observa que "toda tecnologia gradualmente cria um ambiente humano totalmente novo" (MCLUHAN: 1964, p. 9). Ou seja, o uso da tecnologia traz consigo consequências para a vida social, para a maneira como as pessoas interagem umas com as outras e com as próprias tecnologias. A ferrovia é usada como exemplo para demonstrar a modificação provocada pela tecnologia na vida social: "a estrada de ferro não introduziu movimento, transporte, roda ou caminhos na sociedade humana, mas acelerou e ampliou a escala das funções humanas anteriores, criando tipos de cidades, de trabalho e de lazer totalmente novos". (MCLUHAN: 1964, p. 9). É possível perceber 2 divisões dos efeitos da tecnologia para a humanidade para McLuhan: ou elas são extensões humanas ou auto-amputações" (MCLUHAN: 1964, p. 9). Nesse sentido, ou as tecnologias funcionam como próteses, indo além da capacidade corporal humana ou substituindo uma função humana, ao "substituir" uma função corpórea humana pela tecnologia. Assim, a tecnologia, "enquanto ferramenta que expande a ação do homem no mundo, ao mesmo tempo que o auxilia a ser adaptar melhor ao meio e produzir seu próprio alimento, também contribuiu para o seu desenvolvimento cognitivo" (MENDONÇA, OLIVEIRA E COSTA: 2016).

Pierre Lévy questiona: "seria a tecnologia um ator autônomo, separado da sociedade e da cultura [...]?" (LÉVY: 1999, p. 22). Pelo contrário, Lévy instiga a "em vez de enfatizar o impacto das tecnologias, poderíamos igualmente pensar que as tecnologias são produtos de uma sociedade e de uma cultura" (LÉVY: 1999, p. 22). Um dos exemplos do entrelaçamento de tecnologia, sociedade e cultura pode ser verificado através do Ciberespaço, conforme o próximo tópico.

2.1.6. INTERNET/ CIBERESPAÇO

De acordo com Lemos, "o paradigma digital e a circulação de informação em rede parecem constituir a espinha dorsal da contemporaneidade" (LEMOS: 2007, p. 192). Castells conceitua a Internet como "um meio de comunicação que permite, pela primeira vez, a

comunicação de muitos com muitos, num momento escolhido, em escala global" (CASTELLS: 2003, p.240).

O termo "ciberespaço" foi criado pelo escritor de ficção científica William Gibson, em 1984. No livro *Neuromancer*, o autor fala sobre o universo das redes digitais. Assim, o termo ciberespaço foi adotado por criadores e usuários das redes (LÉVY: 2007, p. 92). De acordo com Lévy, "o ciberespaço dissolve a pragmática da comunicação que, desde a invenção da escrita, havia reunido o universo e a totalidade" (LÉVY: 2007, p. 92). O impacto social do ciberespaço evoca o efeito radical na comunicação que a escrita provocou.

Para Lévy, ciberespaço é sinônimo de rede. Sua formação se dá pela "interconexão mundial dos computadores". Para o autor, o conceito de ciberespaço abarca tanto a estrutura física necessária para a comunicação digital, quanto as informações trafegadas e os usuários conectados que navegam pela rede. (LÉVY: 2007, p. 17).

No livro *Contested Commons: The Future of American Power in a Multipolar World* (2010), os autores observam que o conceito de ciberespaço foi feito nos anos 80. A princípio, o ciberespaço era tido como apartado do mundo físico. Porém, o ciberespaço também compreende a parte física, pois é formado com a conexão entre sistemas físicos e redes, que ficam circunscritos por normas estabelecidas em protocolos de *software* e comunicações.

Tais regras e protocolos estão dentro de fronteiras soberanas dos estados-nação. Contudo, os dados que são transferidos pela rede podem ser transmitidos para além das barreiras físicas de territórios nacionais: a comunicação feita através do ciberespaço é quase instantânea. É possível transferir grandes quantidades de dados a grandes distâncias, sem parar em barreiras físicas ou fronteiras políticas (RATTRAY; EVANS; HEALEY, 2010).

No livro *Contested Commons: The Future of American Power in a Multipolar World*, Greg Rattray, Chris Evans e Jason Healey tratam sobre o conceito, origem e a "geografia" do ciberspaço no capítulo *American Security in the Cyber Commons.* Conforme os autores:

> O ciberespaço, um conceito cunhado na década de 1980, foi visto inicialmente como um espaço fundamentalmente separado do mundo físico. Alguns teóricos chegaram ao ponto de afirmar que o ciberespaço transcende as fronteiras geográficas e nacionais e, portanto, prejudica as noções tradicionais de soberania e segurança. No entanto, o ciberespaço é fundamentalmente um ambiente físico, criado pela conexão de sistemas e redes físicos e gerenciado por regras definidas em protocolos de software e comunicação - todos localizados nos limites soberanos dos estados-nação. O ciberespaço compreende sistemas e infra-estruturas físicas e lógicas que são governadas pelas leis da física e pela lógica do código de computador. (...) O ciberespaço é único, pois as interações são governadas por hardware e software fabricados pelo homem, de modo que a "geografia" do ciberespaço é mais mutável do que outros ambientes. Montanhas e oceanos são difíceis de mover, mas

> elementos do ciberespaço podem ser ligados e desligados com o apertar de um botão. (RATTRAY; EVANS; HEALEY, 2010, p. 140, tradução nossa).

A instantaneidade e a liberdade na transmissão de dados podem representar oportunidades de possíveis adversários aproveitarem-se das vulnerabilidades da rede. O ciberespaço apresenta singularidade em sua "geografia": como o ator humano consegue fazer mudanças no *software* e *hardware*, é possível ligar e desligar funções, alterar o funcionamento de alguma programação, excluir código etc. (RATTRAY; EVANS; HEALEY, 2010). Apesar disso, não há infinitude na maleabilidade do ciberespaço, que é regido por leis físicas do eletromagnetismo, propriedades lógicas do código e as capacidades das organizações e das pessoas.

Para Friedman e Singer, o ciberespaço é essencialmente o domínio de rede de computadores usados por pessoas para armazenamento, compartilhamento e comunicação online (FRIEDMAN; SINGER, 2010, p. 14). Também destacam que o ciberespaço é um ambiente de informação, que não se limita ao mundo virtual, pois envolve os computadores e sistemas de infraestrutura necessários para o tráfego de dados. Ou seja: para acessar o virtual, o usuário precisa de um dispositivo físico (notebook, computador, celular), que esteja conectado por modens, fibra ótica, cabos etc.

Friedman e Singer comentam sobre a geografia do ciberespaço, que é similar à divisão humana artificial do globo terrestre. A infraestrutura está sujeita aos conceitos de soberania, nacionalidade e propriedade. "O ciberespaço pode ser global, mas não é 'apátrida' ou 'bem comum global', ambos os termos frequentemente usados no governo e na mídia." (FRIEDMAN; SINGER, 2010, p. 14, tradução nossa). Outra característica importante salientada pelos autores é a constante evolução do ciberespaço. Há uma combinação híbrida que está em constante mutação: a tecnologia e os seres humanos que atuam no ciberespaço. Por causa das alterações constantes, "o ciberespaço de hoje é o mesmo, mas também totalmente diferente do ciberespaço de 1982." (FRIEDMAN; SINGER, 2010, p. 14, tradução nossa). Tanto a criação como o desenvolvimento da Internet contaram com a cooperação de base científica, inciativa tecnológica, inovação da sociedade e estratégia militar (CASTELLS: 2007).

Daniel Ventre destaca que o ciberespaço não está circunscrito somente à Internet. Os drones, satélites, sistemas industriais informatizados, os RFID, Radio-Frequency Identification (identificação por radiofrequência), computadores (conectados ou não) também fazem parte do ciberespaço (VENTRE: 2012, p. 34). Além da explicação clara e abrangente por escrito, Ventre também apresenta uma imagem elucidativa sobre como o ciberespaço perpassa os outros ambientes, através da transversalidade, conforme a figura a seguir:

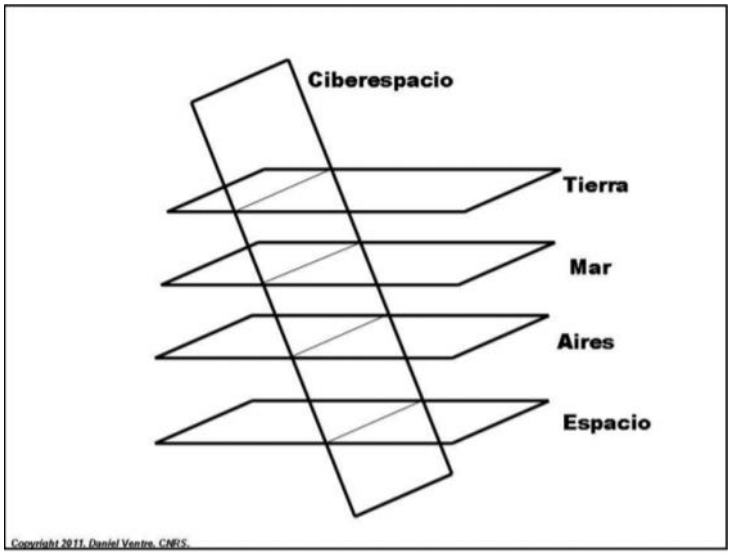

Figura 1: Ciberespaço. (VENTRE: 2012).

Nota-se na figura que o ciberespaço não se limita (nem é limitado) em nenhuma das dimensões: terra, mar, ar ou espaço. Ele atravessa todas as quatro dimensões, embora nenhuma das demais transpasse a sua própria camada, nem atinja as demais.

De acordo com Libick, o ciberespaço é um meio virtual constituído de três camadas. A primeira camada é a física, que contém os *hardwares* e componentes de infraestrutura, ligados ou não por fios. A segunda camada é a sintática, que envolve o *software*, contendo as instruções fornecidas pelos usuários e designers às máquinas, além dos protocolos pelos quais as máquinas fazem interação umas com as outras. A terceira camada é a semântica, que por ter codificação inteligível, é destinada à interação com os usuários (LIBICK: 2009, p. 12).

Pelo exposto através da conceituação de diversos autores, observa-se que o ciberespaço não está limitado à Internet. As pessoas atuam no ciberespaço como usuárias através de dispositivos diversos de *software* e de *hardware*. O ciberespaço perpassa o espaço virtual, muda a vida social e está em constante evolução. Para James Gleick, a peculiaridade do ciberespaço, que o distingue das tecnologias pregressas é a "sua mistura de escalas, da maior até a menor, sem prejuízo, transmitindo para milhões, comunicando-se especificamente com grupos, enviando mensagens instantâneas de um indivíduo para o outro" (GLEICK: 2013, p. 85).

2.1.7. DEFESA/ DEFESA CIBERNÉTICA

Conforme o Glossário das Forças Armadas MD35-G-01, a defesa é:

> 1. Ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança. 2. Neutralização ou dissuasão de ações hostis que visem a afetar a segurança de uma organização militar ou ponto sensível, pelo emprego racional de meios adequados, distribuídos conforme um planejamento, devidamente controlados e comandados. 3. Reação contra qualquer ataque ou agressão real ou iminente (BRASIL: 2015, p.84).

Segundo Portela, "defesa cibernética tem uma relação direta com a guerra, defesa dos interesses nacionais, garantia da sobrevivência e da soberania" (PORTELA: 2016, p. 108). A Defesa Cibernética é descrita pelo Glossário das Forças Armadas MD35-G-01, pelo Manual de Campanha EB70-MC-10.232, do Exército Brasileiro e pela Doutrina Militar de Defesa Cibernética MD31-M-07 como:

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (BRASIL: 2015, p.85); (BRASIL: 2017, p.2-2); (BRASIL: 2014, p. 18).

A Doutrina Militar de Defesa MD51-M-04 conceitua defesa como "ato ou o conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança." (BRASIL: 2007, p. 18). A Doutrina Militar de Defesa Cibernética MD31-M-07 informa que a Defesa Cibernética está:

> (...) se estabelecendo como atividade fundamental ao êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle (C^2), por meio da proteção dos ativos de informação, ao mesmo tempo permitindo que esse exercício seja negado ao oponente. Na condição de atividade especializada, sua execução se baseia em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares (BRASIL: 2014, p. 13).

A Doutrina Militar de Defesa Cibernética MD31-M-07 também apresenta as seguintes características relacionadas à Defesa Cibernética: insegurança latente, alcance global, vulnerabilidade das fronteiras geográficas, mutabilidade, incerteza, dualidade, paradoxo tecnológico, dilema do atacante, função assessoria, assimetria.

> **Insegurança Latente** - nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas.
> **Alcance Global** - a Defesa Cibernética possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao Espaço Cibernético.
> **Vulnerabilidade das Fronteiras Geográficas** - as ações de Defesa Cibernética não se limitam a fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar.
> **Mutabilidade** - não existem leis de comportamento imutáveis no Espaço Cibernético, pois podem adaptar-se as condições ambientais e da criatividade do ser humano.
> **Incerteza** - as ações no Espaço Cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.
> **Dualidade** - na Defesa Cibernética, as mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvos e, por administradores, para descobrir as fraquezas de equipamentos e redes.
> **Paradoxo Tecnológico** - quanto mais tecnologicamente desenvolvido estiver um sistema, mais dependente da TI estará e consequentemente mais vulnerável às ações cibernéticas. Contudo, paradoxalmente, este mesmo oponente possuirá mais condições de se defender dos ataques cibernéticos, em virtude de seu alto grau de desenvolvimento tecnológico.
> **Dilema do Atacante** - dúvida que o atacante enfrenta na busca ou não da correção de uma vulnerabilidade identificada, sabendo que a correção tornará mais eficiente a sua defesa, enquanto que a não correção aumenta sua capacidade de ataque.
> **Função Assessoria** - as ações de Defesa Cibernética não são um fim em si mesmas, sendo, geralmente, empregadas para apoiar a condução de outros tipos de operação.
> **Assimetria** - baseada no desbalanceamento de forças, causado pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais que podem vir a causar danos tão prejudiciais quanto aqueles perpetrados por Estados ou organizações com maiores condições econômicas, por exemplo (BRASIL: 2014, p. 20 e 21).

As características apresentadas mostram a singularidade de se operar no espaço cibernético. A vulnerabilidade é constante. Um possível ataque pode acontecer em quaisquer momentos, embora nem sempre alcancem os efeitos inicialmente planejados, justamente por causa dessa singularidade. O desenvolvimento do saber sobre condições tecnológicas é essencial para se defender de um possível ataque (ou para perpetra-lo).

A Defesa Cibernética está sob a responsabilidade do Ministério da Defesa, por meio das Forças Armadas. A Doutrina Militar de Defesa Cibernética MD31-M-07 determina que no

contexto do Ministério da Defesa, as ações no Espaço Cibernético são denominadas em quatro níveis: *político, estratégico, operacional e tático*, com as seguintes características:

> nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;
> nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e
> níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas (BRASIL: 2014, p. 17).

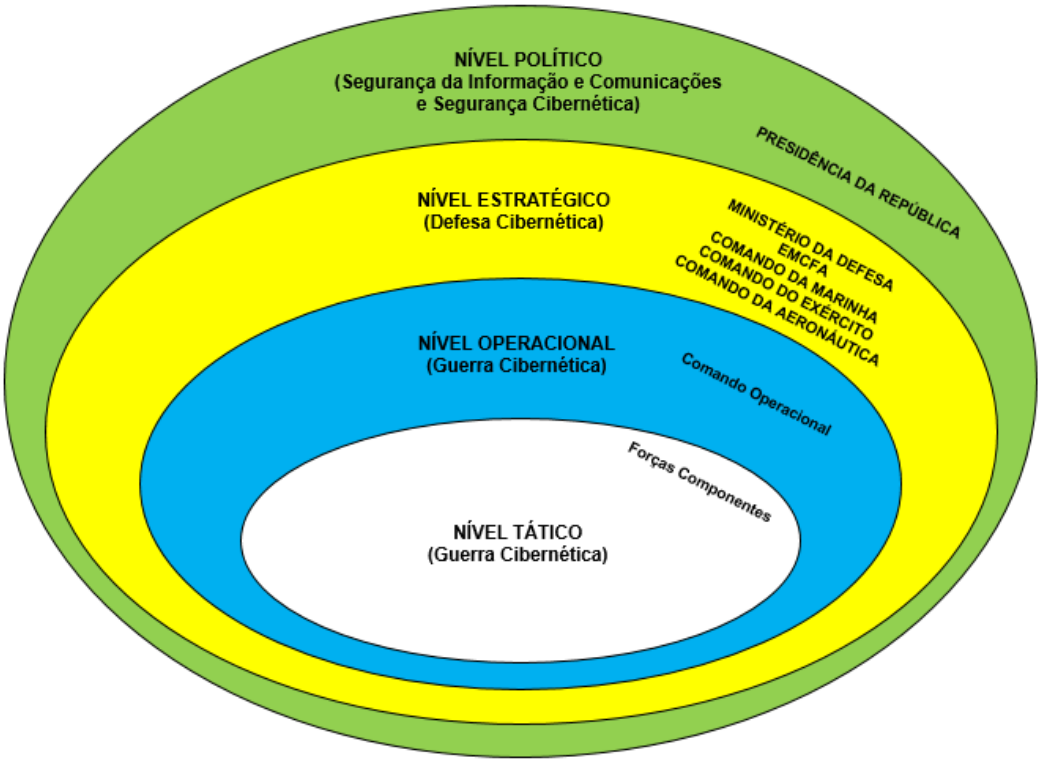

Figura 2: Níveis de decisão no contexto do Ministério da Defesa, referentes às ações no Espaço Cibernético (BRASIL: 2014, p. 17).

2.1.8. SEGURANÇA/ SEGURANÇA CIBERNÉTICA

O Glossário das Forças Armadas MD35-G-01 define a segurança como:

> SEGURANÇA - 1. É a sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza. 2. Condição que resulta do estabelecimento e conservação de medidas de proteção que assegurem a inviolabilidade contra atos ou influências hostis. (BRASIL, 2015, p.248).

A Política Nacional de Defesa conceitua a Segurança como “a condição que permite ao País preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais” (BRASIL: 2012, p. 15).

Já a Segurança Cibernética é definida tanto no Glossário das Forças Armadas MD35-G-01 (BRASIL, 2015, p.249) e também na Doutrina Militar de Defesa Cibernética MD31-M-07 (BRASIL: 2014, p. 19) como: “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”. A Doutrina Militar de Defesa Cibernética MD31-M-07 conceitua a segurança cibernética da mesma maneira (BRASIL: 2014, p. 19).

O Manual de Campanha EB70-MC-10.232, do Exército Brasileiro também utiliza a mesma descrição para a segurança cibernética (BRASIL: 2017, p.2-3). Para Portela, a segurança cibernética “está relacionada com todos os litígios que podem ameaçar o ambiente cibernético de um Estado.” (PORTELA: 2016, p. 108). O Livro Verde destaca que a segurança cibernética se caracteriza “cada vez mais como uma função estratégica de Estado, e essencial à manutenção e preservação das infraestruturas críticas de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, Informação, dentre outras” (MANDARINO; CANONGIA: 2010, p. 19). A Segurança Cibernética está sob a responsabilidade Presidência da República (BRASIL: 2014, p. 17).

2.1.9. ATAQUE CIBERNÉTICO

Conforme a conceituação da Doutrina Militar de Defesa Cibernética MD31-M-07 (BRASIL: 2014, p. 23) e o Glossário das Forças Armadas MD35-G-01 (BRASIL, 2015, p. 39), ataque cibernético “compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente”.

Para Fruhlinger, um ataque cibernético é caracterizado pelo uso de um ou mais computadores contra outro computador, computadores ou redes. Fruhlinger classifica os ataques cibernéticos em duas modalidades: 1. Ataques em que o objetivo é desativar o computador de destino. 2. Ataques que objetivam acesso aos dados do computador atacado para talvez, obter privilégios de administrador (FRUHLINGER: 2018).

A Joint Chiefs of Staff (JP) 3-12 referente às operações no ciberespaço, conceitua ataque cibernético como ações que criam efeitos de negação notáveis (degradação, ruptura ou destruição) no ciberespaço ou manipulação que leva a efeitos de negação nos domínios físicos (ESTADOS UNIDOS DA AMÉRICA: 2008, p. II-7).

Segundo Friedman e Singer, os ataques cibernéticos são distintos dos ataques tradicionais por usarem meios diferentes dos cinéticos. Ao invés de usar espada, bomba ou força corporal, os ataques cibernéticos atuam através dos meios digitais. Os autores também consideram que as barreiras geográficas e fronteiras políticas não são fatores limitantes para a execução de ataques cibernéticos. Podem atingir diversos alvos em diferentes partes concomitantemente. Friedman e Singer informam que alvo dos ataques cibernéticos são computadores e as informações contidas no aparelho. O ataque cibernético pode causar um dano físico, mas primeiro, precisa atingir um dispositivo digital. A autoria dos ataques cibernéticos é de difícil atribuição. A previsibilidade dos efeitos desse tipo de ataque não é simples. Segundo os autores, é geralmente mais fácil prever um ataque físico (o raio de uma bomba lançada, por exemplo). Já um vírus de computador pode infectar sistemas que não foram considerados anteriormente. (FRIEDMAN; SINGER, 2010, p. 69).

Já para Libick, que trata sobre ataque cibernético no contexto de guerra cibernética, a definição de ataque cibernético é: a interrupção ou corrupção deliberada de um sistema de interesse para um estado, provocado por outro estado (LIBICKI: 2009, p. 23).

Diante do exposto, pode-se resumir que um ataque cibernético é executado em um meio digital contra alvo(s) digital(is).

2.1.10. CRIME CIBERNÉTICO/CIBERCRIME

A Comissão Europeia considera cibercrime como atos criminosos cometidos on-line por meio de redes de comunicação eletrônica e sistemas de informação (EUROPEAN COMMISSION: 2019). Para a Comissão Europeia, o crime cibernético não tem fronteiras e é um problema que pode ser classificado em três definições amplas:

> 1. *Crimes específicos da Internet*, que incluem ataques a sistemas de informação ou phishing (por exemplo, *sites* falsos de bancos para solicitar senhas que permitam o acesso às contas bancárias das vítimas). 2. *Fraude e falsificação online*, feitos por meio de instrumentos como roubo de identidade, phishing, spam e códigos maliciosos. 3. *Conteúdo online ilegal*, que inclui material sobre abuso sexual infantil, incitamento ao

ódio racial, incitamento a atos terroristas e glorificação da violência, terrorismo, racismo e xenofobia (EUROPEAN COMMISSION: 2019).

Para Carrapiço, "o cibercrime é a denominação dada a um conjunto específico de crimes relacionados com a utilização de computadores e de redes informáticas" (CARRAPIÇO: 2005, p. 181). Bortot define que "os crimes cibernéticos são, assim como os crimes comuns, condutas típicas, antijurídicas e culpáveis, porém praticadas contra ou com a utilização dos sistemas da informática" (Bortot: 2017 p.341). Para Rust, "quando o hacker invade um ativo cibernético, independente de qual que seja sua intenção, ele está praticando um ato criminoso que pode causar danos muito severos" (RUST: 2019).

Conforme Zuccaro, a motivação para realizar um crime cibernético provém de indivíduos ou grupos pequenos, que têm fins privados. Para o autor, esses crimes visam na maior parte dos casos "ganhos econômicos, como, por exemplo, o roubo de senhas bancárias, fraudes com cartões de créditos e outros afins" (ZUCCARO: 2011, p. 61)

Os termos "cibercrime" e "crime cibernético" são usados como sinônimos para caracterizar crimes cometidos através do uso de aparelhos, sistemas e redes de informática. Em resumo, pode-se dizer que o crime cibernético são os delitos cometidos no ambiente cibernético.

2.2. DA ARPANET À INTERNET DAS COISAS

Segundo o historiador Geoffrey Blainey, a Primeira Guerra Mundial e Segunda Guerra Mundial influenciaram muitos eventos ocorridos na segunda metade do século XX, como a corrida espacial e o surgimento dos computadores (BLAINEY: 2011, p.5). A Segunda Guerra Mundial impulsionou a criação dos computadores, que tinham uso restrito aos cálculos científicos militares. Os computadores eram máquinas de calcular de grandes proporções, que ocupavam salas refrigeradas, sendo operados por cientistas.

O ENIAC (Electrical Numerical Integrator and Calculator) foi construído nos Estados Unidos a partir de 1943, durante a Segunda Guerra. Somente em 1946 ele foi finalizado para análises táticas e matemáticas. Suas proporções eram gigantescas: 5,50 metros de altura, 25 metros de comprimento, pesava 30 toneladas e ocupava 180 metros quadrados. Gleick descreve a máquina como "um monstrengo de trinta toneladas feito de válvulas termiônicas, relés e fios soldados à mão" (GLEICK: 2013, p. 248). Ele servia para o cálculo de tabelas para disparo da artilharia. Quando o ENIAC foi ligado pela primeira vez, consumiu tanta energia que as luzes de Filadélfia piscaram (HISTÓRIA DO COMPUTADOR, 2017). O Colossus, desenvolvido

pela Inglaterra em 1943, tinha o propósito de desvendar os códigos usados na guerra pelos alemães. Ele é considerado como precursor do computador digital eletromagnético.

Lévy ressalta que o uso de computadores por civis começou na década de 1960 e somente alguns visionários poderiam talvez, vislumbrar como o uso da tecnologia computacional atingiria a vida social. Até então, os computadores eram "grandes máquinas de calcular, frágeis, isoladas em salas refrigeradas, que cientistas em uniformes brancos alimentavam com cartões perfurados e que de tempos em tempos cuspiam listagens ilegíveis" (LÉVY: 2007, p. 31).

Em contraste com os computadores de grande porte usados durante a guerra, o microprocessador possibilitou uma nova fase da produção industrial: a miniaturização. Com a diminuição do peso e das dimensões dos computadores, houve impacto social. Lévy indica que alguns setores terciários, como bancos e seguradoras, se apropriaram dos ganhos produtivos proporcionados pelos aparelhos eletrônicos, tendência seguida até hoje (LÉVY: 2007, p. 31).

Além do microprocessador, os transistores e circuitos integrados substituíram as grandes válvulas usadas nos primeiros computadores. Para Laignier, a miniaturização, ocorrida entre os anos 50 e 70, transformou o computador em objeto de consumo, de uso pessoal, uma vez que a redução das medidas das máquinas possibilitou a saída do "ambiente laboratorial (militar, científico, acadêmico)" (LAGNIER: 2009, p, 123).

Com a invenção e o uso do computador pessoal e a difusão da Internet que contribuiu para a era da computação, houve um novo paradigma tecnológico no campo da cibernética e as tecnologias digitais passaram a compor o ciberespaço. Esse cenário foi iniciado durante a Guerra Fria, em 1958, um ano que remonta a origem da Internet e a construção de um processador de mensagens em um minicomputador pela Agência de Projetos de Pesquisa Avançada (ARPA). Também durante a Guerra Fria se deu o desenvolvimento da Arpanet, conforme explica Castells:

> A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processing Techniques Office (IPTO), fundado em 1962 com base numa unidade preexistente. O objetivo desse departamento (...) era estimular a pesquisa em computação interativa. Como parte desse esforço, a montagem da Arpanet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar on-line tempo de computação. Para montar uma rede interativa de computadores, o IPTO valeu-se de uma tecnologia revolucionária de transmissão de telecomunicações, a comutação por pacote, desenvolvida independentemente por Paul Baran na Rand Corporation (um centro de pesquisas californiano que frequentemente

> trabalhava para o Pentágono) e por Donald Davies no British National Physical Laboratory. O projeto de Baran de uma rede de comunicação descentralizada, flexível, foi uma proposta que a Rand Corporation fez ao Departamento de Defesa para a construção de um sistema militar de comunicações capaz de sobreviver a um ataque nuclear, embora esse nunca tenha sido o objetivo por trás do desenvolvimento da Arpanet (CASTELLS: 2003, p.13).

Dessa forma, foi criada a Arpanet, que interligava militares sem ter um centro definido ou uma rota única para transmitir informações (SANTAELLA: 2004, p.86). Isto tornava a rede praticamente indestrutível. A princípio, seu uso era limitado às universidades mais avançadas em tecnologia e institutos de pesquisa. Portanto, pelo tipo de informação compartilhada, era necessário que a Arpanet pudesse resistir à destruição ou retirada de qualquer computador que estivesse conectado na rede. Para Briggs e Burke, era necessário que a Arpanet resistisse inclusive "até à destruição nuclear de toda a 'infra-estrutura' de comunicações (...) Essa era a visão do Pentágono. A visão das universidades era que a Net oferecia 'acesso livre' aos usuários professores e pesquisadores" (BRIGGS e BURKE, 2006, p. 301).

Clarke e Knake salientam que quando o Departamento de Defesa inventou a Internet, sua utilização para a guerra não foi desprezada (CLARKE; KNAKE: 2015, posição 798). A rede possibilitava o compartilhamento de informações de maneira on-line. Depois de uma demonstração pública e profícua da Arpanet em uma conferência internacional, ela foi integrada a outras redes de computadores, o que introduziu o "novo conceito: uma rede de redes" Para que as redes conseguissem se comunicar, era necessário usar protocolos com padrões definidos. Por isso, em 1973, cientistas da computação se reuniram em um seminário para definir o projeto do protocolo de controle de transmissão (TCP) (CASTELLS: 2003, p.14).

Em 1975 já haviam 2 mil usuários de internet e centros de pesquisa conectados via Arpanet (BRIGGS e BURKE, 2006, p. 301). Nesse mesmo ano, ela foi transferida para o DCA: Defense Communication Agency, que estabeleceu o TCP/IP como protocolo na Defense Data Network, a fim possibilitar que a comunicação em rede via computador ficasse disponível para os diferentes ramos das forças armadas. (CASTELLS: 2003).

Em 1979 foi criado o primeiro provedor de serviços comerciais on-line: o CompuServe. Ele era usado pelo grupo Time/Warner. Em seguida, foi criada a American On-line (AOL), que, ao contrário do que o nome indica, estava ligada a grupos alemães e franceses. Em seguida, foi criado o provedor Prodigy (BRIGGS e BURKE, 2006). Contudo, o serviço oferecido por esses provedores não estava conectado em rede. Mas, o pioneirismo desses três empreendimentos serviu como base para o desenvolvimento dos servidores que foram criados posteriormente (CASTELLS: 2003).

Em 1983, o Departamento de Defesa criou a MILNET, com o objetivo de mitigar possíveis vulnerabilidades na segurança da rede. A MILNET era usada para fins especificamente militares, sem o tráfego de outras informações. A Arpanet ficou voltada para tráfego de dados relativos à pesquisa e passou a ser denominada como ARPA-INTERNET. No ano seguinte, 1984, a National Science Foundation (NSF) montou sua própria rede de comunicações entre computadores, a NSFNET (CASTELLS: 2003).

Em 1990 a Arpanet saiu de operação por motivo de obsolescência. Nesse mesmo ano, diversos provedores estabeleceram suas próprias redes para conexão à Internet, com fito comercial. Os provedores e demais redes que surgiram depois da Arpanet contribuíram para a difusão do uso da rede e aumento de usuários. A arquitetura da Arpanet possibilitou essa ampliação por ser descentralizada, construída em múltiplas camadas e com protocolos abertos de comunicação (CASTELLS: 2003. BIGGS e BURKE, 2006).

Com a retirada da Arpanet, o governo-norte americano passou a responsabilidade da administração da rede para a National Science Foundation. Em 1992 a Internet já tinha alcance global e a NSF planejou a privatização da rede, que sairia do controle direto do governo dos EUA. Em 1995, com o fim da NSFNET, houve a abertura para a privatização da Internet (CASTELLS: 2003. BIGGS e BURKE, 2006). O termo “Web”, usado como sinônimo para a Internet, vem de WWW, sigla que significa World Wide Web. Até 1991 não havia uma forma de navegação padrão na Internet. Por isso, o cientista da computação Tim Berners-Lee criou o primeiro website que ensinava como criar um navegador, instalar e configurar um servidor Web (CASTELLS: 2003).

Para ter acesso à Internet, o usuário precisa usar um navegador como o Firefox, Internet Explorer, Chrome, Opera etc. O primeiro navegador com Interface gráfica foi o Mosaic, criado em 1993 pelo estudante de computação Marc Andreessen. O Mosaic impulsionou o acesso à Internet através do seu ambiente graficamente amigável que permitia a ligação entre os usuários e o ambiente virtual da Internet. No final do ano de 1994, Andreensen criou um navegador chamado Netscape Navigator a partir do Mosaic. O diferencial do Netscape Navigator era que além da aparência amigável, rodava em diversos sistemas operacionais (PEREIRA: 2008)

Em 1995, após acompanhar o sucesso do Netscape Navigator, a Microsoft lançou junto com o Windows 95 o Internet Explorer, seu próprio navegador. Outros navegadores comerciais passaram a ser desenvolvidos, aumentando o acesso à Internet. Nas palavras de Castells:

> Em meados da década 1990, a Internet estava privatizada e dotada de uma arquitetura técnica aberta, que permitia a interconexão de todas as redes de computadores em qualquer lugar do mundo; a www podia então funcionar

> com software adequado, e vários navegadores de uso fácil estavam à disposição do público (CASTELS: 2003, p. 33).

A abertura da arquitetura da Internet para mais usuários possibilitou o seu desenvolvimento. Os usuários não eram mais apenas utilizadores: tornaram-se produtores de tecnologia. Ao invés de uma equipe de trabalho limitada, a Internet contou com diversas pessoas que implementaram melhorias e ajustes. Castells diz que "é uma lição comprovada da história da tecnologia que os usuários são os principais produtores da tecnologia, adaptando-a a seus usos e valores e acabando por transformá-la" (CASTELLS: 2003, p. 28).

Uma das transformações no uso da rede é a Internet das Coisas. Muitas vezes a Internet é usada como sinônimo de Rede mundial de computadores. Em um futuro breve, ambientes como casas, carros e escritórios estarão muito mais conectados, no que se pode chamar de rede mundial de objetos inteligentes ou simplesmente Internet das Coisas. Para os especialistas, a próxima revolução tornará comum que não apenas dispositivos como computadores e celulares sejam ligados em rede, mas também objetos comuns (EVANS: 2011). E não apenas estejam conectados, mas comuniquem-se entre si para realizar tarefas por conta própria. Essa comunicação entre coisas sem intervenção humana vem sendo classificada como M2M (Machine-to-Machine) (CLARK: 2016).

Num futuro próximo, é possível imaginar uma pessoa chegando em casa de carro e a garagem abrindo sozinha mediante a um comando dado pelo próprio veículo, baseado em geolocalização e biometria. Ao abrir a porta de entrada, um sensor identifica a presença da pessoa e envia um comando para o aparelho de ar-condicionado que climatiza a sala de estar na temperatura que mais agrada. Ao mesmo tempo, a central-multimídia começa a tocar o podcast que o motorista estava ouvindo enquanto dirigia. Tal abstração exemplifica um dos funcionamentos da Internet das Coisas. Dispositivos são ligados e aparelhos funcionam de determinada maneira sem que o usuário interaja diretamente com eles.

O conceito Internet das Coisas (IoT, na sigla em inglês) começou no fim da década de 1990, quando Kevin Ashton fez seu uso no título de sua apresentação feita para a Procter & Gamble (P&G), mais precisamente em 1999, como ele mesmo afirma em no artigo *That "Internet of Things" Thing* do RFID Journal. A ideia, que posteriormente possibilitou o IoT, era instalar microchips nos produtos para monitorar se eles estavam no estoque ou precisavam ser repostos. Assim, Ashton idealizou um sistema de sensores que poderiam conectar o mundo físico à Internet. De acordo com Ashton,

> Se tivéssemos computadores que soubessem de tudo o que há para se saber sobre as coisas usando dados que foram colhidos, sem qualquer interação

> humana, seríamos capazes de monitorar e mensurar tudo, reduzindo o desperdício, as perdas e o custo. Gostaríamos de saber quando as coisas precisarão de substituição, reparo ou atualização e se eles estão na vanguarda ou se tornaram obsoletos (ASHTON: 2009).

Desde seu surgimento, a tecnologia vem se desenvolvendo e cada vez toma mais espaço no dia a dia das pessoas. Há algumas décadas sequer era possível imaginar um carro que estivesse conectado em rede. Entretanto, a empresa Tesla realiza pesquisas para desenvolver carros autônomos que se comunicam em rede para planejar e executar seu deslocamento sem a necessidade de interação humana (G1: 2016). Elon Musk, CEO da Tesla, prometeu carros totalmente autônomos até o final de 2019 (GNIPPER: 2019).

Outra aplicação da IoT é uma geladeira inteligente, lançada pela Samsung em 2016. Além das funções usuais de uma geladeira, esse modelo dispõe de câmeras internas que monitoram os alimentos e permitem saber, mesmo à distância, os produtos que estão em falta através do smartphone. Com ela também é possível monitorar as datas de validade dos alimentos e visualizar informações da internet em uma tela embutida de 21,5 polegadas (HIGA: 2016).

Já estão disponíveis no mercado alguns objetos comuns, que foram adaptados para IoT. Alguns desses objetos são as "pulseiras inteligentes", as *smartbands*. Esses dispositivos tecnológicos vestíveis tornaram-se muito comuns, principalmente entre pessoas preocupadas com a saúde. A pulseira monitora passos, distância percorrida, horas de sono e batimentos cardíacos. Através de conexão bluetooth, os dados são enviados para um aplicativo de smartphone que consolida e organiza as informações coletadas (IG: 2018).

Já no campo da medicina, o conceito também vem sendo estudado e aplicado. A denominada Bio-IoT é a Internet das coisas aplicada a sistemas biológicos. Entregas de medicamentos, implantes médicos, próteses inteligentes, assistentes cirúrgicos e sistemas de monitoramento de pacientes à distância são algumas das aplicações da tecnologia. Há estudos de segurança nessa área, já que foram encontradas vulnerabilidades e riscos de ataques de *hackers*. A FDA fez um recall de quase 500 mil marca-passos sujeitos a ataques (SHAH: 2017). Charles Arthur salienta que "embora a internet das coisas seja frequentemente usada em ambientes domésticos, ela tem uma capacidade perigosa de se tornar brava." (ARTHUR: 2018, p.188), (tradução nossa).

Uma evolução do termo é IoE, que significa *Internet of Everything* ou Internet de Todas as Coisas, em Português, e ainda WoT ou *Web of Things* (Web das Coisas, em português). Tem-se convencionado usar IoT e IoE se referindo às máquinas, sensores, "coisas físicas"

(*hardwares*) que se comunicam e trocam informações entre si através da rede, enquanto WoT se refere a *softwares*, aplicativos e websites que trocam informações entre si. A característica primordial que define se algo é Internet das Coisas é a ausência de necessidade da interação humana (SAKOVICH: 2019).

O Brasil tem ganhado evidência cada vez maior quando o assunto é Internet das Coisas. Isso porque o país já figura como o quarto maior mercado consumidor de equipamentos conectados do mundo. O Brasil tem capacidade para ampliar ainda mais sua participação no cenário mundial. Segundo dados apresentados pela ANATEL, a Agência Nacional de Telecomunicações, o número de conexões entre máquinas no Brasil aumentou 20% entre os meses de outubro de 2016 e outubro de 2017. Estima-se que o Brasil já tem cerca de 20 milhões de conexões máquina-máquina. A previsão é que o número salte para 42 milhões em 2020. No cenário mundial, o total de objetos conectados deve ficar entre 100 milhões e 200 milhões, conforme a consultoria Teleco. (CANALTECH: 2017).

Com um crescimento cada vez maior, a nova tecnologia vira alvo de pessoas mal-intencionadas, que se aproveitam das brechas de segurança para cometer crimes. No final de julho de 2018 foi divulgada uma notícia relevante para quem trabalha com proteção cibernética. Segundo a SpiderLabs, um grupo de pesquisa da Trustwave, houve um ataque em escala global em que ocorreu a invasão de pelo menos 170 mil roteadores da marca MikroTik. A maioria das invasões ocorreu no Brasil. Os ataques têm como objetivo ter acesso à máquina a partir dos roteadores e assim usar o processamento do computador para minerar criptomoedas (KENIN: 2018). Esse processo é conhecido como cryptojacking (NORTON: 2019).

Um ataque semelhante ocorreu na Alemanha em 2016. Um *hacker* britânico de 30 anos chamado Daniel Kaye conseguiu deixar 900 mil roteadores de casas e empresas sem acesso à internet. Para isso ele usou um *botnet* de DDoS chamado Mirai. Esse *malware* é capaz de infectar dispositivos sem proteção e usá-los para procurar e invadir outros dispositivos, de maneira sucessiva (ARTHUR: 2018). Em janeiro de 2019, o mesmo Kaye foi condenado a 32 meses de prisão por promover um outro ataque, desta vez na Libéria. O alvo foi uma empresa de telefonia local, a Lonestar. Com isso, uma grande parte do país ficou sem acesso à internet e telefonia por 2 dias. Kaye mais uma vez usou o Mirai para invadir roteadores de internet e webcams desprotegidos. Ele recebeu US$ 10.000,00 pelo serviço, que teria sido encomendado por um funcionário da Cellcom, empresa concorrente da Lonestar na Libéria. (NCA: 2019).

Nas palavras de Roberto Martinez, analista sênior de segurança da empresa de segurança cibernética Kaspersky, “todas as tecnologias têm traços positivos e negativos. O número de

dispositivos conectados nos mostra a dependência que temos da tecnologia, no entanto, um dos maiores riscos na IoT continua sendo a segurança" (KASPERSKY: 2017) Isso porque de acordo com um relatório divulgado pela Kaspersky, nos primeiros 5 meses do ano de 2017, foram detectadas mais de 7.000 amostras de *malware* em dispositivos conectados à internet. Esse número é 74% maior que o total detectado entre 2013 e 2015 (KASPERSKY: 2017). Foi em 2016, com o surgimento do *malware* Mirai que o mundo percebeu os enormes riscos em torno dos dispositivos "inteligentes" conectados em rede (ARTHUR: 2018).

Atualmente a Internet é utilizada em escala global, conectando pessoas a outras pessoas através de dispositivos tecnológicos e conectando dispositivos com outros dispositivos Para Harari, "a ascensão da internet nos fornece uma degustação do que está por vir. O ciberespaço hoje é crucial em nossa vida cotidiana, em nossa economia e em nossa segurança" (HARARI: 2016, posição 6194). Essa mesma capacidade de conexão é capaz de basear inovações. Uma das áreas que será beneficiada é a indústria, que foi afetada pela chamada Indústria 4.0.

Preocupada com o futuro da indústria na Alemanha uma associação de representantes de negócios, políticos e pesquisadores, reunidos em Hannover cunhou o termo "Industrie 4.0", um conceito que descreve a revolução das cadeias globais de valor, apoiada em inovações tecnológicas. Trata-se da Indústria 4.0, que já é considerada a quarta revolução industrial. Para muitos deles, o novo conceito irá mudar completamente a maneira como se transforma matéria prima em bens de consumo (SCHWAB: 2016)

No livro *A Quarta Revolução Industrial*, Klaus Schwab afirma, sobre as "fábricas inteligentes" que "a quarta revolução industrial cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível. Isso permite a total personalização de produtos e a criação de novos modelos operacionais" (SCHWAB: 2016, p. 35)

A ideia nessa nova revolução é basear todo o processo de produção em tecnologias como Sistemas Ciber-físicos, Internet das Coisas e Big Data (DUTRA; VIANNA; FRAZZON: 2017). Isso tudo para fazer com que o processo se torne cada vez mais autônomo, eficiente e limpo. Esse conceito tem base na visão de Kagermann, Wahlster e Helbig, que no *relatório Recommendations for implementing the strategic initiative INDUSTRIE 4.0*, para a indústria alemã, previram o seguinte cenário: no futuro, as empresas estabelecerão redes globais para incorporar suas máquinas, sistemas de armazenamento e instalações de produção na forma de sistemas ciberfísicos. Segundo os autores, no ambiente de fabricação, tais sistemas ciberfísicos compreenderão máquinas inteligentes, sistemas de armazenamento e instalações de produção

capazes de trocar informações de forma autônoma, realizando ações e controlando umas às outras de forma independente (KAGERMANN et. al.: 2013, p. 5).

2.3. NOVOS DESAFIOS NO CIBERESPAÇO

O ciberespaço possibilita novas formas de interação e tráfego de informações. Isto constitui novos desafios para a defesa cibernética. A segurança no ciberespaço tange a compreensão de "(...) uma série de tarefas complexas: entender o que é guerra cibernética, aprender como e por que ela funciona, analisar seus riscos e se preparar, pensando em como controlá-la" (CLARKE; KNAKE: 2015, posição 229). Julian Assange, que é escritor, ciberativista e membro do conselho consultivo do WikiLeaks diz que "uma guerra furiosa pelo futuro da sociedade está em andamento. Para a maioria, essa guerra é invisível" (ASSANGE: 2013, p.10).

> WikiLeaks está diretamente ligado à Internet e ao vazamento de informações. Inclusive de governos e Estados. O objetivo é descrito no livro Cypherpunks – Liberdade e o Futuro da Internet: "Além de divulgar documentos, o WikiLeaks produziu dezenas de matérias, vídeos e artigos de opinião. (...) A tendência, é claro, já existia: na era da internet qualquer um pode ser produtor de notícia. Porém, o WikiLeaks avança mais um passo, trazendo essa lógica para o lugar do jornalismo em essência, ao valer-se dos segredos de Estado, documentos que comprovam violações de direitos humanos por empresas, o rastro documental dos crimes dos poderosos – que sempre foram a base para o jornalismo investigativo. Permite, assim, que dezenas de veículos independentes, jornalistas, ativistas – e usuários – se apropriem dessa documentação e se tornem também provedores de jornalismo de qualidade. Há aí uma noção hacker intrínseca na maneira de o WikiLeaks praticar jornalismo: se por um lado a organização se alia a veículos tradicionais de mídia – assim como a veículos não tradicionais –, por outro ela incentiva a disseminação de conteúdos livres, fora dessa indústria. E a indústria da notícia é hoje uma das principais trincheiras na disputa pelo vasto mundo da Internet" (ASSANGE: 2013, p.13).

É possível violar a privacidade de pessoas, organizações e países através da rede. Existem tecnologias que permitem a identificação, vigilância e investigação através da Internet. Um exemplo de tecnologia de identificação são os cookies: marcadores digitais instalados de maneira automática pelos websites. Eles permitem o armazenamento de informações no disco rígido do computador para posterior recuperação. Depois que o cookie está instalado na máquina, todas as ações online são registradas pelo *site* instalador, que monta um banco de dados com o número de acesso às páginas, número de visitantes, tempo de acesso e quem são os visitantes novos e os antigos. (CASTELS: 2003).

Já as tecnologias de vigilância trabalham com a identificação do usuário individualmente. Conforme Castells, tais tecnologias "interceptam mensagens, instalam marcadores que permitem o rastreamento de fluxos da comunicação a partir de uma localização específica de computador e monitoram a atividade de máquinas 24 horas por dia" (CASTELS: 2003, p. 14). As tecnologias de investigação são oriundas das tecnologias de vigilância e do armazenamento de informações digitais. Todas as informações transmitidas eletronicamente podem ser processadas, identificadas e combinadas para análises coletiva ou individual.

Para Assange, há a militarização do ciberespaço, no sentido de uma ocupação militar:

> Quando nos comunicamos por internet ou telefonia celular, que agora está imbuída na internet, nossas comunicações são interceptadas por organizações militares de inteligência. É como ter um tanque de guerra dentro do quarto. É como ter um soldado entre você e a sua mulher enquanto vocês estão trocando mensagens de texto. Todos nós vivemos sob uma lei marcial no que diz respeito às nossas comunicações, só não conseguimos enxergar os tanques – mas eles estão lá. Nesse sentido, a internet, que deveria ser um espaço civil, se transformou em um espaço militarizado. Mas ela é um espaço nosso, porque todos nós a utilizamos para nos comunicar uns com os outros, com nossa família, com o núcleo mais íntimo de nossa vida privada. Então, na prática, nossa vida privada entrou em uma zona militarizada. É como ter um soldado embaixo da cama. É uma militarização da vida civil (ASSANGE: 2013, p.45).

Tal militarização possibilita ataques remotos. Não há a necessidade de combates corpo a corpo, trincheiras ou armas bélicas para promover um ataque ou uma ciberguerra. Conforme Harari: "no futuro (...) um país como a Coreia do Norte, ou o Irã, poderia utilizar bombas lógicas para interromper a transmissão de energia na Califórnia, explodir refinarias no Texas e fazer trens colidirem em Michigan" (HARARI: 2016, posição 298). Apesar da possibilidade de ataques, Harari faz uma advertência salutar: "não se deve confundir capacidade com motivação. Embora introduza novos meios de destruição, a guerra cibernética não cria necessariamente incentivos para que sejam usados" (HARARI: 2016). Ou seja: a possibilidade de realizar ataques que causem malefícios não significa que eles serão necessariamente utilizados.

Assange ressalta a dualidade entre paz e guerra cibernéticas e o uso da tecnologia para se fazer guerra:

> (...) algumas pessoas que parecem ser autoridades em relação à guerra começam a falar sobre a tecnologia como se a entendessem. Essas pessoas muitas vezes falam sobre a ciberguerra e nenhuma delas, nem uma sequer, fala sobre a construção da ciberpaz ou qualquer coisa relacionada à construção da paz. Elas só falam sobre a guerra porque é com isso que elas ganham, e elas tentam controlar a tecnologia e os processos legais como um meio de promover os próprios interesses. Então, quando não temos controle algum sobre a nossa tecnologia, essas pessoas a usam para seus próprios fins – mais especificamente, para a guerra (ASSANGE: 2013 p.43)

Para se proteger de ameaças, é necessário conhecer pontos fracos na defesa. Seja ela cibernética ou não. Informações sensíveis e até privilegiadas são armazenadas em servidores virtuais e os danos perpetrados por ataques cibernéticos podem atingi-las. Os ataques podem até ser mais rápidos que invasões feitas *in loco*. Conforme Harari diz, as guerras cibernéticas "podem durar apenas alguns minutos" (HARARI: 2016, posição 5057). Os danos podem ser permanentes no caso de vazamento de segredos de Estado, por exemplo. Clarke e Knake advertem que:

> Como qualquer tecnologia que se desenvolve, barreiras como o alto custo são superadas a cada ano. A realização de um ataque cibernético devastador não exigiria um grande esforço industrial como a construção de uma bomba nuclear. Contudo, o entendimento de um software para controle de uma rede elétrica não é uma capacidade disponível tão facilmente. Uma coisa é descobrir como invadir uma rede e outra bem diferente é saber o que fazer quando você está dentro dela (CLARKE, KNAKE: 20175, posição 2513).

A guerra cibernética é distinta da guerra convencional. De acordo com Cornish (2011), o cerne do problema é que, embora possa haver muita política associada a eventos reais ou potenciais de guerra cibernética em todo o mundo, não significa que a guerra cibernética é um fenômeno politicamente estrito no sentido Clausewitziano. Cornish diz que o ciberespaço é como "terra nullius" (CORNISH et al.:2011, p. 38). Está atualmente fora do alcance do discurso político maduro. A ausência de um quadro político restritivo em torno da guerra cibernética é o que torna o ciberespaço tão atraente (CORNISH et al.: 2011). Atraente, perigoso e carente de estudos sobre o novo cenário. Bauman diz que:

> A maquinaria do Estado-nação, inventada e cultivada para garantir a soberania territorial e separar claramente os de dentro dos de fora, foi apanhada despreparada pelo "cabeamento" do planeta. Dia após dia, uma atrocidade terrorista após outra, as instituições de lei e ordem dirigidas pelo Estado aprendem sobre sua própria inépcia em lidar com os novos perigos que gritantemente atacam as categorias e distinções ortodoxas consagradas, aparentemente testadas e confiáveis (BAUMAN: 2008, p.163).

A principal característica dos ataques cibernéticos é o anonimato, garantido pelo simples uso de *proxys* que mascaram a identidade dos autores de ataques. Se o agressor não é identificado, não há como apontar um culpado, por mais que existam suspeitas. Na impossibilidade de se identificar um responsável, é difícil retaliar ciberataques.

Numa época em que a Internet industrial mostra cada vez mais seu poder, os temores, principalmente das grandes potências mundiais se tornam cada vez mais reais. Um ataque a

central elétrica de uma grande cidade poderia provocar danos catastróficos, semáforos sem funcionar, trens e metrôs parados, hospitais impossibilitados de fazer cirurgias de emergência etc. O sequestro de dados estratégicos de empresas poderia provocar um colapso nas bolsas de valores ao redor do mundo e muito dinheiro virtual poderia simplesmente desaparecer ou mudar de mãos. Um ataque a uma central de comunicações poderia deixar milhões de pessoas sem acesso a telefonia móvel ou fixa e poderia paralisar totalmente um sistema de logística de alcance mundial. (CLARKE; KNAKE: 2015; DE SÁ; MACHADO; ALMEIDA: 2019; HARARI: 2016; ZETTER: 2017). Conforme De Sá, Machado e Almeida:

> De fato, dependendo das circunstâncias, um incidente – cibernético ou não – em um sistema naval (civil ou militar) pode trazer impactos aos setores de transporte, energia, defesa, alimentos etc. com prováveis prejuízos econômicos, ambientais e à segurança (DE SÁ; MACHADO; ALMEIDA: 2019, p. 91)

A Internet possibilitou a criação de novo tipo de guerra silenciosa, porém muito mais poderosa e imprevisível que o conflito que a originou: A Segunda Guerra Mundial. Muito ainda terá que ser investido e estudado pelas nações a fim de encontrar as melhores soluções para se defender de ataques, mas essa nova modalidade eletrônica de conflito não dá mostras de perder sua força e letalidade em um futuro avistável.

Gerenciar ameaças e reduzir a vulnerabilidade no ciberespaço é um desafio complexo por causa do número, do alcance e dos diferentes tipos de usuários. É possível que um ataque cause danos em infraestrutura crítica e em larga escala. É preciso que os Estados criem estratégias para combater as ameaças (KREPINEVICH: 2012). A segurança do ciberespaço demanda ações em vários níveis e por um grupo diversificado de atores porque centenas de milhões de dispositivos estão interligados por uma rede de redes.[7]

Nos últimos anos a utilização cada vez maior de serviços na nuvem e o número crescente de novos dispositivos conectados à rede desafia os métodos habituais de proteção digital (ISTR, 2017, p.23). Essa nova realidade faz com que a possibilidade de sofrer ataques cibernéticos seja um desafio permanente para a política de defesa dos países. Estar preparado para se defender em caso de ataques cibernéticos tem sido tratado como ponto estratégico pelos governos atuais (MANDARINO; CANONGIA, 2010, p. 28). Ataques de diversas naturezas têm sido cada vez

[7] No final de 2012, conexões móveis de banda larga (tecnologias 3G e 4G) contabilizaram um quarto das conexões totais (excluindo M2M). Esse valor aumentou para 55% até o final de 2016, com 4 bilhões de conexões de banda larga móvel. Fonte: GSMA. The Mobile Economy 2017. Disponível em <https://tinyurl.com/y8txral8>. Acesso em 10 dez. 2017.

mais comuns e se intensificam com o passar dos anos no chamado ciberespaço (PWC, 2016. p. 4). Os ataques acontecem contra entidades privadas, estatais e também contra Estados nacionais (KREPINEVICH, 2012, p. V).

A empresa McAffee, especializada em segurança digital, divulgou um relatório em 2010 com o seguinte título: *Sob fogo cruzado. Infraestrutura Crítica na Era da Guerra Cibernética*. O relatório apontava que as redes estavam sob ataques constantes, inclusive de países estrangeiros. Em 2007, 120 países tinham ou estavam desenvolvendo capacidades de espionagem ou guerra cibernética. O relatório de outra empresa especializada em segurança digital, a Norton, divulgou o relatório *Norton Cyber Security Insights Report 2016*. Somente no Brasil, 42.4 milhões de usuários foram afetados pelo cibercrime em 2016. O prejuízo financeiro foi de US$10.3 bilhões apenas em 2016 e considerando apenas o Brasil (NORTON: 2016).
Com o passar dos anos, a disseminação da rede cresceu exponencialmente e a utilização da Internet se tornou uma atividade mais do que rotineira na vida das pessoas.

Toda a praticidade que a Internet proporciona muitas vezes esconde o grande perigo da vulnerabilidade da rede que pode passar despercebido pelo usuário comum. Desde o "The Creeper", o primeiro vírus de computador criado em 1971 (KLEINA: 2011), cujo único objetivo era irritar o operador da máquina infectada e provar para o invasor que era possível imputar comandos remotamente em outro computador sem a autorização do seu usuário, a vulnerabilidade da rede tem sido cada vez mais explorada. Em 1999 o "Melissa" (PANDA: 2013) ganhou destaque na mídia global por ser o primeiro vírus capaz de se espalhar com velocidade, atingir um número de dispositivos sem precedentes e causar um prejuízo de alguns milhões de dólares a agências governamentais e empresas privadas.

O ano de 2013 foi marcado por um acontecimento relevante na área de segurança digital. Edward Snowden, ex-analista da NSA (Agência de Segurança Nacional do Governo dos Estados Unidos), após deixar a Agência, fez a divulgação de dados que eram sigilosos. No mês de junho, ele entregou milhares de documentos confidenciais da NSA para os jornalistas Glenn Greenwald e Ewen MacAskill, ambos do jornal inglês The Guardian. Os documentos demonstravam o modus-operandi da Inteligência Americana e revelavam detalhes dos procedimentos de espionagem que o Governo dos Estados Unidos usava para vigiar cidadãos americanos. Segundo as informações de Snowden, são utilizados servidores de empresas grandes e conhecidas como Facebook, Google e até a Apple (G1: 2013).

Além de espionar seus próprios cidadãos, o governo dos Estados Unidos fazia o monitoramento de cidadãos, empresas e até chefes de estado de outros países da Europa e da

América Latina, incluindo o Brasil. Ficou comprovado que houve um monitoramento de conversas da então presidente Dilma Rousseff, de seus assessores e de aliados visando obter informações relacionadas à Petrobras, empresa brasileira de petróleo.

> A NSA não tinha interesse nessas boas relações; os espiões norte-americanos estavam interessados no pensamento particular de Dilma. Um slide da NSA obtido pela Spiegel mostrava que analistas tinham obtido acesso a mensagens de Dilma. Fort Meade investigava "os métodos de comunicação e seletores associados da presidenta brasileira e de seus principais assessores", relatou a revista. A agência também havia descoberto outros "alvos de alto valor" dentro do círculo íntimo da presidenta (HARDING: 2014, p. 139)

2.4. GUIA DE DEFESA CIBERNÉTICA NA AMÉRICA DO SUL

O Guia de Defesa Cibernética na América do Sul foi lançado em 2017. Ele tem como público-alvo "acadêmicos, tomadores de decisões, agentes de defesa cibernética e entusiastas da temática" (OLIVEIRA et al: 2017, p. 25). O livro reúne dados públicos sobre iniciativas nas áreas de segurança e defesa cibernética dos 12 países sul-americanos: Argentina, Bolívia, Brasil, Chile, Colômbia, Equador, Guiana, Guiana Francesa, Paraguai, Peru, Suriname, Uruguai e Venezuela. "Argentina, Brasil e Colômbia ganharam espaços próprios, enquanto os demais países foram abordados em três grupos, conforme as populações de usuários." (OLIVEIRA et al: idem).

O objetivo do documento é mostrar como o espaço cibernético afeta o espaço físico e apresentar ao público uma referência de como o tema vem sendo abordado no Brasil e em outros países da América do Sul. A importância do estudo do tema é abordada na apresentação do livro:

> Apesar do caráter intangível do espaço cibernético, certos aspectos geográficos tradicionais, como território e população, interferem no seu dimensionamento, seja pela infraestrutura necessária para a constituição de redes de informação, seja pela quantidade de seus usuários.
> O Brasil, quinto país do mundo em extensão territorial e em número de habitantes, contando com a metade dos usuários de Internet da América do Sul, é um ator relevante nas discussões da temática cibernética, tanto em nível acadêmico quanto nas relações internacionais, bem como no estabelecimento de políticas e estratégias adequadas à segurança e à defesa nessa nova dimensão (OLIVEIRA et al: 2017, p. 17).

Os capítulos são divididos entre: contexto e características (do país ou países abordados); fragilidades do espaço cibernético; documentos e marcos de referência e defesa cibernética. O livro apresenta gráficos baseados em estatísticas como uso do da Internet e tipos de ataques cibernéticos perpetrados. No contexto geral sobre a América do Sul, o Guia demonstra o crescimento de usuários entre os anos 2000 e 2014. O estudo informa que no

começo do século XXI havia similaridade na quantidade de usuários nos países da América Latina. Contudo, o Brasil elevou o número de usuários ao longo dos anos muito além dos outros países analisados:

> A discrepância no número de usuários do Brasil e dos demais Estados é justificada pela elevada população brasileira. A percentagem populacional de usuários de Internet de um país pode apresentar dúbia consequência para a defesa cibernética. A grande concentração de usuários pode ser benéfica, pois a familiaridade de uma nação com o espaço cibernético pode ser utilizada como recurso de poder cibernético. Entretanto, todos os usuários conectados a esse espaço também representam um canal de acesso para ameaças externas, ou seja, cada usuário pode ser alvo de ataques cibernéticos. (...)
> a grande discrepância de usuários entre o Brasil e o resto do subcontinente pode demonstrar um poderio cibernético ou uma grande vulnerabilidade, dependendo da forma com que esse recurso for gerido. Assim, não basta observarmos a quantidade de usuários de cada país da América do Sul, mas também a percentagem da sociedade que tem acesso ao espaço cibernético (OLIVEIRA et al: 2017, p. 30).

O livro deixa clara a importância de se estudar sobre defesa cibernética no Brasil: "Ao comparar o número de usuários desse país com o dos demais, encontramos uma enorme discrepância. Isso porque o total de usuários brasileiros se equipara à somatória de todos os demais usuários sul-americanos" (OLIVEIRA et al.: 2017, p. 30).

Ainda tratando sobre a América do Sul de forma geral, o Guia cita que é difícil mensurar as vulnerabilidades do espaço cibernético. Nem todos os Estados fazem um estudo relacionando os crimes cibernéticos e os impactos econômicos. Por isso, não foram encontrados dados especificamente ligados aos crimes cibernéticos na América do Sul. "No entanto, podemos ter uma noção desses custos por meio dos dados referentes à América Latina. Dessa forma, os crimes cibernéticos custam aos bancos latino-americanos cerca de US$ 93 bilhões por ano" (OLIVEIRA et al.: 2017, p. 35).

Assim como faz com outros países, o Guia de Defesa Cibernética na América do Sul apresenta as políticas brasileiras que serão tratadas a seguir.

2.5. POLÍTICAS BRASILEIRAS PARA SEGURANÇA E DEFESA CIBERNÉTICA

Em um texto oriundo de conferências na Escola Naval e no Instituto Rio Branco em 2013, Celso Amorim, o então Ministro da Defesa brasileira, afirma que: "País pacífico não é sinônimo de país indefeso. O complemento de uma política externa pacífica é uma política de defesa robusta" (AMORIM: 2013, p. 135). Mesmo que exista a sensação de pacifismo, que não haja conflitos bélicos entre nações, é responsabilidade do Estado estabelecer legislações

estruturantes de defesa e segurança. O presente trabalho trata de quatro documentos brasileiros de referência: 1. Livro Verde; 2. A Política Nacional de Defesa (PND), 3. A Estratégia Nacional de Defesa (END), 4. O Livro Branco de Defesa Nacional.

2.5.1. LIVRO VERDE: SEGURANÇA CIBERNÉTICA NO BRASIL

O Livro Verde – Segurança Cibernética no Brasil, foi lançado pelo DSIC: Departamento de Segurança da Informação e Comunicações, que está vinculado ao Gabinete de Segurança Institucional da Presidência da República. A organização do Livro Verde ficou sob a responsabilidade de Raphael Mandarino Junior (Diretor do Departamento de Segurança da Informação e Comunicações – GSI/PR na época da publicação) e Claudia Canongia (Convidada pelo DSIC/GSIPR como representante do Grupo Técnico de Segurança Cibernética - GT SEG CIBER GSIPR-DSIC e ABIN).

O Livro Verde contou com a colaboração de especialistas de diversos órgãos da Administração Pública Federal, direta e indireta, dentre eles: Gabinete de Segurança Institucional da Presidência da República (GSIPR – DSIC e ABIN), Ministério da Justiça (MJ e DPF), Ministério das Relações Exteriores (MRE), Ministério da Defesa (MD), e Comandos da Marinha, do Exército e da Aeronáutica. A Coordenação do Grupo de Trabalho ficou a cargo do Gabinete de Segurança Institucional da Presidência da República (GSIPR), por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC) (MANDARINO; CANONGIA: 2010, p. 11).

O Livro Verde trata sobre a Segurança Cibernética no Brasil apresentando propostas de diretrizes básicas, com o fito de "iniciar amplo debate social, econômico, político e técnico científico sobre a Segurança Cibernética no Brasil" (MANDARINO; CANONGIA: 2010, p. 5). A apresentação do Livro Verde contempla as causas de sua escrita, além de fundamentar a necessidade de estudar e fomentar a Segurança Cibernética:

> Dentre as motivações do Gabinete de Segurança Institucional, órgão essencial da Presidência da República, para esta obra, tem-se a própria prerrogativa do Gabinete de coordenar a atividade de Segurança da Informação, mantendo o compromisso com o Estado. Assim, motivado por esta missão e considerando a necessidade de assegurar dentro 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 (MANDARINO; CANONGIA: 2010, p. 5).

A obra é dividida em três partes gerais: objetivo; visão Brasil e diretrizes a serem contempladas na Política Nacional de Segurança Cibernética. Ela foi lançada em 2010 e anunciava no prefácio o ensejo de contribuir para a elaboração do Livro Branco de Defesa. O prefácio também destaca que a iniciativa é incipiente no fomento das condições primordiais para compreender as premissas que tangem à Segurança Cibernética. Os autores evidenciam que compreender o novo paradoxo e se proteger das ameaças é desafiador. Portanto, não apenas o governo, mas também o setor privado, terceiro setor e a academia devem ter esse tema em suas agendas, não apenas no âmbito nacional, mas em amplitude global. O Livro Verde destaca que a segurança no campo cibernético é um desafio do século XXI que

> vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras [...] Dessa forma, o entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* de desenvolvimento (MANDARINO; CANONGIA: 2010, p. 13).

O objetivo do Livro Verde "visa expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética" (MANDARINO; CANONGIA: 2010, p. 17). Tais estratégias têm como premissa os seguintes vetores: "Político-estratégico, Econômico, Social e Ambiental, CT&I, Educação, Legal, Cooperação Internacional, e Segurança das Infraestruturas Críticas" (MANDARINO; CANONGIA: 2010, p. 17) e estão estruturadas em três períodos de tempo: curto prazo: (2 a 3 anos), médio prazo: (5 a 7 anos), e longo prazo: (10 a 15 anos).

Dentre os tópicos abordados, o Livro Verde aponta que países tidos como desenvolvidos (EUA, Reino Unido, Japão, Espanha, Austrália) estavam lançando ou revisando as Estratégias nacionais de segurança cibernética (MANDARINO; CANONGIA: 2010, p. 28). O texto discorre sobre a situação tecnológica computacional da atualidade. Também aponta a relevância da necessidade do Livro Verde e outras políticas de defesa cibernética face ao desenvolvimento dos sistemas em rede e as ameaças oriundas da conexão. Destaca que é necessária a integração do governo, da academia, do setor privado e da sociedade em geral para o desenvolvimento de ações protecionistas no cenário cibernético.

Para Ávila e Silva, o Livro Verde não apresenta "metas claras e objetivas a serem perseguidas para a formulação de uma política e de uma estratégia nacional de Segurança Cibernética" (ÁVILA; SILVA: 2011, p. 1527). Contudo, a iniciativa da criação do Livro Verde

mostra a preocupação da equipe, representando os órgãos em que trabalham em fomentar planejamentos em relação à segurança cibernética. Tais atitudes são essenciais para o desenvolvimento brasileiro nessa área.

2.5.2. POLÍTICA NACIONAL DE DEFESA (PND)

A Política Nacional de Defesa (PND) estabelece as diretrizes referentes à Defesa Nacional e norteia o Estado para que ele alcance tais objetivos. A Política é o documento de mais alto nível no que tange ao planejamento de defesa. A PND foi aprovada pelo Decreto no 5.484, de 30 de junho de 2005. Outrora, era chamada de Política de Defesa Nacional (PDN). Em 2012, sete anos depois de sua aprovação, o documento foi atualizado e recebeu o nome usado atualmente: Política Nacional de Defesa. A PND tem como foco as ameaças externas. O documento "estabelece objetivos e orientações para o preparo e o emprego dos setores militar e civil em todas as esferas do Poder Nacional, em prol da Defesa Nacional." (PND: 2012, p. 11).

A PND vincula o desenvolvimento do Brasil com o desenvolvimento da própria Defesa. Ou seja: em teoria, quanto mais o país se desenvolver na Defesa, mais desenvolvido estará também como um todo. Por si só, essa premissa norteia a necessidade de investimento em pesquisa e desenvolvimento em Defesa. O documento conceitua segurança e defesa nacional de formas distintas, os termos não são usados como sinônimos. Conforme o documento, a segurança é: "condição que permite ao País preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais" (PND: 2012, p. 15).

Já a Defesa Nacional é determinada como "o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas" (PND: 2012, p. 12). Portanto, a Defesa Nacional é uma das responsabilidades que cabe principalmente ao poder militar.

Um dos objetivos nacionais de defesa postulados pela Política é: "desenvolver a indústria nacional de defesa, orientada para a obtenção da autonomia em tecnologias indispensáveis" (PND: op.cit, p. 30). É essencial que o Brasil tenha condições de mitigar as vulnerabilidades cibernéticas a fim de evitar possíveis ataques. A Política alerta para

necessidade de fortalecer o setor cibernético, uma vez que ele é estratégico para a defesa do Brasil, pois:

> para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento (PND: op.cit, p. 32).

Em resumo, a Política Nacional de Defesa brasileira informa as diretrizes propostas pelo Estado, relaciona as áreas que devem ser desenvolvidas, apresenta quais são as áreas de responsabilidade da Defesa nacional e preconiza o desenvolvimento das bases para a defesa. Para que a Política seja seguida, foi estruturada a Estratégia Nacional de Defesa, que trata como colocar em prática a PND.

2.5.3. ESTRATÉGIA NACIONAL DE DEFESA (END)

A Estratégia Nacional de Defesa (END) foi estabelecida pelo Decreto Nº 6.703, de 18 de dezembro de 2008. Ela foi revisada e publicada juntamente com a PND. A Estratégia Nacional de Defesa versa sobre a característica do pacifismo brasileiro e a necessidade da criação de uma consciência nacional voltada para a Defesa. Tem por objetivo tratar da "garantia da soberania, do patrimônio nacional e da integridade territorial" (END: 2012, p. 41). Ela também trata da estruturação das capacidades relativas às Forças Armadas. A END se coaduna com a PND sobre o desenvolvimento nacional estar atrelado ao desenvolvimento da defesa.

Dentre os fatores necessários para a independência e soberania, está relacionada a "capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear" (END: 2012, p. 44). Conforme a END, a independência nacional é obtida através da "capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento" (Idem). A defesa de um Estado Soberano deve considerar o contexto de iminências para se preparar com eminência.

A END tem duas grandes divisões: a primeira que aborda a formulação sistemática da estratégia, tratando sobre a natureza e o âmbito dela, bem como dos objetivos estratégicos da Marinha, do Exército e da Aeronáutica. Essa primeira divisão também dispõe sobre os três setores estratégicos para o Brasil: espacial, cibernético e nuclear. A segunda grande divisão discorre sobre as medidas necessárias para a implementação da estratégia. Para o setor cibernético, a END prevê como prioridades:

> (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas; (b) Aprimorar a Segurança da Informação e Comunicações (SIC) [...] (c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional [...] (d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual; (e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais; (f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas; (g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e (h) Estruturar a produção de conhecimento oriundo da fonte cibernética (END: op.cit, p. 94).

As ações referentes ao setor cibernético são voltadas ao Departamento de Ciência e Tecnologia do Exército, que deve promover ações multidisciplinares em conjunto com o Ministério da Defesa e o Ministério da Ciência Tecnologia e Inovação. Dentre as ações previstas, estão: sistema integrado de proteção de ambientes computacionais, simulador de defesa cibernética, ferramentas de inteligência artificial e computação de alto desempenho (END: 2012, p. 142). Por fim, a END indica um quadro com o prazo para completar determinadas tarefas e o setor responsável pela execução (END: 2012, p. 152).

No ANEXO A da presente pesquisa, estão destacados todos os tópicos relacionados à cibernética, que integram a Estratégia Nacional de Defesa.

2.5.4. LIVRO BRANCO DE DEFESA NACIONAL (LBDN)

O Livro Branco de Defesa Nacional (LBDN) conta com um resumo dos objetivos principais tratados na PND e na END. O LBDN tem 370 páginas, que tratam de diversos assuntos relacionados à defesa, além de apresentar valores usados investidos e estimados. O LBDN é dividido em seis capítulos, que tratam dos seguintes temas: o Estado brasileiro e a defesa nacional; o ambiente estratégico do século XXI; a defesa e o instrumento militar; defesa e sociedade; a transformação da defesa e economia da defesa.

O LBDN não tem como único escopo a definição de atribuições militares, pois engloba a questão da defesa também no âmbito civil, levando em consideração o ambiente social e estratégico do contexto em que foi redigido. Ele explicita os objetivos para a defesa brasileira de forma transparente para todos os cidadãos do Brasil e também para comunidade

internacional. É possível acessar o LBDN no *site* do Ministério da Defesa em três idiomas: português, espanhol e inglês.

O LBDN foi construído com o envolvimento de diversos setores do Brasil. Além da escolha de militares, o texto conta com o incremento de atores do setor empresarial, acadêmico e da sociedade civil em geral. O então ministro da defesa, Celso Amorim, diz que o LBDN não foi elaborado nos escritórios do Ministério da Defesa, mas contou com a "realização de Oficinas Temáticas, Seminários e Mesas-redondas, contou com a participação de civis e militares, brasileiros e estrangeiros" (LBDN: 2011, p. 13). O LBDN informa a importância do tema e o objetivo de fomentar o Setor Cibernético no Brasil:

> A proteção do espaço cibernético abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede. (...) A implantação do Setor Cibernético tem como propósito conferir: confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional (LBDN: 2011, p. 69).

O LBDN define que a defesa cibernética é de responsabilidade do exército (LBDN: 2011, p. 200) e postula que a ameaça cibernética se tornou uma preocupação "por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (LBDN: 2011, p. 71). Assim como a END, o LBDN ratifica que "os setores cibernético, espacial e nuclear são decisivos para a Defesa Nacional" (LBDN: 2011, p. 102). Visando o desenvolvimento da capacidade de defesa cibernética, o LBDN dispõe de objetivos previstos para serem executados a curto prazo:

> construção da sede definitiva do Centro de Defesa Cibernética e aquisição da infraestrutura de apoio; aquisição de equipamentos e capacitação de recursos humanos; aquisições de soluções de hardware e software de defesa cibernética; e implantação dos projetos estruturantes do Setor Cibernético, ampliando a capacidade de resposta às ameaças (LBDN: 2011, p. 200).

O valor para investimento em defesa cibernética no período entre 2010 a 2023 foi estimado em 895,40 milhões de reais. Tal montante é apenas o segundo maior previsto para atender as estratégias prioritárias estabelecidas pelo Exército no Plano de Articulação e Equipamento (LBDN: 2011, p. 202). As revisões do Livro Branco de Defesa Nacional, da Política Nacional de Defesa e da Estratégia Nacional de Defesa foram encaminhadas para o Congresso Nacional em novembro de 2016, atendendo a Lei Complementar 97/1999, que foi alterada pela Lei Complementar no 136/2010. No glossário do LBDN, o crime cibernético está

conceituado dentro de ilícitos transnacionais como "manifestação da abrangência global e da crescente complexidade técnica das atividades delitivas" (LBDN: 2011, p. 263).

2.6. LEI Nº 12.737/2012, A "LEI CAROLINA DIECKMANN"

Antes de tratar do fato gerador da Lei 12.737, serão expostos os conceitos "público" e "privado", estudados por John B. Thompson na obra *A mídia e a modernidade: uma teoria social da mídia*. Embora o livro de Thompson, publicado pela primeira vez em 1995 não trate especificamente sobre a Internet, as definições usadas contribuem para elucidar o ocorrido envolvendo a atriz Carolina Dieckmann.

Carolina Dieckmann é uma modelo/atriz brasileira. Por aparecer em novelas da Rede Globo de Televisão, ganhou notoriedade no país, ficou "famosa", ou seja: conhecida pelo grande público. Tal público é ávido por informações de figuras conhecidas. Nas palavras de Thompson, "hoje nós estamos acostumados a pensar que os indivíduos que aparecem em nossos televisores pertencem a um mundo público aberto para todos." (THOMPSON: 2002, p. 109).

Embora a atriz tenha aparições públicas (televisivas e presenciais), ela também tem um aspecto privado, reservado de suas ações. Usando a conceituação de Thompson, público é "visível ou observável, o que é realizado na frente de espectadores, o que está aberto para que todos ou muitos vejam ou ouçam" (THOMPSON: 2002, p 112). Em contraposição, a definição de privado é: "o que se esconde da vista dos outros, o que é dito ou feito em privado ou segredo em um círculo restrito de pessoas" (THOMPSON: 2002, p 112). No âmbito do direito, Jesus e Milagre afirmam que "pessoas físicas ou jurídicas têm o direito à intimidade e privacidade, à segurança da informação, e este direito se estende ao que se encontra em seus dispositivos informáticos" (JESUS; MILAGRE: 2016, p. 91).

A vida privada de Carolina Dieckmann foi violada, quando seu e-mail pessoal (privado) foi invadido e fotos íntimas da atriz foram expostas de forma pública. Em maio de 2012, 36 fotografias expuseram a intimidade da atriz na Internet. Ela procurou a polícia no dia 07 de maio, dando início às investigações sobre o caso. Carolina foi extorquida em R$ 10 mil em troca da privacidade (G1: 2012).

O fato acelerou (e apelidou) a Lei 12.737, sancionada em 30 de novembro de 2012, oriunda do projeto 2793, apresentado em 29 de novembro de 2011. A Lei trata da tipificação criminal de delitos informáticos e acresceu o Código Penal (Decreto-Lei 2.848/40). A pena mínima prevê três meses de detenção no caso de invasão em dispositivo informático de outrem,

sem consentimento, visando ter os dados, adulterá-los ou ainda destruí-los. A pena máxima prevê reclusão entre seis meses e dois anos, acrescidos de multa, para os casos em que a invasão ao dispositivo informático captar comunicações privadas, segredos comerciais e/ou industriais e informações sigilosas. Caso o praticante do crime divulgue a informação, venda, ou transmita para outro(s), a pena será aumentada entre um e dois terços. A pena também é acrescida entre um terço até a metade se o crime for perpetrado contra membros do governo ou dirigentes da administração federal, conforme descrito no decreto:

> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal." (Brasil: 2012).

A detenção e a reclusão são previstas na Lei Nº 7.209, de 11 de julho de 1984, no artigo 33: "A pena de reclusão deve ser cumprida em regime fechado, semi-aberto ou aberto. A de detenção em regime semi-aberto ou aberto, salvo necessidade de transferência a regime fechado" (BRASIL: 1984).

A criação da Lei 12.737 demonstra juridicamente a necessidade de proteger possíveis vítimas do roubo de dados, invasão os dispositivos informáticos e quebra de sigilo. O vazamento de fotos de uma figura pública, aliado à cobertura midiática possivelmente

aceleraram a promulgação da Lei. Conforme Jesus e Milagre, "diversos requerimentos de urgência foram apresentados em relação ao Projeto de Lei sob análise, que tramitou em tempo recorde" (JESUS; MILAGRE: 2016, p. 74). Para Paganotti,

> A inércia parlamentar pode ser rompida ante o clamor que demanda resposta rápida e pontual para os problemas discutidos e propagados pela mídia massiva, visto que o episódio de crise gerado pelo ataque contra a atriz foi aproveitado como oportunidade para aprovação do projeto – e projeção de seus defensores – em tempo recorde para o congresso brasileiro (PAGANOTTI: 2014, p.136).

Até o momento da sanção da Lei 12.737, invasão de dispositivo informático com fins de cópia indevida ainda não era tipificada pela legislação brasileira. Jesus e Milagres informam que muitos promotores faziam denúncia desse tipo de situação como crime de furto, que é previsto no Código Penal, no artigo 155. Porém, os autores informam que "na doutrina, muitos asseveravam ser impossível a aplicação do tipo, considerando que a coisa 'dados' não saía da esfera de disponibilidade da vítima, mas tão somente era "copiada". Um 'ctrl+c' não poderia ser considerado furto" (JESUS; MILAGRE: 2016, p. 89). Tipificação de furto, pelo artigo 155: "subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa" (BRASIL: 1940). No caso de um bem material como um celular ou computador (tangíveis e palpáveis), a vítima de furto ficaria sem o bem. No caso de cópia de dados (intangíveis e não palpáveis), a vítima ainda teria a informação.

Alguns pontos da Lei 12.737 são omissos ou permitem mais de uma interpretação. O Art. 154-A prescreve: "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de *mecanismo de segurança* e com o fim de obter, adulterar ou destruir dados ou informações (...)" (BRASIL: 2012, grifo do autor). Não está claro o que pode ser considerado juridicamente um "mecanismo de segurança". Seria um programa antivírus? Uma senha para login no sistema operacional? Um cadeado físico? Um cofre, para a guardar o *hardware*? (JESUS; MILAGRE: 2016, p. 92). Caso a vítima não use um mecanismo de segurança em seu dispositivo (seja por desconhecimento ou por descuido), a lei ainda deveria ser aplicada?

O Artigo 5º da Constituição Federal informa no parágrafo XXXIX que: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (BRASIL: 1988). Mesmo com brechas para interpretação (fato que já ocorre com outras leis, passíveis da interpretação de quem aplica as diretrizes do Direito no Brasil), e mesmo tendo sido aprovada por pressão popular e midiática por envolver alguém famoso, a Lei 12.737 foi um passo positivo para o cenário legal, envolvendo o paradigma cibernético.

2.7. LEI Nº 12.965/2014, O MARCO CIVIL DA INTERNET

O Marco Civil da Internet foi sancionado em 23 de abril de 2014, pela Lei 12.965. A proposta inicial foi feita em 2011, com o projeto de Lei nº 2.126. A ideia inicial foi feita em 2009, com uma "parceria entre a Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ) e a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas" (BRAGATTO, SAMPAIO, NICOLÁS: 2015, p. 9). Isso se deu a partir de um texto publicado pelo CGI.br: Comitê Gestor da Internet no Brasil. O CGI.br tem como responsabilidades: "estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao Domínio de Primeiro Nível '.br'" (CGI.br), além de promover pesquisas e estudos referentes à Internet.

Contudo, Pereira relata que a origem da ideia para o Marco Civil advém do IGF (Internet Governance Forum), promovido pelas Nações Unidas. A Primeira Edição do IGF aconteceu em Atenas, na Grécia, em 2006 e contou com a participação de brasileiros. O segundo IGF foi feito em 2007, no Rio de Janeiro, Brasil (PEREIRA: 2015, p. 30). Depois da aprovação do Marco Civil, o Brasil sediou novamente o evento, na cidade de João Pessoa.

O processo para elaboração do Marco Civil da Internet envolveu não somente membros do governo, mas também a academia, usuários da internet e representantes da iniciativa privada. Para Paganotti:

> O projeto do Marco Civil foi ousado por permitir que usuários, grupos, entidades e especialistas da área pudessem discutir, em igualdade e no mesmo espaço, suas propostas para aprimoramento do projeto. Entretanto, esses grupos que foram engajados na formulação do projeto podem ainda encontrar dificuldade para influenciar os processos fechados e restritos da aprovação do projeto, que está na mão dos partidos políticos tradicionais que dominam a pauta de votação no Congresso (PAGANOTTI: 2014, p.136).

Apesar da vinculação do Marco Civil com a liberdade, houve debates e desconfianças sobre a redação do texto (BBC: 2014). Uma das formas de mitigar a polêmica foi a criação de páginas eletrônicas específicas para que os interessados pudessem acompanhar as novidades relacionadas à elaboração do Marco Civil: http://culturadigital.br/marcocivil. O *site* informa sobre o contexto do projeto, o conteúdo e o resumo sobre a primeira e a segunda fase do processo. A primeira fase do processo debateu as ideias da redação preliminar do Ministério da Justiça. A segunda fase foi discutida tendo como embasamento o projeto de lei (BARRETO, SILVEIRA: 2016 p. 9). Os debates públicos da segunda fase aconteceram entre 8 de abril e 30

de maio de 2010. O *site* explicita que o foco da legislação é a garantia de direitos e não a restrição da liberdade dos usuários.

A própria Internet serviu como instrumento de diálogo para a consolidação sobre o Marco Civil. Conforme Pereira, a participação on-line "funcionou como um típico fórum na Internet, permitindo que os usuários comentassem o dispositivo do anteprojeto de lei em si, além de reagir aos comentários de outros usuários, como em um tradicional fórum de Internet" (PEREIRA: 2015, p. 30). O diálogo para coleta de opiniões foi tão amplificado que o Ministério das Relações Exteriores enviou um comunicado às embaixadas perguntando como a Internet era regulada no país sede da embaixada (PEREIRA: 2015).

O relator do projeto, o deputado Alessandro Molon, na época filiado ao PT-RJ, idealizou que o Marco Civil se tornasse uma Constituição da Internet, "definindo direitos e deveres de usuários e provedores da web no Brasil." (BBC: 2014). A Lei 12.965 também serve de súmula de conceitos para alguns termos relacionados ao assunto, a saber: Internet, terminal, endereço de protocolo de internet (endereço IP), administrador de sistema autônomo, conexão à internet, registro de conexão, aplicações de Internet e registros de acesso a aplicações de internet, conforme abaixo:

> Art. 5º Para os efeitos desta Lei, considera-se:
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. (BRASIL: 2014).

Ao conceituar tais termos, a Lei deixa claro tanto para o legislador quanto para os cidadãos cada tópico abordado. A margem para uma interpretação errônea ou de má fé é

mitigada. Um exemplo de tal situação foi exposto no presente trabalho: o que seriam os "mecanismos de segurança", tratados na Lei 12.737? Quais seriam tais mecanismos? A ausência da segurança por falha, omissão ou desinformação do usuário invalidariam uma possível sentença para um possível crime cibernético? Há a necessidade de definir o que está sendo tratado na Lei para corroborar o comum entendimento.

O Marco Civil é dividido em três capítulos, com a seguinte estrutura: o capítulo I aborda as *disposições preliminares* da lei. O capítulo II trata *dos direitos e garantias dos usuários*. O capítulo III aborda a questão *da provisão de conexão e de aplicações de internet*, subdividido em duas seções. A primeira trata *da neutralidade de Rede*. A segunda seção fala da proteção *aos Registros, aos Dados Pessoais e às Comunicações Privadas*. O primeiro artigo resume o objetivo geral do Marco Civil: "Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria" (BRASIL: 2014).

Os princípios usados para a elaboração do Marco Civil podem ser observados na própria redação da Lei, no segundo artigo, itens II, III e IV:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> **I - o reconhecimento da escala mundial da rede;**
> **II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;**
> **III - a pluralidade e a diversidade;**
> **IV - a abertura e a colaboração;**
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.
> (BRASIL: 2014. Grifos do autor).

A consulta às embaixadas levou em consideração o reconhecimento da escala mundial da rede, entendendo que o contexto global da rede é válido para tratar sobre o assunto no Brasil. (PEREIRA: 2015). Há relações diferentes entre governos de países e o uso da Internet. Porém, é inegável que apesar de possíveis sanções ou cerceamentos, a Internet é usada globalmente. Ao envolver os cidadãos usuários da Internet, respeitou-se o "exercício da cidadania em meios digitais". O fórum foi livre para o debate de ideias sobre a futura lei, mantendo o diálogo possível. Ao envolver políticos, entidades privadas, usuários e a academia, houve a abertura para "a pluralidade e a diversidade" (BRASIL: 2014). As opiniões dos atores envolvidos não eram necessariamente uníssonas. Um jurista e um profissional de tecnologia poderiam ter ideias diferentes sobre a liberdade e o uso da rede. Permitir as opiniões e equilibrá-las favoreceu a heterogenia. Por fim, a iniciativa de envolver tantos atores contribuiu diretamente para "a abertura e a colaboração" (BRASIL: 2014).

O terceiro artigo expressa os princípios relativos ao uso da Internet no Brasil. A Lei 12.965 assegura liberdade de expressão; a privacidade; a proteção dos dados pessoais; a neutralidade da rede; estabilidade, segurança e funcionalidade da rede; responsabiliza os agentes conforme as suas atividades na Internet; garante a característica participativa da Internet e a liberdade para os negócios que são feitos conforme a lei.

O texto do Marco Civil remete aos direitos já defendidos pela Constituição Brasileira: a liberdade é um dos direitos e uma das garantias fundamentais, assegurada pelo artigo 5º: "Todos são iguais perante a lei, sem distinção de qualquer natureza, **garantindo-se aos brasileiros e aos estrangeiros residentes no País** a inviolabilidade do direito à vida, à **liberdade**, à igualdade, à segurança e à propriedade (...)" (BRASIL: 1988. Grifo do autor). A privacidade também é asseverada no artigo 5º, inciso X: "são invioláveis **a intimidade, a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL: 1988. Grifo do autor). A livre iniciativa é tratada no artigo 170: "A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social (...)" (BRASIL: 1988).

O Marco Civil relembra e reassegura direitos já previstos na Constituição. O que o Marco Civil apresenta como diferenciação é: Seu processo democrático, com a participação de diversos atores em sua elaboração. A proteção de dados pessoais. A conceituação de termos referentes à Internet e seu uso. A preservação e a garantia da neutralidade da rede, para que as informações trafegadas não sejam categorizadas entre preferidas e preteridas, sendo entregues (ou não) aos usuários, com isonomia.

A Lei 12.965 não tem caráter punitivo, nem repressor. Portanto, não esgota as categorias possíveis de cibercrimes nem define as penas em caso de transgressão. Ele é um instrumento que assegura direitos e garantias dos usuários e fornecedores da Internet.

2.8. MARINHA DO BRASIL E A CIBERNÉTICA

A Estratégia Nacional de Defesa delegou o Programa Nuclear Brasileiro à Marinha (END: 2012, p. 141). O setor cibernético ficou sob a responsabilidade do Departamento de Ciência e Tecnologia do Exército (END: 2012, p. 142). Embora não seja responsabilidade precípua da Marinha, a Força também se ocupa com o desenvolvimento de temas relacionados à cibernética. Silva trata sobre o pioneirismo da Marinha do Brasil no uso de recursos informáticos desde o

fim da década de 60. O autor conta que a Marinha foi a primeira das três forças armadas do Brasil que começou a usar sistemas de armas computadorizados nos anos 70, nas fragatas da classe Niterói (SILVA: 2014, p.204).

O CASNAV (Centro de Análise e Sistemas Navais) foi criado em 1975, com o objetivo de desenvolver procedimentos e táticas de emprego para os sistemas navais, além de elaborar sistemas digitais que ajudem no processo de decisão. Conforme o Ministério da Defesa, o CASNAV também faz "o desenvolvimento de algoritmos e sistemas aplicáveis à segurança da informação e à criptologia, e de sistemas de informação para apoio administrativo" (MINISTÉRIO DA DEFESA : 2019). Silva destaca que os projetos de segurança focados em certificação digital de Chaves-Públicas desenvolvidos desde a década de 90 "inspiram a implementação de um sistema de chaves-públicas de segurança para ser utilizado em toda administração pública federal" (SILVA: 2014, p.205). Ou seja: embora a Marinha não esteja voltada especificamente a combater uma possível guerra cibernética, ela se mantém pioneira que tange à tecnologia computacional.

O Apêndice I ao Anexo A, do PEO 2016 – 2020 do CASNAV preconiza a necessidade de preparação em casos de guerra cibernética e guerra centrada em rede:

> Deveremos estar preparados, também, para desenvolver sistemas criptológicos, sistemas de apoio à Guerra Cibernética e à Guerra Centrada em Rede, agentes inteligentes e sistemas dotados de realidade virtual e desenvolver, em geral, sistemas que reduzam as probabilidades de sucesso de ataque dos Hackers (CASNAV: 2016, p.17)

No âmbito específico de documentação da Marinha que trata sobre a cibernética, destaca-se o PETIM 2016-2019: Plano Estratégico de Tecnologia da Informação da Marinha. O documento é inteiramente focado na importância da TI e da atuação da Marinha em relação ao tema. O Plano Estratégico informa que:

> este papel, particularmente na Marinha do Brasil (MB), acompanha a tendência de expansão e evolução das tecnologias, difundindo cada vez mais o uso de equipamentos de informática, sistemas, programas e redes de computador, como suportes às tarefas de praticamente todos os ramos de atividades (BRASIL: 2016, p. 1).

De maneira geral, o Plano Estratégico de Tecnologia da Informação da Marinha busca fortalecer os planos já existentes e ir além: aprender e adaptar-se empiricamente às mudanças através do desenvolvimento dos pontos fortes e a diminuição dos pontos fracos (BRASIL: 2016, p. 1). Um dos fatores para alcançar a meta está descrito no Objetivo Estratégico 06: "fortalecer a capacidade da Marinha de atuar na defesa do ambiente cibernético". (BRASIL: 2016, p. 12).

Afinal, um aspecto crucial para fomentar o aprendizado no campo da Tecnologia da Informação passa por compreender e saber atuar no setor cibernético.

A Doutrina Básica da Marinha EMA-305 incluiu em sua 2ª revisão o tema referente às ações de guerra cibernética. Ela conta com um tópico específico sobre ações de guerra cibernética, que conceitua as características desse tipo de conflito (ver 2.1.2. Guerra Cibernética no presente trabalho). Além de definir o termo, a Doutrina estabelece os impactos e danos que esse tipo de situação pode causar: "A condução da GC pode impactar a MB, nos campos administrativo e operativo; e o País, nos níveis político, estratégico e operacional" (BRASIL: 2014, p. 3 - 24). Também explicam as razões de um possível ataque cibernético e os seus alvos:

> A velocidade inerente às Ações de GC pressupõe rapidez nas comunicações, medidas pré-planejadas e regras de comportamento. Essas ações englobam a Exploração Cibernética, para fins de produção de conhecimento de Inteligência, do Ataque Cibernético e da Proteção Cibernética.
> De forma geral, os "alvos" da GC são as infraestruturas estratégicas, assim consideradas as instalações, serviços, bens ou sistemas que, caso tenham a sua operação comprometida, afetam o cumprimento da missão de uma organização. Os ataques cibernéticos são passíveis de ocorrer, porque os sistemas computacionais possuem vulnerabilidades, e podem visar à subtração de dados; conhecimento das vulnerabilidades de redes e dispositivos; alterações de páginas na internet; interrupção de serviços; e degradação da infraestrutura estratégica (BRASIL: 2014, p. 3 - 24).

A Doutrina diz que entre as características do poder naval, que "deve explorar as características de mobilidade, de permanência, de versatilidade e de flexibilidade" (BRASIL: 2014, p. 1 - 5), está a *versatilidade* para alteração da postura militar a fim de executar diversas tarefas em ambientes díspares, inclusive o cibernético. Para tanto, a Doutrina exemplifica ações referentes à operação de inteligência:

> 3.4.18 - Operação de Inteligência compreende um conjunto de ações de busca que empregam técnicas operacionais e meios especializados, tendo como efeito desejado a obtenção de dados de interesse militar cujo conhecimento nos são negados. Sua execução requer planejamento detalhado e centralizado, assim como pessoal qualificado e adestrado para esse tipo de atividade. Além do homem, a tecnologia é bastante explorada na obtenção dos dados negados. Sensoriamento remoto, medidas de apoio à guerra eletrônica e Ações de Guerra Cibernética são alguns exemplos de seu emprego nas Operações de Inteligência.
> Os dados obtidos pelas Operações de Inteligência complementam os selecionados pela atividade de coleta, possibilitando a formulação dos conhecimentos necessários para a elaboração de planos militares decorrentes, nos seus mais diversos níveis, bem como para a adequada compreensão da Consciência Situacional Marítima (BRASIL: 2014, p. 3 - 19).

A EMA-305 coaduna com a Política Nacional de Defesa e com a Estratégia Nacional de Defesa, no sentido de garantir o interesse nacional com fomento tecnológico e fortalecimento

do setor cibernético, uma vez que os três setores estratégicos espacial, nuclear e cibernético são essenciais para a defesa nacional (END: 2012, p. 93).

Em 2018 o Centro de Instrução de Guerra Eletrônica do Exército Brasileiro ofereceu o Curso de Guerra Cibernética para integrantes do próprio Exército, além da Marinha e da Força Aérea Brasileira. Os militares puderam aprender mais sobre o setor cibernético nos exercícios práticos e teóricos (MARINHA DO BRASIL: 2018a). Também em 2018, A Marinha participou do 1º Encontro de Especialistas em Defesa Cibernética, juntamente com Exército e Aeronáutica. O encontro marcou o 8º aniversário do Centro de Defesa Cibernética (CDCiber) e teve oficinas práticas focadas em análise de incidentes, gestão de riscos cibernéticos, análise de artefatos maliciosos, forense computacional, teste de invasão e inteligência cibernética (MARINHA DO BRASIL: 2018b).

Tanto o curso de Guerra Cibernética como o 1º Encontro de Especialistas em Defesa Cibernética demonstraram a colaboração entre as Forças Armadas e a disponibilidade da Marinha e Aeronáutica em aprenderem sobre o setor cibernético. Tais ações cumprem a determinação do decreto Nº 6.703, de 18 de dezembro de 2008: "Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio país não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede (...)" (BRASIL: 2008, Decreto Nº 6.703).

Para fins de visualização da cronologia dos documentos apresentados, elaborou-se uma linha do tempo, contemplando uma década de documentações que tratam especificamente sobre a cibernética, conforme apresentado ao longo do capítulo 2.

Figura 3: Documentação brasileira relativa à cibernética, produzida entre 2007 e 2017. (Elaboração própria).

2.9. PONTOS TRATADOS NO CAPÍTULO 2 USADOS PARA ANÁLISE DOS CASOS INTERNACIONAIS

A pesquisa sobre os conceitos abordada no capítulo 2 servirá como base para a seleção e análise dos casos internacionais. A compreensão dos conceitos é fundamental para identificar se os episódios selecionados são passíveis de enquadramento na taxonomia apresentada ao longo do segundo capítulo da presente pesquisa.

A seleção dos casos se baseará em dois critérios. O primeiro deles é: o enquadramento dos acontecimentos na definição de Richard Clarke e Robert Knake, além da conceituação de Krepinevich. Segundo Clarke e Knake, as guerras cibernéticas são "(...) ações de um estado-nação para invadir computadores ou redes de outra nação com a intenção de causar danos ou transtornos" (CLARKE; KNAKE: 2015, posição 335). Tal definição coaduna com o conceito de Krepinevich, para guerra cibernética, que envolve ações de estados-nação para penetrar computadores ou redes, com o propósito de causar dano ao inserir ou corromper ou falsificar dados, danificar dispositivos de rede e ou computadores, causando danos em sistemas de controle de computador (KREPINEVICH: 2012). Para a seleção dos casos, levar-se-á em consideração os promotores dos ataques cibernéticos. Os casos selecionados têm referências que indicam um estado-nação como autor de um dano e/ou transtorno causado, conforme as definições de Clarke, Knake e Krepinevich. Ou seja: casos envolvendo empresas ou *hackers* agindo por si, sem um estado-nação autorizando ou solicitando o ataque não serão considerados para estudo na presente pesquisa.

O segundo critério para a escolha dos casos considera a disponibilidade de fontes que tratam sobre os episódios após o enquadramento como "guerra cibernética". A busca das fontes visa esclarecer qual ator perpetrou o ataque, quem sofreu o ataque, qual foi o dano causado, o que motivou a guerra cibernética, a forma como se deu o acontecimento e o tipo de artefato usado para causar danos ou transtorno no alvo.

Também serão consideradas as características da guerra cibernética, descritas por Parks e Duggan. A escolha dos casos levará em conta os danos provocados no ambiente cibernético com impactos no "mundo físico". Em tais casos, a distância entre alvo e atacante não são impeditivos para a realização do ataque. Verificar-se-á se os ataques provocados pela guerra cibernética são derivados, dão suporte ou originam confrontos da guerra cinética, também considerados por Parks e Duggan. A guerra cinética é feita nos domínios terra, mar, ar

e espaço. Aparatos como tanques, navios, aviões e soldados militares são os protagonistas da guerra cinética (PARKS; DUGGAN, 2011).

A seleção dos casos está intrinsecamente ligada aos ataques feitos no “ambiente cibernético”, conceituados por Lemos, Castells, Lévy, Rattray, Evans, Healey, Friedman, Singer, Ventre, Libick e Gleick, conforme explorado ao longo do capítulo. Os ataques feitos no ambiente cibernético são possíveis graças à evolução da tecnologia computacional. O aparato conceitual permite compreender que a Internet não abarca todas as possibilidades de ataque cibernético. A Internet, conforme visto na seção 2.1.6, é apenas uma parcela do ambiente cibernético. Portanto, a escolha dos casos não ficará restrita pelo entendimento errôneo que somente é possível realizar ataques cibernéticos através da Internet.

Por fim, será usado o conceito de "ataque cibernético", sendo uma ação usada na guerra cibernética. Além das características descritas por Fruhlinger e Libick, consideradas no capítulo, usar-se-á o conceito explicado pela Doutrina Militar de Defesa Cibernética MD31-M-07 e o Glossário das Forças Armadas MD35-G-01, para a definição de ataque cibernético: “compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL: 2014, p. 23); (BRASIL, 2015, p. 39).

As premissas acima foram consideradas para a seleção dos casos internacionais de ataques cibernéticos tratados no próximo capítulo. Os princípios e conceitos serão usados para escolha e tratamento dos casos, a saber: União Soviética (1982), Estônia (2007), Síria (2007), Geórgia (2008), Irã (2009/10) e empresas e entidades americanas (2015). Tais episódios serão analisados sob a ótica conceitual tratadas no presente capítulo.

CAPÍTULO 3: ATAQUES CIBERNÉTICOS INTERNACIONAIS

O terceiro capítulo apresenta os casos de ataques cibernéticos internacionais se enquadram no conceito de “guerra cibernética”, conforme exposto nas seções 2.1.2 e 2.9. Os casos foram enquadrados sob a perspectiva conceitual tratada no segundo capítulo do presente trabalho. Os casos serão apresentados por ordem cronológica dos acontecimentos:

1982: União Soviética

2007: Estônia

2007: Síria

2008: Geórgia

2009/2010: Irã (2009/10),
2015: Empresas e entidades americanas

Todos os episódios estudados no presente capítulo envolvem uma nação-estado executando o ataque (embora a autoria não seja sempre confirmada pelo atacante) e causando danos para os atacados. Os casos mencionados acima e tratados na pesquisa que se segue foram selecionados pelo impacto causado, repercussão internacional e documentação acessível. Conforme De Sá, Machado e Almeida informam:

> Até o presente, a humanidade não experimentou a guerra cibernética de forma tão ampla quanto o fez com a guerra cinética. Se, por um lado, os conhecimentos sobre a guerra cinética foram construídos com base em observações e registros feitos ao longo de milhares de anos, por outro, os conceitos sobre a guerra cibernética se baseiam em experiências adquiridas ao longo de algumas décadas. Ainda assim, os ataques cibernéticos já ocorridos representam uma valiosa fonte de informações para o estudo da guerra cibernética e suas vertentes. (DE SÁ; MACHADO; ALMEIDA: 2019, p. 93).

3.1. 1982: ATAQUE CONTRA A UNIÃO SOVIÉTICA

Em 1982, antes da difusão da Internet, a União Soviética sofreu o primeiro ataque cibernético, perpetrado por uma bomba lógica (MILLER; DALE: 2012; CLARKE; KNAKE: 2015; OGIE: 2017). O objetivo da União Soviética era construir um gasoduto de 3.000 milhas para fornecer gás natural para a Europa Ocidental. Para conseguir tal feito, precisava obter crédito e tecnologia no exterior. O presidente dos Estados Unidos Ronald Reagan proibiu que as empresas norte-americanas fornecessem equipamentos para a construção do gasoduto, que era estratégico para a União Soviética (DE SOUZA: 1984).

O documento da CIA *The Soviet Gas Pipeline in Perspective - Special National Intelligence Estimate*, (de setembro de 1982), tratava sobre o grau em que as relações ocidentais de comércio, tecnologia e energia ajudaram e poderiam ajudar no futuro a União Soviética a aumentar sua força militar e impor ônus indesejados às nações ocidentais. O documento aponta que “only the increase in gas exports through the Siberia-to-Western Europe pipeline will prevent a marked decline in Soviet hard currency imports in the 1980s” (CIA: 1982, p. 3). O relatório aponta os esforços soviéticos em melhorar a tecnologia para fazer o gasoduto, mas mesmo com os avanços, “soviets will still need all the help they can get in building major gas trunklines” (CIA: 1982, p. A-3). Se por um lado a União Soviética precisava da tecnologia para

construir o gasoduto, por outro, era importante para os EUA que o gasoduto não fosse construído.

Além de não querer o avanço tecnológico e econômico (e possivelmente militar) da União Soviética, o governo norte-americano tinha outro motivo para que o gasoduto não fosse construído. No início dos anos 1980, a KGB recebeu uma lista de tecnologias ocidentais que deveriam ser roubadas para proveito soviético. Um agente da KGB fez um acordo com a França: entregou a lista e ficou morando no país. A França, por sua vez, repassou a lista para os Estados Unidos, que ficaram sabendo quais itens eram importantes para os soviéticos. A CIA possibilitou o roubo dos itens tecnológicos pelos soviéticos, que não sabiam os itens tinham falhas propositais. A União Soviética precisava canalizar petróleo e gás das reservas siberianas, mas não conseguiu comprar bombas, válvulas e controles automatizados com as empresas americanas. A solução encontrada foi roubar os controles automatizados de uma empresa canadense. Entretanto, o roubo foi propositalmente facilitado pela CIA, pois o *software* havia sido adulterado previamente com uma bomba lógica, ou seja, um código malicioso (CLARKE; KNAKE: 2015).

Foi implementado um trojan no sistema SCADA (*Supervisory Control and Data Acquisition*) que controlava o gasoduto siberiano (MILLER; DALE: 2012). No começo, o *software* funcionou conforme o esperado. Porém, depois de algum tempo em funcionamento aparentemente normal, Clarke e Knake relatam que "em um segmento do gasoduto, o *software* fez com que uma extremidade da bomba trabalhasse na taxa máxima, enquanto na extremidade oposta outra válvula fechasse. A pressão resultou na maior explosão não nuclear já registrada, com mais de três quilotoneladas" (CLARKE; KNAKE: 2015). Conforme Zetter, "o resultado foi uma bola de fogo de uma explosão tão grande e feroz que foi detectada pelos olhos dos satélites em órbita" (ZETTER: 2017, p. 124).

Além de ser o primeiro caso passível de ser considerado como guerra cibernética, a explosão no gasoduto serve de alerta. A vulnerabilidade para ataque a um sistema não está somente na conexão via Internet. Os ataques na cadeia de suprimentos (*supply chain*) são plausíveis de acontecerem (LIBICKI: 2009). Quando um país (ou mesmo empresas) não controlam toda a cadeia de produção, é possível que comprem itens tecnológicos que já tenham bombas lógicas previamente instaladas, com o fito de sabotagem, espionagem ou mesmo destruição.

3.2. 2007: ATAQUE CONTRA A ESTÔNIA

Em 2007 a Estônia sofreu o maior ataque DDoS já executado (LIBICKI: 2009; CLARKE; KNAKE: 2015). A motivação para o ataque surgiu de uma revolta de vários cidadãos de ascendência soviética após o governo estoniano trocar o local de um monumento soviético homenageando o extinto bloco comunista por sua participação na Segunda Guerra Mundial. A estátua do Soldado de bronze de Tallinn, antes chamada de Monumento aos Libertadores de Tallinn, é uma das obras russas que fica fora do território russo, a fim de celebrar a coragem dos soldados soviéticos e a participação da Rússia na Segunda Guerra. A estátua foi inaugurada em 1947, quando a Estônia estava sob o domínio soviético, na época da Guerra Fria. Doze soldados soviéticos estavam enterrados embaixo da estátua (EGOROV: 2017). Por esse motivo, o monumento é importante para os russos que vivem na Estônia e também na Rússia. Contudo, a maioria dos estonianos solicitou que as marcas de cinco décadas de opressão soviética fossem erradicadas do país. O legislativo estoniano aprovou a Lei das Estruturas Proibidas, que permitia a retirada de símbolos da ocupação russa. A resposta russa foi que isso profanaria o túmulo dos heróis mortos. A lei foi vetada, para evitar um incidente diplomático. Houve um conflito de opiniões entre os que queriam retirar os símbolos (incluindo o Soldado de bronze de Tallinn) e os que queriam manter a memória em forma de monumento (CLARKE; KNAKE: 2015).

Nos dias 26 e 27 de abril de 2007, russos e estonianos foram às ruas para ratificar suas opiniões. Foram duas noites de motins e saques. Cento e cinquenta e seis pessoas ficaram feridas, mil pessoas ficaram detidas e uma morreu (MCGUINNESS: 2017). O enfrentamento de 27 de abril foi chamado de “Noite de Bronze”. Para evitar mais revoltas e conflitos, a polícia removeu a estátua para um cemitério militar. A ação, em vez de pôr um fim na disputa, acirrou ainda mais os ânimos (CLARKE; KNAKE: 2015). Os protestos e confrontos manifestados nas ruas foram refletidos na Internet. Os agressores realizaram múltiplos ataques contra vários *sites* do país. Um deles, usaram uma técnica conhecida como DDoS (*Distributed Denial of Services*). Os alvos foram múltiplos. *Sites* de bancos estonianos, de veículos mídia e *sites* do governo foram atingidos por um ataque de negação de serviço em larga escala (FRIEDMAN; SINGER, 2010).

DDoS (*Distributed Denial of Service*) são ataques de negação de serviço. O problema é causado não através de uma invasão ao sistema, mas pela sobrecarga massiva, que inviabiliza o acesso pelos usuários. Os DDoS têm o objetivo de congestionar uma rede (tornando seu

acesso lento), ou derrubar uma rede (impedindo completamente o acesso). Esse tipo de ataque é controlado remotamente, usando computadores chamados de *botnets* ou zumbis. O usuário pode perceber lentidão no acesso, mas não visualiza o ataque na tela do seu computador, pois o DDoS roda em segundo plano (CLARKE; KNAKE: 2015). Assim, o ataque fica distribuído, pois cada uma das máquinas "zumbis" capturadas recebeu instruções enviadas pelo atacante para disparar ininterruptas requisições a um determinado alvo com o objetivo de causar a sobrecarga na rede. O ataque contra a Estônia foi lançado por uma *botnet* de 85.000 máquinas (ZETTER: 2017). Conforme o ataque avançou, mais de um milhão de "computadores zumbis" estavam envolvidos na investida contra os serviços on-line estonianos (CLARKE; KNAKE: 2015).

Por ser um dos países mais conectados à Internet, (LIBICKI: 2009; CLARKE; KNAKE: 2015), a Estônia foi um alvo certeiro para o ataque. Quanto mais a população é conectada à Internet e quanto mais os serviços públicos são distribuídos on-line, maior será o dano causado por esse tipo de procedimento. A investida persistiu por três semanas. No período mais crítico de atuação do DDoS, aproximadamente sessenta websites ficaram off-line, incluindo o maior banco da Estônia e os *sites* do governo (ZETTER: 2017).

Na busca pelos responsáveis, os rastros virtuais levaram até ao Kremlin, pois o código malicioso estava escrito em alfabeto cirílico. Esse fato, aliado ao contexto que ocasionou a tensão na noite de Bronze, levou especialistas a assumirem que Rússia a havia provocado o ataque cibernético. O governo russo negou envolvimento no ataque. Porém, não recebeu os investigadores que procuravam determinar o que realmente aconteceu. O pedido formal da Estônia foi negado pelo governo russo (LIBICKI: 2009; CLARKE; KNAKE: 2015).

Em janeiro de 2008, quase um ano após o ataque, um estoniano de ascendência russa foi condenado por executar pelo menos parte do ataque (LIBICKI: 2009). Segundo Krepinevich, alguns especialistas acreditam que o ataque contra a Estônia foi um teste russo para ataques cibernéticos, embora um porta-voz do governo russo tenha informado que os endereços IP poderiam ter sido falsificados ou as máquinas sequestradas, para incriminar a Rússia (KREPINEVICH: 2012). Libicki salienta que os ataques podem ter sido feitos por *hackers* indignados, tanto Estônia como na Rússia. Ou por membros da máfia russa ou por agentes do governo russo agindo em segredo (LIBICKI: 2009).

Em resposta ao ataque e sem a confirmação da autoria, a Estônia fechou suas fronteiras para acesso externo à Internet, embora tenham sido achados poucos dos *bots* envolvidos que realmente estavam dentro da Estônia, o que demonstra que os limites do ciberespaço não são

circunscritos pelas fronteiras territoriais. Para evitar mais ataques, apenas os usuários que moravam na Estônia poderiam acessar os *sites* estonianos, que ficaram vetados para usuários externos. Adicionalmente, a Estônia contratou empresas de roteamento para adicionar redundância às suas conexões externas com a Internet (LIBICKI: 2009). A Estônia também apelou para a OTAN, a fim de conseguir um acordo de defesa, mas o pedido foi negado, conforme explica Zetter:

> quando a Estônia acusou a Rússia de ser a fonte dos ataques e pediu ajuda da OTAN, tentando invocar um acordo coletivo de autodefesa nos termos do Artigo 5 da Organização do Tratado do Atlântico Norte, foi recusada. A OTAN decidiu que o ataque não constituiu um ataque armado nos termos do tratado. O problema reside no fato de a União Europeia e a OTAN não terem definido previamente as obrigações dos seus países membros na ocasião de um ataque cibernético contra um deles. A OTAN também não definiu ataques cibernéticos como uma clara ação militar, assim o Artigo 5 não entra automaticamente em jogo. Nos termos do Artigo 5, "um ataque armado contra um ou mais [membros] da Europa ou da América do Norte será considerado um ataque contra todos". No caso de tal ataque, espera-se que cada membro "apoie a parte ou as partes atacadas tomando imediatamente, de forma individual ou em conjunto com as outras partes, as medidas que julgar necessárias, incluindo o uso de força armada, para restaurar e manter a segurança da área do Atlântico Norte". O Primeiro Ministro da Estônia, Andrus Ansip, contestou a conclusão da OTAN perguntando: "qual é a diferença entre o bloqueio de portos e aeroportos de estados soberanos e o bloqueio de instituições governamentais e sites de jornais?" É uma questão válida que não foi adequadamente resolvida. Se bloquear carregamentos comerciais pode ser considerado um ato de guerra, frustrar o comércio eletrônico seria o equivalente no ciberespaço? E que tipo de resposta isso mereceria? Em 2010 a OTAN tentou resolver a questão concluindo que, se um aliado fosse atingido por um ataque cibernético, a OTAN ajudaria a defender as redes da vítima, mas a assistência ficava aquém de oferecer ajuda à vítima para conduzir um contra-ataque. (ZETTER: 2017, p.393).

Durante e depois do ciberataque, os países membros da OTAN e da União Europeia discutiram sobre segurança cibernética e punições cabíveis para os responsáveis por ataques virtuais (HERZOG: 2011). Em 2008 a OTAN criou um centro de defesa cibernética próximo do local onde ficava a estátua do Soldado de bronze em Tallin (CLARKE; KNAKE: 2015). As pesquisas feitas no centro de defesa cibernética foram publicadas em dois manuais: o primeiro Manual Tallinn, publicado em 2013 e o segundo, Manual Tallinn 2.0, publicado em 2017, dez anos após o ataque, tratam sobre a aplicação da lei em casos de conflitos cibernéticos. O ataque alertou sobre a necessidade de legislação aplicada aos crimes virtuais, além de proteção digital constante. Há um novo paradigma que deve ser considerado. Conforme a observação de Herzog: "Um novo desafio surgiu para as sociedades livres: as democracias devem encontrar maneiras de haver equilíbrio entre permitir a liberdade na Internet, por um lado, e manter

sistemas adequados de alerta precoce e monitoramento, por outro." (HERZOG: 2011, p. 56, tradução nossa).

O *site* estoniano (https://estonia.ee/smart-tech/) informa que o país é um dos mais bem instruídos em matemática, ciências e Tecnologias da informação e comunicação (TICs), com empresas e instituições de pesquisa e desenvolvimento com força de trabalho altamente qualificada. Em 2005 o país já permitia que os estonianos fizessem a votação online. A página inicial do *site* oferece benefícios da sociedade digital com a residência eletrônica. O *site* convida o usuário a se tornar um "E-residente" para: estabelecer e gerir uma empresa baseada na União Europeia inteiramente online, obter acesso a uma variedade de serviços públicos e privados na Estónia e assinar digitalmente contratos e outros documentos. A página (https://e-resident.gov.ee/), também da Estônia, mostra os "E-residentes" estonianos espalhados pelo mapa-múndi. O texto informa que é o primeiro país a oferecer a e-Residency, uma identidade digital emitida pelo governo, com status que permite acesso ao ambiente de negócios digital transparente da Estônia. A página de "visão global" (https://estonia.ee/overview/) informa que a Estônia é conhecida pela ambição digital e que há muito mais para descobrir. Ou seja: apesar de ter sofrido o maior ataque de DDoS já registrado, o país reconhece a importância de continuar aprendendo e se desenvolvendo digitalmente.

3.3. 2007: ATAQUE CONTRA A SÍRIA

Na madrugada entre 06 e 07 de setembro de 2007 a Síria sofreu um ataque na usina nuclear de Al Kibar, que estava em construção (FOLLATH; STARK: 2009; DIPERT: 2013; CLARKE; KNAKE: 2015; ZETTER: 2017) Os militares sírios não perceberam o ataque até que perceberam um clarão, uma onda sonora e destroços produzidos por dezoito toneladas de munição, lançadas por aviões de guerra F-16 e F-15 (CLARKE; KNAKE: 2015; DEFESANET: 2018). Esse foi o fim da "Operação Orchard".

O processo que deu início a operação começou em 2006, quando um alto funcionário do governo da Síria, sob a vigilância do Mossad (serviço secreto do Estado de Israel), deixou o notebook ao sair do quarto. Os agentes israelenses instalaram um trojan[8] para acesso aos dados

[8] "Trojan horse (Cavalo de Troia) - Os Cavalos de Troia são impostores. Os arquivos apresentam-se como programas desejáveis, mas são maliciosos. Uma distinção muito importante dos vírus verdadeiros é que esses arquivos não se replicam, como os vírus fazem. Os Cavalos de Troia contêm um código malicioso que, quando acionado, causa a perda ou o roubo dos dados. Para que ele se espalhe, basta convidar esses programas a entrarem em seu computador como, por exemplo, abrindo um anexo de e-

no dispositivo (FRIEDMAN; SINGER, 2010). Uma das informações reveladas pelo roubo de dados, foram as fotos do complexo em Al Kibar, que mostravam um processo de construção desde 2002. Pelas fotos da construção, percebia-se que o projeto era realizado para que não fosse possível perceber o seu verdadeiro propósito. As fotos do interior do complexo indicavam que possivelmente seria usado para fissão nuclear. Elas também mostravam um homem asiático e um árabe: Chon Chibu (cientista nuclear norte-coreano) e Ibrahim Othman (diretor da Comissão de Energia Atômica da Síria) (FRIEDMAN; SINGER, 2010; FOLLATH; STARK: 2009). Norte-coreanos também trabalhavam no prédio que foi destruído (CLARKE; KNAKE: 2015).

A Síria não sabia da invasão ao computador, nem que seus radares não estavam localizando ameaças como deveria. Apesar de investir milhões de dólares em sistemas de defesa aérea, os aviões israelenses F-16 e F-15 não foram detectados na noite da destruição da usina. (FRIEDMAN; SINGER, 2010). De acordo com Clarke e Knake, "o que apareceu em suas telas de radar foi o que a Força Aérea Israelense plantou lá, uma imagem de um dia qualquer. A imagem vista pelos sírios não tinha nenhuma relação com a realidade" (CLARKE; KNAKE: 2015, posição 321).

A Síria pediu explicações para a Rússia, país que vendeu o sistema de defesa aérea. Se o problema fosse na implementação ou no uso, seria detectado e ajustado. A Rússia não queria que seus produtos ficassem sob suspeita, pois em breve, fechariam a venda de um sistema de mísseis e radares de defesa aérea para o Irã. Porém, o problema não foi causado por descuido no uso ou na implementação, como destacam Clarke e Knake: "quando os israelenses atacaram a Síria, eles utilizaram pulsos de luz e elétricos (...) para transmitir "0s" e "1s" e controlar o que os radares da defesa aérea síria viam" (CLARKE; KNAKE: 2015, posição 333).

Não se sabe com certeza qual foi a ação executada por Israel para "enganar" os radares russos. No artigo *Other-than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy*, Randall R. Dipert propõe três teorias:

> 1. Israel inseriu *backdoor* no *hardware* ou no *software* do sistema de informação sírio para permitir a ativação e a ofuscação do radar no comando através da Internet. Essa

mail. Os Cavalos de Troia também são conhecidos por criar uma porta dos fundos em um computador. A porta dos fundos dá a outro usuário acesso a um sistema e possivelmente permite o comprometimento de informações confidenciais ou pessoais. Diferentemente de vírus e worms, Cavalos de Troia não se reproduzem infectando outros arquivos, nem se autorreplicam." NORTON. Glossário. Trojan horse (Cavalo de Troia). Disponível em < https://tinyurl.com/y259wvmk>. Acesso em 23 jun. 2019.

teoria é incompleta para Dipert, uma vez que o sistema sírio provavelmente estava com air-gap).

2. A informação de controle foi enviada para o receptor do sistema Syrianradar por uma aeronave israelense. Dipert considera essa possibilidade improvável, pois para ele, um sistema de radares não seria usado para comunicação, uma vez que é praticamente impossível que os sinais codificados usados para tentar assegurar aos sírios que o eco do rádio não era proveniente do transmissor israelense.

3. A hipótese mais plausível para Dipert é que o sistema usava cabos óticos enterrados. Uma a equipe poderia ter localizado um cabo óptico ou um repetidor-amplificador eletrônico e conseguiu explorar o fluxo bidirecional de informações dentro do cabo, inserindo software ou dados brutos que manipulavam o processamento de informações de toda a rede de defesa aérea para dar um falso negativo (não mostrando a ameaça). Ou causava o mau funcionamento do sistema por um curto período de tempo. (DIPERT: 2013, p. 40).

Clarke e Knake também apresentam três possibilidades para a execução do ataque, sendo a terceira similar à hipótese apontada por Dipert:

1. Um VANT (Veículo Aéreo não Tripulado) foi enviado antes dos aviões para voar dentro do radar da defesa antiaérea síria. O radar enviaria um feixe direcional de ondas de rádio que bateriam no VANT, a não ser que ele estivesse com revestimento de material que absorve ou desvia os feixes. O VANT não seria percebido, mas receberia a informação do radar. Ele poderia enviar a mesma frequência de rádio de volta para o radar da defesa síria, fazendo com o sistema não operasse corretamente. Esse procedimento faria com que os aviões não fossem detectados.

2. Os agentes de Israel podem ter comprometido o sistema de defesa russo, usado pela Síria, inserindo uma *backdoor* no código. Essa seria uma maneira para acessar eletronicamente a rede de defesa antiaérea, dando o controle para Israel, que impediria o radar de apontar seus aviões no espaço aéreo sírio.

3. Algum agente israelense pode ter localizado um cabo de fibra ótico usado pelo sistema de defesa sírio e fez uma “emenda na linha”, permitindo a conexão e criando uma *backdoor* para acesso de Israel. Para Clarke e Knake, essa hipótese é improvável, porém plausível. Algum espião poderia ter tal informação e acesso (CLARKE; KNAKE: 2015, posições 368 e 369).

Independente da forma de execução, destaca-se que antes do ataque cinético contra a Síria, executado com aviões lançando munição, Israel fez dois ataques cibernéticos: o *trojan* no notebook do funcionário sírio e o ataque contra o sistema de radares. O ataque ao radar provou que é possível não apenas invadir um notebook para roubo de informações, como também é factível "sumir" com aviões e atacar um alvo, provocando destruição cinética com apoio da cibernético.

3.4. 2008: ATAQUE CONTRA A GEÓRGIA

A Geórgia estava sob o controle soviético até 1991, quando declarou a sua independência pela segunda vez. A primeira tentativa de independência aconteceu em 1918, com a desintegração do império russo, provocado pela Revolução Russa. A Geórgia foi invadida e passou a fazer parte da União das Repúblicas Socialistas Soviéticas. Dois anos depois de declarar a independência pela segunda vez, a Rússia apoiou dois territórios que queriam a independência da Geórgia: Ossétia do Sul e Abkházia. Ambos estabeleceram governos independentes da Geórgia, apesar de legalmente ainda fazerem parte dos domínios georgianos.

Tais ações resultaram em três ataques em sequência: o primeiro foi executado pela Ossétia do Sul contra a Geórgia, com uso de mísseis em uma série de ataques e invasões nas aldeias georgianas. Em resposta, houve o segundo ataque, da Geórgia contra a Ossétia do Sul, que teve os exércitos expulsos do território georgiano. O terceiro ataque, da Rússia contra a Geórgia, foi em apoio a Ossétia do Sul. Em agosto de 2008 a Geórgia foi atacada pela Rússia, com bombardeio e controle sobre uma pequena parte do seu território (CLARKE; KNAKE: 2015).

Além de sofrer com ataque cinético pela Rússia, os georgianos também foram atacados por diversas ações cibernéticas (SHAKARIAN: 2011). Antes mesmo da invasão no território físico da Geórgia, os sites do governo já eram atacados no ambiente virtual (SHAKARIAN: 2011; CLARKE; KNAKE: 2015). A primeira fase do ataque cibernético contra a Geórgia aconteceu em 07 de agosto de 2008, no mesmo dia em que a Rússia expulsava o exército da Geórgia do território da Ossétia do Sul. Sites do governo georgiano e a mídia local foram invadidos por *hackers*. O coronel chefe do Centro de Previsão Militar da Rússia, alegou que as invasões eram uma resposta da Ossétia do Sul. Shakarian considera que "o fato de esses alegados contra-ataques terem ocorrido apenas um dia antes do desencadeamento da campanha

terrestre levou muitos especialistas a sugerirem que os hackers sabiam a data da invasão" (SHAKARIAN: 2011, p. 67).

Na primeira fase do ataque, os sites georgianos sofreram com ataques DDoS, que usavam *botnets* ligadas às organizações criminosas russas, incluindo a RBN (Russian Business Network) (SHAKARIAN: 201). Ataques DDoS bloquearam o acesso dos georgianos aos sites de notícias da CNN e da BBC. Posteriormente, seis diferentes *botnets* foram usadas. Além de usar sites de quem não participava do ataque, haviam sites que recrutavam voluntários para se juntar à guerra cibernética contra a Geórgia. Bastava baixar um *software hacker* para participar do ataque (CLARKE; KNAKE: 2015).

Durante a segunda fase do ataque cibernético, além do bloqueio causado pelo DDoS, o site da presidência da Geórgia foi descaracterizado. Os *hackers* incluíram imagens que comparavam Hitler ao presidente da nação. O tráfego de Internet de todo o país foi afetado. "A entrada da maioria dos roteadores da Rússia e da Turquia que enviava tráfego para Geórgia foi tão inundada com os ataques que nenhum tráfego de saída poderia passar. Os hackers assumiram o controle direto do resto dos roteadores que suportavam o tráfego para a Geórgia" (CLARKE; KNAKE: 2015, posição 552). Tal ação impossibilitou que os usuários de Internet na Geórgia conseguissem enviar e-mail para outros países. Também não era possível acessar sites de notícias do exterior. Instituições financeiras, instituições de ensino e empresas também foram alvo dos ataques (SHAKARIAN: 2011). O domínio ".ge" (equivalente ao ".br") não estava mais sob o controle da Geórgia, que foi obrigada a migrar sites do governo para servidores em outros países. A página do presidente, por exemplo, foi repassada para um servidor no Blogspot do Google, que fica nos Estados Unidos (CLARKE; KNAKE: 2015).

Para evitar ataques no sistema bancário, os servidores georgianos foram desligados. Em resposta, os atacantes fizeram com que as *botnets* simulassem que a Geórgia estava realizando ataques. Os bancos estrangeiros cancelaram as operações com os bancos georgianos. Posteriormente, o sistema de cartões de crédito e de telefonia também foram atacados e pararam de funcionar (CLARKE; KNAKE: 2015). Como consequência, o sistema bancário georgiano ficou paralisado por dez dias. (SHAKARIAN: 2011). A essa altura, a Geórgia já tinha sofrido a invasão em seu território, invasão em sites do governo, bloqueio aos sites de notícias internacionais. Os cidadãos não conseguiam acessar normalmente a Internet, fazer transações bancárias, ligações pelo celular, nem pagamento com cartões de crédito.

Similar ao que aconteceu no ataque contra a Estônia, funcionários da segurança cibernética da Geórgia descobriram que muitos dos ataques poderiam ser rastreados até

servidores controlados pela Rússia (LIBICKI: 2009; KREPINEVICH: 2012). Contudo, o governo russo negou a autoria dos ataques e alegou que não tinha controle sob a resposta popular contra a Geórgia (CLARKE; KNAKE: 2015).

Apesar da negativa russa, Sharkarian descreve indícios que ligam o país ao ataque (além da invasão na Geórgia, como apoio a Ossétia do Sul): as *botnets* começaram a atuar muito rapidamente, enquanto o território georgiano era invadido, o que pode indicar preparo prévio. "Há outros indícios de que houve preparação. Em julho de 2008, servidores da Geórgia (e até a página da Presidência, na internet) foram "inundados" com a mensagem "win+love+in+Russia". Esses ataques foram originados a partir de uma botnet chamada Machbot Network, conhecida por ser utilizada por várias organizações criminosas russas" (SHAKARIAN: 2011, p. 71).

Em relação ao conflito cinético, houve um acordo de cessar-fogo em 12 de agosto de 2008. Duas semanas depois, a Rússia reconheceu a Abkházia e a Ossétia do Sul como estados independentes (KREPINEVICH: 2012). Com ou sem o envolvimento direto do governo russo no ataque cibernético contra a Geórgia, fica evidente a coordenação entre os ataques cinéticos e cibernéticos. Ambos foram perpetrados no mesmo período contra uma mesma nação e a Rússia foi beneficiada com os ataques cibernéticos. Conforme Zetter: "a cronologia dos ataques, imediatamente antes da invasão russa à Ossétia do Sul, foi para muitos prova suficiente de que a campanha digital era parte de uma ofensiva militar" (ZETTER: 2017, p. 371). Para Krepinevich, "just as radio and radar were integrated into operations during World War II to enhance the effectiveness of military forces, cyber weapons appear to have been employed by the Russians to enhance their forces' effectiveness" (KREPINEVICH: 2012, p. 55).

3.5. 2009: ATAQUE CONTRA O IRÃ

O Stuxnet, foi a primeira arma cibernética usada para causar danos físicos em um país (ZETTER: 2017; FALLIERE et al.: 2011; CLARKE; KNAKE: 2015 O ataque em conjunto feito pelos Estados Unidos da América e Israel teve como alvo as centrífugas nucleares iranianas (ARTHUR: 2018; ZETTER: 2017; FRIEDMAN; SINGER, 2010). O objetivo do Stuxnet era se infiltrar em sistemas de controle de centrífugas de enriquecimento de urânio iranianas e fazer com que elas funcionassem acima de sua capacidade. Tal ação promovia uma

sobrecarga nos equipamentos e consequentemente, a sua quebra (KREPINEVICH: 2012. p. 134).

Contudo, descobrir a arma cibernética, seu modo de ação, seus efeitos e seu alvo não foi uma tarefa simples. As respostas de como, quando e porquê relativas ao Stuxnet seriam completamente respondidas em 2010 (FALLIERE et al.: 2011). Porém, a introdução do *worm* remete a 2008, que aproveitou uma falha no Microsoft Windows (KREPINEVICH: 2012). As ameaças do tipo *worm* não dependem que o usuário repasse o código infectado adiante, pois consegue se autorreplicar através de vulnerabilidades (CLARKE; KNAKE: 2015). O Stuxnet se espalhou através da Internet, fazendo cópias de si próprio, a fim de aumentar o número de sistemas e dispositivos infectados. A maior parte das 'auto-cópias' infectadas foram descobertas no Irã (FALLIERE et al.: 2011). O Stuxnet estava escondido tanto para quem trabalhava na usina como para as empresas que oferecem proteção no ambiente cibernético. Os responsáveis pelo ataque camuflaram o que estava sendo feito. Esse fato remete à característica da camuflagem na Guerra cibernética, observada por Parks e Duggan: "cyberwarfare protagonists must try to hide evidence in the existing data streams". (PARKS; DUGGAN, 2011, p. 32).

O alvo do ataque, a instalação em Natanz, não tinha conexão à Internet nem a quaisquer outras redes (CLARKE; KNAKE: 2015). Havia um *air gap* a ser superado. Para a propagação do código malicioso, foram usados pen drives: dispositivos pequenos, que gravam dados em memória flash. Os invasores "contavam com alguém carregando a infecção de uma máquina para outra através de um pen drive ou, uma vez em uma máquina, por meio da rede local" (ZETTER: 2017, p. 92). Além de conseguir se replicar, o Stuxnet também conseguia fazer atualizações quando necessário, mesmo em dispositivos não conectados à Internet. Bastava uma rede local, com compartilhamento de arquivos para que a nova versão fosse instalada. O Stuxnet se propagou rapidamente, mesmo sem usar a Internet como forma de distribuição. Algumas empresas do Irã têm escritórios e contratados com clientes em outros países, o que ajudou a espalhar o *worm* (ZETTER: 2017).

A Symantec, empresa que trabalha produzindo antivírus para proteção de sistemas, recebeu o código malicioso para análise. Normalmente, em caso de ameaças comuns, um algoritmo faz a varredura nos códigos ameaçadores, agrupados por uma fila. Porém, quando algo incomum é localizado, há uma pesquisa manual para investigar a inconsistência. Ficou claro para os peritos que começaram a analisar o Stuxnet que essa era uma ameaça complexa,

diferente do que tinham visto antes. O arquivo principal era bem maior do que os *malwares*[9] analisados antes. Tendo em vista que as ameaças analisadas anteriormente tinham em média 10 a 15 KB, contra 500 KB do Stuxnet (ZETTER: 2017).

O Stuxnet se aproveitava de falhas específicas em um programa de *software*, desconhecida pelo fabricante, empresas de proteção e usuários. (CLARKE; KNAKE: 2015). Isso cria uma vulnerabilidade no sistema, permitindo uma entrada para o ataque, chamadas de "zero day", pois há zero dias entre a vulnerabilidade ser descoberta e o dia quando ocorre o ataque cibernético que explora a brecha no sistema. (KREPINEVICH: 2012). O Stuxnet usou quatro zero days diferentes para garantir a efetividade do ataque (CLARKE; KNAKE: 2015; (FRIEDMAN; SINGER, 2010).

O objetivo do Stuxnet consistia em invadir os dispositivos, reprogramar os sistemas de controle industrial através da modificação do código em controladores lógicos programáveis (PLCs) para que passassem a operar conforme a vontade do atacante, sem que os operadores percebessem o que estava acontecendo (FALLIERE et al.: 2011; CLARKE; KNAKE: 2015). Os PLCs são utilizados em diversos sistemas automatizados de controle, que incluem o sistema chamado de SCADA (*Supervisory Control and Data Acquisition*), em português, controle de supervisão e aquisição de dados. Eles são projetados para monitoria e envio de instruções para determinadas máquinas (ZETTER: 2017; CLARKE; KNAKE: 2015).

A alteração era feita quando o Stuxnet encontrava o *software* WinCC-7, da fabricante Siemens. Os dispositivos de controle usados nos motores da usina em Natanz, no Irã, eram comandadas pelo *software* Siemens WinCC. Com a penetração do Stuxnet, o controle dos equipamentos foi mudado, de modo que os motores oscilassem até estragar as centrífugas (CLARKE; KNAKE: 2015). A troca dos equipamentos começou a ser feita com uma frequência maior que a esperada. Há especulações que entre novecentas a duas mil centrífugas tenham sido danificadas pelo Stuxnet, antes de descobrirem a causa do problema (ZETTER: 2017).

O Stuxnet demonstrou que um código virtual pode causar danos em objetos físicos (FRIEDMAN; SINGER, 2010; KREPINEVICH: 2012), pois *software* causou danos em

[9] "Vírus, *worms e phishing scams* são conhecidos coletivamente como *malware* (código malicioso). Eles se aproveitam tanto de falhas em softwares quanto de deslizes de usuários, como entrar em sites infectados ou abrir anexos de e-mail. Os vírus são programas que são passados de usuário para usuário (através da Internet ou através de uma mídia portátil, como um *pendrive*) e que levam algum tipo de carregamento para comprometer o funcionamento normal de um computador, fornecer um ponto de acesso oculto ao sistema, ou copiar e roubar informações pessoais" (CLARKE; KNAKE: 2015, posição 1583).

hardware. Conforme Zetter: "o Stuxnet é o único ataque cibernético conhecido que causou a destruição física de um sistema. Mas há indícios de que os Estados Unidos estão preparando outros" (ZETTER: 2017, p. 2015). O planejamento do Stuxnet para causar destruição física nas centrífugas é um exemplo claro do que Parks e Duggan apontam como os efeitos cinéticos perpetrados pela Guerra cibernética: "Attackers can attack entities in the cyberworld as much as they want, but unless something happens in the physical world as a result, they might as well be playing Core Wars" (PARKS; DUGGAN, 2011, p. 32). O modo de ataque do Stuxnet é cibernético, com resultados cinéticos.

O potencial que o ambiente cibernético possibilita vai além da espionagem, invasão para ver, alterar e vazar informações, pois o Stuxnet provou ser possível criar uma arma com potencial destrutivo e usá-la à distância. O vazamento de determinada informação, a alteração do valor bancário de uma conta, as exposições de fotos, por exemplo, também têm potencial destrutivo, mas não mortífero. Embora o uso do Stuxnet por si só não tenha dizimado a vida de ninguém[10], ele mostrou que isso pode ser possível, conforme Zetter explica:

> A arma digital não apenas lançou uma nova era de guerras; ela alterou o panorama de todos os ataques cibernéticos, abrindo as portas para uma nova geração de ataques a partir de agentes de estado, ou não, com o potencial de causar dano físico ou mesmo perda de vidas de formas nunca antes demonstradas (ZETTER: 2017, p. 367).

O Stuxnet provou como um ataque planejado e executado de maneira virtual pode alcançar os mesmos efeitos destrutivos que uma bomba convencional (ZETTER: 2017).

> Kennette Benedict, diretora-executiva do "Bulletin of the Atomic Scientists", identificou uma série de paralelos entre o Stuxnet e as primeiras bombas atômicas em um artigo que escreveu para a publicação sobre a falta de antevisão que ocorreu no desenvolvimento e no lançamento de ambas as tecnologias. (...) Que ironia, então, observou Benedict, "que o primeiro uso militar conhecido da guerra cibernética tenha sido ostensivamente para prevenir a proliferação de armas nucleares. Uma nova era de destruição em massa terá início em um esforço para encerrar um capítulo da primeira era de destruição em massa". Apesar das semelhanças, há pelo menos uma diferença crucial entre as bombas atômicas dos anos 1940 e o Stuxnet. As dificuldades eram grandes para alguém construir ou obter uma arma nuclear – ou qualquer míssil ou bomba convencional, para esse efeito. Mas armas cibernéticas

[10] Dois atentados ocorreram em 29 novembro de 2010 contra dois cientistas nucleares. O caso está relacionado à tentativa de solapar o progresso das usinas iranianas, mas não foram executados pelo Stuxnet. Fereydoon Abbasi, especialista em separação nuclear de isótopos, membro da Guarda Revolucionária do Irã, sofreu uma tentativa de assassinato enquanto estava no carro com a esposa. Uma bomba foi colocada na porta do seu veículo. O cientista conseguiu escapar do veículo com a mulher. Ambos ficaram feridos, mas sobreviveram ao atentado. Majid Shahriari, professor de física nuclear também foi atacado. Atacantes em uma moto colaram uma bomba na porta onde estava Shahriari. Segundos depois a bomba explodiu, matando Majid Shahriari. (ZETTER: 2017).

> podem ser facilmente obtidas em mercados negros ou, dependendo da complexidade do sistema que se tem como alvo, podem ser construídas de forma customizada e improvisada por um habilidoso programador adolescente. A tarefa acaba ficando simples, já que cada arma cibernética carrega os esquemas de sua concepção embutidos em si. Quando você lança uma arma cibernética, você não envia somente a arma aos seus inimigos, você envia a propriedade intelectual que a criou, bem como a habilidade de lançar a arma de volta contra você. Seria comparável a um cenário onde, se em 1945 não fossem apenas precipitações radioativas que caíssem das bombas lançadas sobre Hiroshima e Nagasaki, mas todas as equações e esquemas científicos necessários para construí-las também (ZETTER: 2017, p. 368).

Porém, por mais que armas cibernéticas consigam provocar efeitos cinéticos, elas têm o uso limitado. Uma arma cibernética pode se tornar obsoleta e até inutilizável caso as configurações do alvo sejam alteradas. A obsolescência também acontece quando o ataque é executado e os meios são descobertos (ZETTER: 2017). Após a destruição inicial, a tendência é identificar como o ataque foi projetado, qual vulnerabilidade foi explorada e quais são as maneiras de prevenir novos danos. A investigação sobre o Stuxnet envolveu diversos profissionais, ganhou notoriedade na mídia, (FALLIERE et al.: 2011), gerou relatórios, documentários e livro.

Se as centrífugas iranianas fossem destruídas cineticamente, o Irã saberia imediatamente sobre o problema. O ataque cibernético, além de não colocar vidas dos atacantes em risco, também obnubilou a ação. O dano era feito silenciosamente, sem que os iranianos percebessem de pronto que a falha nas centrífugas era proposital (FRIEDMAN; SINGER, 2010). Mesmo quando o Stuxnet foi localizado e neutralizado, não se pôde afirmar a identidade do(s) atacantes(s) pelo código malicioso (ZETTER: 2017). Todos esses fatores contribuíram para que o ataque tenha sido feito com uma guerra cibernética, ao invés de artefatos cinéticos.

Se por um lado o Stuxnet mostrou que as brechas em sistemas podem ser exploradas para causar danos, os profissionais que trabalham para proteger os sistemas, redes e dispositivos aprenderam com esse ataque. Há uma relação intrínseca entre atacar e defender. Sempre que houver um avanço na característica do ataque, também haverá um avanço para mitigar as vulnerabilidades. A melhoria no código ou sistema ou equipamento ou rede ou em todos os itens pode demorar, mas será prioridade para o alvo atacado. Além disso, as empresas, usuários e até países que não sofreram o ataque, mas sabem que há uma nova ameaça, procurarão se proteger.

3.6. 2015: ATAQUE CONTRA SETORES PÚBLICO E PRIVADO NORTE-AMERICANOS

No ano de 2018, a revista Bloomberg Businessweek (ROBERTSON; RILEY: 2018) publicou uma reportagem que denunciava suposta espionagem do governo da China a dezenas de empresas americanas. A suspeita de espionagem começou em 2015, quando a Amazon iniciou um processo de aquisição de uma startup visando investir no que mais tarde seria o Prime Video, concorrente da Netflix, provedora de entretenimento via streaming. A empresa se chamava Elemental e tinha sede em Portland, Oregon. Ela havia criado uma tecnologia de transmissão de vídeos em massa para dispositivos dos mais variados. Seu *software* foi responsável pela transmissão on-line dos Jogos Olímpicos, da comunicação com a Estação Espacial Internacional, além da transmissão de filmagens feitas pela CIA com seus drones.

Para certificar-se da segurança da Elemental, a Amazon contratou uma outra empresa que seria responsável por atestar a segurança do negócio. Uma fonte da Bloomberg afirma que ao iniciar o processo de exame, revelaram-se alguns problemas. Com isso a Amazon quis analisar mais de perto os servidores da Elemental, responsáveis pela compactação dos vídeos transmitidos. Ao verificar com mais cuidado, descobriu-se que os servidores foram fabricados por uma empresa chamada Super Micro Computer Inc., localizada em San Jose, na Califórnia. A comumente chamada Supermicro é uma das maiores fornecedoras de placas-mãe para servidores do mundo. Esses mesmos servidores foram encaminhados para a empresa terceirizada de segurança fazer testes.

Durante os testes nos servidores foi encontrado um pequeno microchip do tamanho de um grão de arroz. Esse microchip não fazia parte do design original das placas. Ao descobrir isso, a Amazon avisou as autoridades dos Estados Unidos. Descobriu-se também que quase 30 empresas dispunham dos servidores da Elemental. Dentre elas, um grande banco, a gigante Apple, além do Departamento de Defesa americano, a CIA e também navios da Marinha dos Estados Unidos.

Segundo uma fonte da Bloomberg, um agente da unidade do Exército de Libertação Popular da China teria se infiltrado no processo de produção de uma das fábricas que produzem as peças com o objetivo de implantar os microchips nos componentes que mais tarde fariam parte das placas-mães. Posteriormente, eles seriam incorporados aos servidores de empresas americanas e órgãos do governo. Apesar de pequeno, o microchip teria duas funções: 1. alterar o núcleo do sistema operacional possibilitando aceitar que modificações fossem feitas; 2. entrar

em contato com computadores controlados pelos espiões buscando mais instruções e novos códigos. Por conta de seus 900 clientes espalhados por 100 países, a Supermicro era o alvo perfeito para um ataque desse tipo. Segundo um ex-funcionário da inteligência americana, "Atacar componentes da Supermicro é como atacar o Windows. É como atacar o mundo todo" (ROBERTSON; RILEY: 2018).

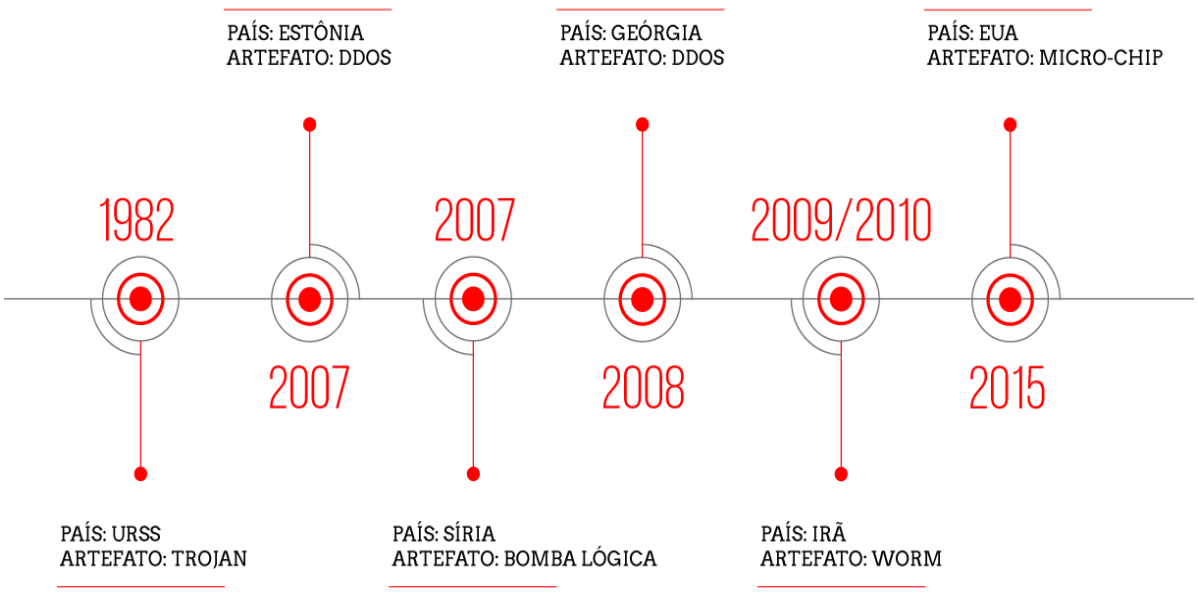

Figura 4 - Linha temporal dos ataques cibernéticos internacionais entre 1982 e 2015 (Elaboração própria).

CAPÍTULO 4: ANÁLISE DAS RESPOSTAS

O presente capítulo apresenta a análise feita a partir das respostas dadas por quatorze profissionais que atuam no campo de proteção cibernética. Destaca-se que os entrevistados têm profunda afinidade e conhecimento sobre o tema. As respostas foram enviadas por e-mail e os respondentes não serão identificados na pesquisa, conforme acordado anteriormente. A não identificação tem por fito permitir respostas francas concernentes à realidade brasileira.

Após o levantamento de bibliografia e informações no capítulo 2, que tratou sobre os conceitos relativos aos termos ligados ao objeto da pesquisa; sobre a evolução tecnológica computacional e sobre as políticas brasileiras para proteção cibernética, foi estabelecida uma

base para a seleção dos casos apresentados ao longo do capítulo 3. Conforme o título da presente pesquisa, o objetivo macro é obter reflexões para a Defesa Cibernética Brasileira a partir do estudo de casos internacionais. Portanto, elaborou-se um questionário com perguntas abertas, destinado a profissionais que têm afinidade com o tema e que atuam e estudam sobre conteúdos relacionados à defesa cibernética.

Uma síntese dos casos de ataques cibernéticos foi elaborada ao final de cada tópico do capítulo 3, a saber: 3.1. 1982: Ataque contra a União Soviética; 3.2. 2007: Ataque contra a Estônia; 3.3. 2007: ataque contra a Síria; 3.4. 2008: Ataque contra a Geórgia; 3.5. 2009: Ataque contra o Irã; 3.6. 2015: Ataque contra setores público e privado norte-americanos. Optou-se por enviar tal síntese em formato de tabela para os respondentes, como parte integrante do questionário, a fim de relembrar os casos ocorridos e demonstrar quais casos foram selecionados para compor a presente pesquisa.

Para a criação das perguntas, tomou-se por base o estudo dos casos internacionais, que geraram as seguintes perguntas macro:

- Quais são os maiores desafios para o governo brasileiro diante da possibilidade de uma guerra cibernética?
- Que ações são essenciais para que o Brasil esteja protegido contra ataques cibernéticos?
- Para a sociedade brasileira, quais seriam os principais problemas a serem enfrentados no caso de uma guerra cibernética?
- Que fatores têm colaborado para o aumento cada vez maior dos ataques cibernéticos no Brasil?
- Quais são os principais *gaps* do Brasil no cenário cibernético mundial? Como superá-los?

As perguntas acima não foram enviadas para os entrevistados, uma vez que não tinham relação direta com os casos de guerra cibernética relatados na presente pesquisa. A partir da característica de cada caso estudado, dentro do intervalo compreendido entre 1982 e 2015, foi escolhida uma peculiaridade referente a cada episódio para buscar extrair reflexões para Defesa cibernética no Brasil. O teor completo do questionário foi enviado como anexo por e-mail para os respondentes selecionados que se disponibilizaram a responder a pesquisa. A seguir, estão as perguntas formuladas com a finalidade de obter ensinamentos de especialistas para a proteção cibernética brasileira:

1) Quais funções exerceu na área de segurança/defesa cibernética ao longo da carreira? (A resposta não será exposta no texto da dissertação).

2) O ataque sofrido pela União Soviética ocorreu em 1982, quando o uso da Internet ainda não estava difundido. Os soviéticos não detinham o conhecimento tecnológico necessário para construir o gasoduto e tiveram que usar a tecnologia e equipamentos do Canadá. Houve uma sabotagem no sistema SCADA que controlava as válvulas do gasoduto, culminando na maior explosão não nuclear já registrada.

2.1) O desenvolvimento brasileiro em ciência, tecnologia e inovação é capaz de mitigar ataques na cadeia de suprimentos (*supply chain*)?

2.2) A proteção cibernética passa necessariamente pelo desenvolvimento de CT&I em geral?

2.3) Quais ações/políticas capazes de mitigar este tipo de ataque já foram adotadas no Brasil?

2.4) Quais ações/políticas ainda não tomadas poderiam ser implementadas?

3) A Estônia é um dos países mais conectados à Internet no mundo. Tal fato contribuiu para que os serviços básicos do país fossem afetados em 2007 por ataques de negação de serviço DDoS. Durante o ataque, os estonianos ficaram sem acesso aos serviços eletrônicos essenciais como bancos, páginas do governo, serviços de comunicação e de comércio.

3.1) É possível minimizar o risco de o Brasil sofrer esse tipo de ataque?

3.2) Se for possível, de qual(is) forma(s)?

4) Em 2008 a Geórgia sofreu um ataque conjunto: ao território do país e ao ambiente cibernético. Similar ao ataque contra a Estônia, a população ficou sem acesso aos sites de notícias internacionais, houve paralisação dos bancos, sites do governo foram ridicularizados e a Geórgia perdeu o controle de seus domínios ".ge".

4.1) Caso o Brasil sofra um ataque similar contra os sites oficiais do governo, sistema bancário e de comunicação, existe um plano de contingência que seja capaz de evitar que, assim como na Geórgia, a população fique sem acesso às fontes oficiais de informação e aos serviços essenciais?

4.2) Caso o plano não exista, é exequível criar ações nesse sentido? Quais?

5) Em 2007 a Síria sofreu ataque aéreo em uma instalação nuclear por duas brechas nos sistemas: 1) os radares sírios tiveram interferência israelense, para não apontar a ameaça. 2) as

informações sobre a construção do reator foram obtidas por uma invasão no computador de um alto funcionário do governo da Síria.

5.1) Os sistemas do governo e seus agentes têm proteção cibernética necessária para evitar ataques via trojan?

5.2) Se não têm, quais seriam as etapas necessárias para assegurar a proteção e detecção de uma possível espionagem?

6) O Irã experimentou os efeitos da chamada "primeira arma cibernética" na destruição de centrífugas nucleares, em 2009/2010. Através de ação feita no mundo virtual, usando o *worm* chamado de *Stuxnet*, foi provado que um código virtual pode causar danos em objetos físicos.

6.1) Que infraestrutura(s) crítica(s) do Brasil poderiam eventualmente sofrer um ataque similar, com execução no mundo virtual, causando danos físicos significativos?

6.2) Como proteger tais infraestruturas?

7) Que outras lições envolvendo **ataques cibernéticos** podem ser tiradas dos casos internacionais aqui citados para **proteção cibernética** brasileira no contexto atual?

O documento enviado para os respondentes com o questionário e as fontes usadas para estudo dos casos consta no Anexo B da presente pesquisa. A seguir, será apresentado no capítulo 4 uma análise de cada uma das respostas para as perguntas propostas.

4.1. ANÁLISE DA RESPOSTA À QUESTÃO 1

1) Quais funções exerceu na área de segurança/defesa cibernética ao longo da carreira? (A resposta não será exposta no texto da dissertação).

Dentre os quatorze entrevistados que responderam ao questionário, há membros de altos escalões das Forças Armadas Brasileiras que atuam com defesa cibernética; consultores em segurança da informação; responsáveis por empresas de segurança cibernética; mestres e doutores em áreas correlatas à tecnologia, segurança de sistemas informáticos e proteção cibernética; professores universitários de graduação e pós-graduação, atuantes na área de tecnologia e proteção da informação. Todos os profissionais convidados para o preenchimento do questionário têm anos de experiência no tema geral da pesquisa.

4.2. ANÁLISE DA RESPOSTA À QUESTÃO 2

2) O ataque sofrido pela União Soviética ocorreu em 1982, quando o uso da Internet ainda não estava difundido. Os soviéticos não detinham o conhecimento tecnológico necessário para construir o gasoduto e tiveram que usar a tecnologia e equipamentos do Canadá. Houve uma sabotagem no sistema SCADA que controlava as válvulas do gasoduto, culminando na maior explosão não nuclear já registrada.
2.1) O desenvolvimento brasileiro em ciência, tecnologia e inovação é capaz de mitigar ataques na cadeia de suprimentos (supply chain)?

As respostas ficaram divididas. Três respondentes disseram que sim. Dois desses respondentes justificaram a resposta afirmativa, informando que há restrições e que o aumento da capacidade de resiliência nos sistemas depende do desenvolvimento da indústria nacional em soluções voltadas para *Information Technology* (IT) e *Operational Technology* (OT). Dois respondentes responderam "não". Um não descreveu a justificativa para a resposta e outro deixou claro o motivo:

> Dificilmente hoje em dia, em que pese a dependência globalizada de componentes, até grandes potências vivem esse dilema. No entanto, o esforço de aumentar o percentual de nacionalização ou montagem certificada de componentes pode reduzir o risco (mitigar) tais ameaças.

Um dos respondentes elucidou que para responder à questão com embasamento, é necessário usar métricas. O balizador indicado foi o modelo "CMM (Capacity Maturity Model), do Global Cyber Security Capacity Center (GCSCC), desenvolvido pela Universidade de Oxford, Reino Unido". Tal métrica, baseada em uma metodologia com arcabouço conceitual comparativo de vários tópicos e com pesquisa em vários países, identifica que "em uma escala de 1 a 5, em média o Brasil atinge somente o estágio 2 nos conjuntos de fatores de Technologies relacionados a mitigação de ataques na cadeia de suprimentos". Ou seja: é necessário que o Brasil seja mais desenvolvido em ciência, tecnologia e inovação, a fim de minimizar as possibilidades de ataques na cadeia de suprimentos (supply chain).

Os demais respondentes não disseram "sim" ou "não" diretamente, mas indicaram que apesar do desenvolvimento do Brasil em ciência, tecnologia e informação, é preciso avançar mais e fomentar o aprendizado de novas tecnologias. Destaca-se a resposta de um entrevistado que certa maneira resume as respostas "sim" e "não, além da justificativas para a pergunta:

> Sim e Não. Sim, se toda tecnologia utilizada pela empresa na implementação de sua cadeia de suprimentos for de domínio / conhecimento nacional e estiver sendo testada constantemente. Não, se a tecnologia utilizada não for de domínio nacional.

Percebe-se que apesar dos esforços, é necessário que o país invista continuamente no estudo de novas tecnologias para que produza equipamentos para a cadeia de suprimento nacional. Contudo, com a globalização e o custo com a formação de profissionais capacitados que trabalhem na indústria nacional, é utópico acreditar que o Brasil será totalmente independente de equipamentos, peças sistemas e afins produzidos por outros países. Conforme o ataque relatado no tópico 3.6, até os Estados Unidos, tido como desenvolvido tecnologicamente, está sujeito a esse tipo de ataque envolvendo a cadeia de suprimentos. Conforme Clarke e Knake, é "difícil para o governo dos EUA comprar apenas *hardware* e software feitos nos EUA em condições seguras. Atualmente, é difícil encontrar qualquer *hardware* ou software de forma segura" (CLARKE; KNAKE: 2015, posição 1835).

2.2) A proteção cibernética passa necessariamente pelo desenvolvimento de CT&I em geral?

As respostas para a pergunta acima foram unânimes entre os respondentes. Para que o Brasil esteja protegido no setor cibernético, é necessário o desenvolvimento de CT&I. Um dos entrevistados sugere que é necessário formar a mentalidade das pessoas através do ensino escolar: "a sensibilização e conscientização deveria começar no ensino fundamental", pois "tais atividades também deveriam ser objeto de campanhas para parcela significativa da sociedade, que não cresceu ou não teve contato com a importância da proteção cibernética".

Uma das respostas leva em consideração a rapidez que as mudanças tecnológicas promovem e a necessidade constante de se adaptar:

> a CT&I tem importância fundamental para o desenvolvimento de técnicas, procedimentos, softwares (incluindo os de varredura) e hardwares capazes de mitigar ataques cibernéticos. No entanto, o desenvolvimento da CT&I deve ser constante para acompanhar a mutabilidade do ambiente cibernético.

As observações dos respondentes coadunam com a Estratégia Nacional de Defesa: "Independência nacional alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa, como para o desenvolvimento." (END: 2012, p. 44).

2.3) Quais ações/políticas capazes de mitigar este tipo de ataque já foram adotadas no Brasil?

Dentre as respostas, observou-se que alguns tópicos foram abordados no segundo capítulo da presente pesquisa, como a elaboração do Livro Verde: Segurança Cibernética no Brasil; a Estratégia Nacional de Defesa (END) e o Livro Branco de Defesa Nacional (LBDN). Outras ações que não foram abordadas na presente pesquisa e podem ser objeto de um estudo futuro, foram:

- Exercício Guardião Cibernético.
- Decreto Nr 9.573 - Política Nacional de Segurança de Infraestrutura Crítica.
- Decreto Nr 9.637 - Política Nacional de Segurança da Informação.
- A criação de EED (Empresas Estratégicas de Defesa)

Destaca-se abaixo a transcrição da resposta de um dos entrevistados, que propôs diversas ações para aumentar a capacidade do Brasil no sentido de mitigar ataques de uma possível guerra cibernética:

> I - planejar, e supervisionar a atividade nacional de segurança da informação, no âmbito da administração pública federal, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;
> II - formular e implementar políticas públicas de segurança da informação;
> III - elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação, no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;
> IV - manter Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, de responsabilidade nacional, para a proteção cibernética;
> V - coordenar e realizar ações destinadas à gestão de incidentes computacionais, no que se refere à prevenção, ao monitoramento, ao tratamento e à resposta a incidentes computacionais de responsabilidade nacional;
> VI - coordenar a rede de equipes de tratamento e resposta a incidentes computacionais - CSIRTs, formada pelos órgãos e pelas entidades governamentais;
> VII - propor e participar de tratados, acordos ou atos internacionais relacionados à segurança da informação, em especial, ao tratamento e à troca de informação sigilosa;
> VIII - assistir o Gabinete de Segurança Institucional da Presidência da República no exercício das funções de Autoridade Nacional de Segurança para o tratamento de informação classificada decorrente de tratados, acordos e atos internacionais;
> IX - atuar como órgão central de credenciamento de segurança para o tratamento de informação classificada;
> X - fiscalizar o credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para o tratamento da informação sigilosa;

> XI - articular, para o estabelecimento de diretrizes para as políticas públicas de Segurança da Informação, com os governos dos Estados, do Distrito Federal e dos Municípios, com a sociedade civil e com órgãos e entidades do governo federal; e
> XII - exercer outras atribuições determinadas pelo Secretário de Coordenação de Sistemas.

Verifica-se pelas respostas que as ações e políticas já adotadas pelo Brasil são importantes para a proteção cibernética em um possível ataque. Contudo, é necessário continuar o fomento nas ações práticas e em legislações que acompanhem o desenvolvimento tecnológico, que abrem brechas para novos tipos de ameaças e vulnerabilidades.

2.4) Quais ações/políticas ainda não tomadas poderiam ser implementadas?

A diversidade das respostas indica como o Brasil ainda precisa evoluir no setor tecnológico/cibernético. As sugestões foram analisadas, mapeadas e estão apresentadas abaixo, em forma de tópicos, divididas por assuntos:

1) Um dos respondentes indicou que o GSI já está elaborando Projeto de Lei sobre a Política Nacional de Segurança da Informação.

2) Outro entrevistado indicou que é necessário adotar uma regulamentação a fim de obrigar "empresas que lidam com infraestrutura crítica a implantarem a gestão do risco cibernético e também ficarem sujeitas a auditorias periódicas".

3) Colocar em prática os planos de ação e estratégias indicados na Política Nacional de Segurança da Informação.

4) Criação de políticas e leis voltadas para a segurança cibernética das infraestruturas críticas do Brasil que ainda não foram identificadas e por isso, são brechas de vulnerabilidades.

5) Melhoria das métricas apontadas no modelo CMM (Capacity Maturity Model) do Global Cyber Security Capacity Center (GCSCC), desenvolvido pela Universidade de Oxford, Reino Unido.

6) É necessário dar prosseguimento ao Exercício Guardião Cibernético.

7) Estimular o desenvolvimento de ações conjuntas de Defesa Cibernética com diversos órgãos públicos e privados.

8) Estímulo às empresas nacionais para desenvolvimento e melhoria da infraestrutura de rede, com a melhoria e criação de software e hardware.

9) Mapear as cadeias de valores dos produtos críticos e definir as dependências das tecnologias que o Brasil não domina.

10) Fomentar o senso de necessidade de proteção cibernética na sociedade, partindo por exemplo, da mudança ideológica nas universidades, pois, segundo um respondente, "pesquisadores que se associam a indústria (em alguns locais) são vistos como 'vendidos'".

Mais uma vez, percebe-se pelas respostas que é necessário que o Brasil evolua em suas políticas e ações para que possa estar preparado para combater ataques cibernéticos. Tais ações passam desde o estímulo à indústria, empresas privadas e universidades como na formação de uma mentalidade social que preze por esse tipo de segurança.

4.3. ANÁLISE DA RESPOSTA À QUESTÃO 3

3) A Estônia é um dos países mais conectados à Internet no mundo. Tal fato contribuiu para que os serviços básicos do país fossem afetados em 2007 por ataques de negação de serviço DDoS. Durante o ataque, os estonianos ficaram sem acesso aos serviços eletrônicos essenciais como bancos, páginas do governo, serviços de comunicação e de comércio.
3.1) É possível minimizar o risco de o Brasil sofrer esse tipo de ataque?

Doze dos quatorze respondentes responderam "sim", indicando a possibilidade de mitigar os riscos para o Brasil. Um deles salienta que é possível reduzir os riscos, mas "segurança 100% não existe". Dois entrevistados responderam que não é possível mitigar os riscos. Um deles justificou a impossibilidade devido a infraestrutura atual.

3.2) Se for possível, de qual(is) forma(s)?

As respostas incluem diversas sugestões (semelhante ao que foi respondido na questão 2.4). Novamente foi indicada a necessidade de incluir o tema na grade curricular começando já no nível fundamental. Também foi sugerida a necessidade de novas legislações e a aplicação prática de medidas já tratadas em legislações existentes. Também é preciso fortalecer a aplicação de tecnologias que identifiquem e combatam possíveis ataques cibernéticos. É imprescindível planejar e executar estruturas de segurança para as infraestruturas críticas do Brasil.

A resposta destacada na citação abaixo resume as opiniões dos outros respondentes, embora os entrevistados não tivessem acesso aos questionários dos demais consultados.

> Por meio do estímulo constante à pesquisa, desenvolvimento e evolução da CT&I, assim como o aporte adequado de recursos financeiros para esse fim;

> da continuidade ao processo de integração da Defesa, Indústria e Academia, a fim de desenvolver produtos de uso dual; da criação da mentalidade da segurança cibernética em todos segmentos da sociedade; e do prosseguimento às edições de exercícios do tipo Guardião Cibernético, com a inclusão de cada vez mais setores estratégicos da economia e do País.

4.4. ANÁLISE DA RESPOSTA À QUESTÃO 4

4) Em 2008 a Geórgia sofreu um ataque conjunto: ao território do país e ao ambiente cibernético. Similar ao ataque contra a Estônia, a população ficou sem acesso aos sites de notícias internacionais, houve paralisação dos bancos, sites do governo foram ridicularizados e a Geórgia perdeu o controle de seus domínios ".ge".

4.1) Caso o Brasil sofra um ataque similar contra os sites oficiais do governo, sistema bancário e de comunicação, existe um plano de contingência que seja capaz de evitar que, assim como na Geórgia, a população fique sem acesso às fontes oficiais de informação e aos serviços essenciais?

A maior parte dos entrevistados informou que: a) não tem conhecimento sobre um plano de contingência para tais situações descritas na pergunta. b) ainda não existe um plano pronto, mas está em fase de elaboração. Um dos respondentes afirma que "na Marinha, sim, existe e com frequência ela realiza exercícios sobre interrupção nas comunicações", mas não sabe informar se existe um plano nacional. Um dos respondentes acredita que se tal plano existe, ele deve ser secreto. Dois respondentes afirmaram que o plano existe, conforme descrito abaixo:

> Sim. As ações seriam coordenadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), com a participação do ComDCiber e das Forças Armadas a exemplo do trabalho de Defesa Cibernética que ocorreu durante os Grandes Eventos (Copa das Confederações 2013, Copa do Mundo 2014 e Olimpíadas Rio 2016.
>
> Sim, o PNTIR (Plano Nacional de Tratamento e Resposta de Incidentes Computacionais). Cabe ressaltar que tal plano está em fase de validação e não abrange todos os setores da sociedade.

Esse é outro tópico que poderia (ou deveria) ser pesquisado, uma vez que mesmo especialistas na área têm em geral, um desconhecimento a respeito de um plano de contingência e qual seriam as estratégias e táticas presentes no plano, além de qual órgão é ou deveria ser responsável por tal plano.

4.2) Caso o plano não exista, é exequível criar ações nesse sentido? Quais?

As Soluções propostas foram as seguintes:

1) Alinhamento de procedimentos com setores diversos para minimizar os efeitos de ataques de tal natureza.
2) Desenvolvimento e prática de Planos de Continuidade e Recuperação de Desastres para os serviços mais críticos.
3) Atuação do Ministério da Defesa através do Comando de Defesa Cibernética para criação de um plano e identificando quais atores deveriam executar as ações propostas.
4) O governo deveria contratar uma consultoria especializada para elaborar um plano de contingência que proteja os serviços essenciais e as fontes oficiais de comunicação.
5) Para evitar o isolamento do Brasil em caso de um ataque proposto na questão, é necessário ter cabos submarinos redundantes, que consigam escoar o tráfego na Internet.

Os ataques ocorridos na Geórgia e na Estônia demonstraram que ataques cibernéticos podem comprometer efetivamente os serviços básicos de uma nação. Ter um plano de contingência é necessário não por ser possível evitar completamente tal tipo de ataque, mas para reduzir o possível dano perpetrado.

4.5. ANÁLISE DA RESPOSTA À QUESTÃO 5

5) Em 2007 a Síria sofreu ataque aéreo em uma instalação nuclear por duas brechas nos sistemas: 1) os radares sírios tiveram interferência israelense, para não apontar a ameaça. 2) as informações sobre a construção do reator foram obtidas por uma invasão no computador de um alto funcionário do governo da Síria.
5.1) Os sistemas do governo e seus agentes têm proteção cibernética necessária para evitar ataques via trojan?

Um dos respondentes ressaltou que “os vazamentos de dados de comunicações pessoais de membros do Ministério Público nos últimos dias provam isso. Não temos uma Política de proteção dos ativos críticos, nem mesmo os de defesa”. Outro respondente informou que a proteção é mínima, “sem garantia 100%”. Outro respondente ressaltou uma importante questão na área de proteção cibernética: “as ameaças cibernéticas evoluem muito mais rápido do que as estruturas formais podem acompanhar, logo é difícil afirmar que já se tenha a proteção necessária”.

Mesmo as ações tomadas atualmente não garantem a proteção completa contra ataques via trojan. Mais uma vez, é necessário que o Brasil atualize os sistemas para enfrentar as novas

ameaças e vulnerabilidades. As ações não podem ser estanques. Há a necessidade de estudo, exercícios e adoção de novas maneiras que mitiguem as vulnerabilidades.

5.2) Se não têm, quais seriam as etapas necessárias para assegurar a proteção e detecção de uma possível espionagem?

Seis dos quatorze entrevistados não responderam a questão 5.2. Os demais sugeriram: uso de criptografia em arquivos com informações críticas; fomento da conscientização no setor de proteção cibernética; criação de canais seguros para comunicação; treinamento de autoridades; contratação de uma consultoria especializada; implementação de uma política de segurança nas instituições governamentais; uso de ferramentas que identifiquem e bloqueiem ameaças; capacitação de profissionais para identificação das ameaças.

É patente que não é possível prevenir uma possível espionagem cibernética atuando somente em uma frente. A combinação entre diversas ações é fundamental para diminuir o risco de espionagem em órgãos, sistemas, equipamentos e funcionários do governo.

4.6. ANÁLISE DA RESPOSTA À QUESTÃO 6

6) O Irã experimentou os efeitos da chamada "primeira arma cibernética" na destruição de centrífugas nucleares, em 2009/2010. Através de ação feita no mundo virtual, usando o worm chamado de Stuxnet, foi provado que um código virtual pode causar danos em objetos físicos.
6.1) Que estrutura(s) crítica(s) do Brasil poderiam eventualmente sofrer um ataque similar, com execução no mundo virtual, causando danos físicos significativos?

- Hidroelétricas.
- Usinas termonucleares.
- Refinarias de Petróleo.
- Sistemas de Comunicações.
- Instalações do Programa Nuclear Brasileiro.
- Geração e distribuição de energia elétrica.
- Setor de Comunicações.
- Setor bancário.
- Refinarias.
- Estações de tratamento de água.
- Setor de petróleo e gás.

- Infraestruturas críticas que utilizam sistemas SCADA.

Se apenas um dos setores mencionados pelos respondentes fosse alvo de ataques cibernéticos, o Brasil poderia sofrer prejuízos financeiros e tecnológicos. É preciso proteger as infraestruturas críticas e elaborar maneiras de identificar eventuais ataques, a fim de atenuar avarias e destruições na medida do possível.

6.2) Como proteger tais infraestruturas?

Em geral, os entrevistados assinalaram que é preciso manter boas práticas já aplicadas como o Exercício Guardião Cibernético, promovido pelo ComDCiber. Contudo, foi sugerido que o exercício não fosse feito "em um simulador e sim em instalações reais com os operadores que efetivamente operam os equipamentos e as redes de comunicação". Também é necessário implementar ações preventivas e adequar os procedimentos de segurança da informação. É preciso ainda treinar e capacitar profissionais, incutindo a consciência situacional. Um dos entrevistados ressaltou que "no Brasil, a Política Nacional de Segurança da Informação se desdobrará em Estratégias e em Planos de Ação que permitirão aumentar a resiliência cibernética frente a ataques de grande envergadura sobre as infraestruturas críticas nacionais".

4.7. ANÁLISE DA RESPOSTA À QUESTÃO 7

*7) Que outras lições envolvendo **ataques cibernéticos** podem ser tiradas dos casos internacionais aqui citados para **proteção cibernética** brasileira no contexto atual?*

Nove dos quatorze entrevistados adicionaram conteúdo além do que foi respondido nas perguntas anteriores. Abaixo estão realçadas as respostas que mostram a necessidade e dificuldade de executar a proteção cibernética no contexto do Brasil:

> Nenhum país está imune a esse tipo de ataque, cada vez mais a economia será integrada a redes de troca de dados e por sua vez as forças armadas tem que estar aptas a defender o chamado espaço cibernético de interesse do Brasil. Veja que não estou falando do espaço cibernético brasileiro, mas sim do espaço cibernético de interesse do país, ou seja além das nossas redes e ativos internos, se preocupar com o nível de proteção e defesa das redes e ativos que mais estabelecem conexões com as nossas.
>
> Em função de sua cada vez maior dependência tecnológica e das vulnerabilidades existentes em face ao baixo estágio de maturidade nos fatores apontados pela métrica utilizada**, não é uma questão de "SE", mas de**

> **“QUANDO” o Brasil irá sofrer um grande ataque cibernético em sua infraestrutura, a exemplo dos casos internacionais citados.** (Grifos do autor).

Embora o Brasil não tenha inimigos declarados e não esteja envolvido em conflitos bélicos por território, por exemplo, não exclui-se a possibilidade de ataques cibernéticos executados por outros países. Um dos entrevistados indica que para promover a proteção cibernética brasileira, os atores Governo, Forças Armadas e Sociedade Civil organizada devem trabalhar de forma colaborativa.

5. REFLEXÕES A PARTIR DOS CASOS INTERNACIONAIS

De Sá, Machado e Almeida apresentam uma síntese dos ataques de guerra cibernética já ocorridos e a forma como eles afetaram os alvos:

> - ataques cibernéticos com o objetivo de afetar sistemas de informação e de comunicação, porém sem o propósito de afetar diretamente sistemas físicos (ataques à Estônia e da Guerra Russo-Georgiana);
> - ataques cibernéticos com o propósito de afetar diretamente sistemas físicos (Stuxnet e o ataque ao gasoduto transiberiano); e
> - ataques cibernéticos envolvendo MAE visando prejudicar a obtenção de informações táticas, mas sem o propósito de manipular diretamente sistemas físicos (ataque na Operação Orchard) (DE SÁ; MACHADO; ALMEIDA: 2019, p. 100).

Estudar os casos de guerra cibernética já ocorridos é importante para adotar medidas preventivas. Examinar os tipos de artefatos usados para perpetrar ataques é fundamental para executar ações que mitiguem os riscos e/ou possíveis danos. Identificar os alvos mais críticos na estrutura brasileira para maior proteção é essencial para garantir mais proteção. Pesquisar as motivações e as formas como ataques já executados ocorreram ajudam a pensar estratégias preventivas. Analisar os danos causados por guerras cibernéticas colaboram para identificar as áreas mais vulneráveis e carentes de proteção.

O propósito da análise dos casos de guerra cibernética não deve ser motivado por preocupações alarmistas, mas pela vontade de promover melhoria contínua na proteção cibernética brasileira. Para que o Brasil esteja apto a se proteger no novo paradigma tecnológico, deve manter em prática as ações já postuladas pelas leis e doutrinas específicas sobre a defesa e segurança cibernética. Os casos internacionais ilustram o potencial de danos não apenas cibernéticos, mas também cinéticos provocados por uma guerra cibernética. Os casos também expõem a necessidade de proteção das estruturas críticas e melhoria constante.

As respostas para o questionário elaborado com base nos casos estudados na presente pesquisa são ricas em informações e sugestões para que o Brasil se desenvolva e fomente o saber tecnológico, diminuindo suas vulnerabilidades e aumentando a chance de reparar eventuais danos causados. A guerra cibernética não é uma distopia ou apenas um conceito sem consequências práticas. Ela é real e vem sendo praticada pelo menos desde 1982, antes mesmo da difusão global da Internet. Não existem sistemas totalmente seguros e totalmente incólumes, sem brechas a serem exploradas por possíveis inimigos. Aprender com casos reais ajuda na elaboração de políticas, ações e medidas para proteção cibernética brasileira.

Pelos casos estudado e pela análise dos especialistas, depreende-se de maneira geral as seguintes reflexões, que podem ser aplicadas para a melhoria da proteção cibernética no Brasil:

- É fundamental investir no desenvolvimento brasileiro em Ciência, Tecnologia e Inovação. A participação da indústria nacional no desenvolvimento de soluções voltadas para IT e OT ajuda na mitigação de possíveis ataques na cadeia de suprimentos (supply chain).
- Os ataques cibernéticos estão em constante evolução e reinvenção. A pesquisa no setor cibernético deve ser constante para que o Brasil tenha a chance de atenuar os danos dos ataques; identificar áreas vulneráveis e agir com celeridade caso sofra algum dano.
- O desenvolvimento da CT&I precisa ser contínuo, a fim de para acompanhar a rápida mutabilidade na área cibernética.
- É preciso estudar e desenvolver formas de proteção para as ameaças que surgem rapidamente, utilizando tecnologias como BlockChain, Data Analitics e Inteligência Artificial.
- A sociedade em geral precisa ser instruída sobre a necessidade do Brasil abarcar a proteção cibernética no tangente a Defesa e Segurança nacional.
- Necessidade de estimular mais pesquisas acadêmicas relacionadas ao assunto, a fim de compreender a realidade mundial e buscar se preparar tecnologicamente para o novo paradigma.
- As boas práticas já adotas devem continuar em exercício, para a melhoria e aprendizado constantes.
- Defender as infraestruturas críticas é essencial. Não existem sistemas plenamente seguros e completamente invulneráveis. A possibilidade de ataque, dado o não envolvimento do Brasil em conflito com outras nações, não é garantia de nunca ser atacado em uma guerra cibernética. Nenhum país ou sistema está imune a possíveis ataques.

- As reflexões aprendidas no presente estudo não esgotam a necessidade de outros estudos. Pelo contrário, indicam que é preciso estudar cada vez mais, compreender o novo panorama para que o Brasil esteja ciente e preparado para enfrentar e mitigar possíveis ataques.

6. CONCLUSÃO

Um mundo cada vez mais conectado promove novas possibilidades de interação, sociabilidade, produção de conhecimento e difusão de ideias. Esse novo paradigma cria vulnerabilidades que podem ser exploradas. A pesquisa desenvolvida buscou compreender os conceitos relacionados à Guerra Cibernética. A revisão da literatura permitiu a compreensão de como o avanço da tecnologia computacional pode resultar em combates cibernéticos. Através do estudo de casos já ocorridos de guerra cibernética foi possível identificar e constatar que ela pode provocar efeitos cinéticos, causando prejuízos que vão além da dimensão virtual.

Considera-se que o objetivo geral: identificar possíveis reflexões para a proteção cibernética brasileira a partir do exame de casos de ataques cibernéticos internacionais, foi alcançado. Além do amparo na literatura existente sobre o assunto, foi possível coletar insumos relevantes. Os objetivos específicos, a saber: *apresentar o avanço da tecnologia da Internet desde a sua criação; conceituar termos relacionados à Guerra Cibernética; examinar seis casos de ataques cibernéticos internacionais, que envolveram ações de uma nação-estado executando o ataques; examinar a regulamentação do setor cibernético para defesa do Brasil e analisar potenciais aprendizados para a defesa cibernética brasileira a partir desses casos* foram abarcados ao longo da pesquisa, embora não tenham esgotado o tema por dois motivos principais: recorte teórico e exiguidade de tempo para exame acurado de outras bibliografias.

O segundo capítulo apresentou um panorama sobre a segurança e defesa cibernética no Brasil tomando como pilares: o entendimento dos conceitos relacionados à guerra cibernética; as normas brasileiras que regulamentam e balizam as políticas brasileiras para a defesa nacional, além de leis aplicadas aos crimes cometidos por e contra civis na esfera do ciberespaço. O capítulo também contou com a apresentação do desenvolvimento tecnológico da Arpanet até o paradigma atual, que inclui a "Internet das Coisas". Cabe ressaltar que a pesquisa não se limitou a considerar casos de guerra cibernética apenas quando praticadas via Internet. O ciberespaço, conforme apresentado, é muito mais amplo e as brechas de vulnerabilidade não se concentram apenas na Internet.

O capítulo terceiro foi calcado na pesquisa de situações de guerras cibernéticas já ocorridas. A presente pesquisa se ocupou de analisar os cenários apresentados em cada um deles, buscando compreender as motivações para o ataque, o tipo de artefato utilizado, os alvos do ataque e a motivação para as ações. Defende-se aqui que os casos devem ser estudados e usados como exemplo para que o Brasil tenha condições de defender-se numa possível guerra do tipo cibernética, que poderia atentar contra a soberania do Estado Nacional. Os casos recentes envolvendo autoridades do governo indicam que a questão da proteção cibernética é importante.

Através da realização de um questionário com perguntas abertas, baseado nos seis casos selecionados para estudo foi possível coletar sugestões de profissionais que atuam na área de proteção cibernética. As respostas que foram analisadas, compiladas e sintetizadas no quarto capítulo enriqueceram a pesquisa atual, corroboraram com alguns pontos estudados e ampliaram a possibilidade de novos estudos sobre o tema.

A presente pesquisa não teve como pretensão esgotar o tema. Seria possível aumentar o número de entrevistados, buscar mais participações dentre civis que atuam em consultorias e na academia. Dada a exiguidade do tempo, optou-se por utilizar bibliografia que trata diretamente sobre o tema e já foi utilizada por outros pesquisadores em estudos correlatos. É possível aprofundar o estudo e apresentar mais reflexões, buscando mais casos para estudo e ampliando a participação de entrevistados.

Compreende-se que o tema carece de mais estudos para ampliar o conhecimento do novo paradigma. A pesquisa não esgota de forma alguma o assunto. Ao contrário, dá margem para outras análises, comparações entre casos, mais estudos sobre a situação mundial e a realidade brasileira. Apesar de sintético, é possível apreender reflexões dos casos internacionais, observar e aplicar as recomendações dos especialistas para que o Brasil cumpra as diretrizes da Política Nacional de Defesa e da Estratégia Nacional de Defesa.

REFERÊNCIAS

Apêndice I ao Anexo A, do PEO 2016 – 2020 do CASNAV.

ARTIGO 19. *Da Cibersegurança à Ciberguerra: O Desenvolvimento De Políticas de Vigilância No Brasil.*

ARTHUR. Charles. *Cyber Wars: Hacks that Shocked the Business World*. KoganPage. 2018.

ASSANGE, Julian. *Cypherpunks – Liberdade e o Futuro da Internet*. São Paulo: Boitempo Editorial, 2013.

ASHTON, Kevin. *That 'Internet of Things' Thing In the real world, things matter more than ideas.* RFID JOURNAL. 2009. Disponível em <https://www.rfidjournal.com/articles/view?4986>. Acesso em 22 jun. 2019.

AVAST. *Conheça a Avast.* Disponível em: <https://www.avast.com/pt-br/about> Acesso em: 22 set. 2018.

AVAST BLOG. *Avast update on WannaCry: who was affected, who was targeted, how to remove it, and more.* Disponível em: <https://blog.avast.com/wannacry-update-the-worst-ransomware-outbreak-in-history>. Acesso em: 22 set. 2018.

BBC. *Entenda as polêmicas sobre o Marco Civil da Internet.* 2014. Disponível em <https://www.bbc.com/portuguese/noticias/2014/03/140219_marco_civil_internet_mm>. Acesso em 12 jun. 2019.

_____. MCGUINNESS, Damien. *Como um ataque cibernético transformou a Estônia.* Disponível em <https://www.bbc.com/news/39655415>. Acesso em 18 de jun de 2019.

BRAGATTO, R. C.; SAMPAIO, R. C.; NICOLAS, M. A. *A segunda fase da consulta do marco civil da internet: como foi construída, quem participou e quais os impactos?.* Eptic (UFS), v. 17.

BRIGGS, Asa; BURKE, Peter. *Uma história social da mídia: de Gutenberg à Inter*net. 2a. Edição. Rio de Janeiro: Jorge Zahar Editor, 2006.

BORTOT, Jessica Fagundes. *Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional.* VirtuaJus – Belo Horizonte, v.13 - n.1, p.338-362– 1º sem. 2017. ISSN: 1678-3425. Disponível em: <http://periodicos.pucminas.br/index.php/virtuajus/article/download/15745/15745-56007-1>. Acesso em: 12 jun. 2019.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa, Aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 14 jul. 2017.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. Manual de Campanha Guerra Cibernética. Brasília, EB70-MC-10.232, 1ª ed., Brasília, 2017.

BRASIL. Ministério da Defesa. Doutrina Militar de Defesa Cibernética –MD 31-M07. Brasília, 18 de novembro de 2014. Disponível em:<http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em 05 de out. de 2018.

BRASIL. Estratégia Nacional de Defesa /Política Nacional de Defesa, 2012.Disponível em: <http://www.defesa.gov.br/component/content/article/145-forcas-armadas/estado-maior-conjunto-das-forcasarmadas/doutrina-militar/13188-publicacoes >. Acesso em 05 de out. de 2018.

BRASIL. 2014. Doutrina Militar de Defesa Cibernética MD31-M-07. Brasília 2014.

BRASIL. 2007. Doutrina Militar de Defesa. MD51-M-04. Brasília. 2007

BRASIL. 2014. Estado-Maior da Armada. EMA-305: Doutrina Básica da Marinha. Brasília.

BRASIL. DECRETO Nº 6.703, DE 18 DE DEZEMBRO DE 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, DF. Disponível em: <https://tinyurl.com/y5x6adx7>. Acesso em: 29 mai. 2019.

BRASIL. Lei Federal 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. Brasília: 2012.

BRASIL. Lei Federal nº 7.209, de 11 de julho de 1984. Altera dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, e dá outras providências. Brasília: 1984.

BRASIL. Código Penal. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Brasília: 1940.

BRASIL. Constituição Federal. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Brasília: 1988.

BRASIL. Apresentação do Projeto de Lei nº. 2126/2011, 2011.

BRASIL, Marinha do. Plano Estratégico de Tecnologia da Informação. Conselho de Informação da Marinha, 2016.

BAKER, Stewart et al. MCAFEE. Sob fogo cruzado: Infraestrutura crítica na era da guerra cibernética. 2010. Disponível em <http://img.en25.com/Web/McAfee/CIP_report_final_pt-br_fnl_lores.pdf>. Acesso em 29 nov. 2017.

BAUMAN, Zygmunt. *Medo Líquido*. Rio de Janeiro: Ed. Jorge Zahar Editor, 2008.

BLAINEY, Geoffrey. *Uma breve História do Século XX*. São Paulo: Editora Fundamento Educacional. 2011.

BEMFICA, Flávia. Guerra cibernética atingiu em cheio nosso governo. Disponível em <https://tinyurl.com/y2flefbb>. Acesso em: 15 jun. 2019.

BOMFIM, Camila. G1. *PF suspeita de ação orquestrada na invasão de celulares de Sérgio Moro e de procuradores*. 2019. Disponível em < https://g1.globo.com/politica/noticia/2019/06/11/pf-comeca-a-investigar-invasao-ao-celular-de-moro.ghtml>.

CANALTECH. *Internet das Coisas: Brasil tem cerca de 20 milhões de conexões entre máquinas.* 2017. Disponível em <https://canaltech.com.br/telecom/internet-das-coisas-brasil-tem-cerca-de-20-milhoes-de-conexoes-entre-maquinas-89384>. Acesos em 22 jun 2019.

CARRAPIÇO, Helena - *O Crime Organizado e as novas Tecnologias: uma faca de dois gumes. Nação e Defesa.* N.º 111 - 3.ª Série, 2005, pp. 175-192.

CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: orge Zahar Editor, 2003.

CASTELLS, Manuel. *A sociedade em rede.* São Paulo: Paz e Terra S.A, 2007.

CLARK, Jen. What is M2M technology? Disponível em <https://www.ibm.com/blogs/internet-of-things/what-is-m2m-technology>. Acesso em 02 set. 2019.

CLARKE, Richard. KNAKE, Robert. *Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito*. Rio de Janeiro: Brasport, 2015. Formato: eBook.

COHEN, Eliot. *Technology and warfare.* In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. *Strategy in the contemporary world.* 4ª ed. New York: Oxford University Press, 2013.

CORNISH et al. *On Cyber Warfare*. London: Chatham House Report, 2011.

DEPARTAMENTO DE FÍSICA - UFPR.6.2 *Nuvens.* Disponível em: <http://fisica.ufpr.br/grimm/aposmeteo/cap6/cap6-2.html>. Acesso em 13 jul. 2018.

DE SÁ Alan Oliveira; MACHADO, Raphael Carlos Santos; ALMEIDA, Nival Nunes: *O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo*. R. Esc. Guerra Nav., Rio de Janeiro, v. 25, n. 1, p. 89-128. janeiro/abril. 2019.

DE SOUZA, Patrick. *The Soviet Gas Pipeline Incident: Extension of Collective Security Responsibilities to Peacetime Commercial Trade*, Yale Journal of International Law. 1984. Disponível em < https://tinyurl.com/y272efxh>. Acesso em 21 jun 2019.

DUTRA, Moisés Lima; VIANNA, William Barbosa; FRAZZON, Enzo Morosini. *Big Data aplicado a Sistemas Ciber-Físicos da logística: proposta de modelo conceitual*. 2017. Disponível em < http://200.20.0.78/repositorios/handle/123456789/3216>

ESTADOS UNIDOS DA AMÉRICA. *Joint Chiefs of Staff. Cyberspace Operations*. Joint Publication (JP) 3-12, de 8 de junho de 2018.

EUROPEAN COMMISSION: 2019. *Cybercrime*. Disponível em <https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en>. Acesso em 12 jun. 2019.

EVANS, Dave. *A Internet das Coisas Como a próxima evolução da Internet está mudando tudo*. Cisco Internet Business Solutions Group (IBSG). 2011.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. *W32. stuxnet dossier.* White paper, Symantec Corp., Security Response, v. 5, n. 6.

FOLLATH, Erich; STARK, Holger. *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor.* Der Spiegel, Nov. 02, 2009. Disponível em <http://www.jmhinternational.com/news/news/selectednews/files/2009/11/20091103_Spiegel Online_TheStoryOfOperationOrchard.pdf>. Acesso em 23 jun. 2019.

FRUHLINGER, Josh. 2018. *What is a cyber attack? Recent examples show disturbing trends.* Disponível em <https://tinyurl.com/y5objfpe>. Acesso em 08 jun. 2019.
G1. *Tesla anuncia sistema 100% autônomo para todos os seus carros.* 2016. Disponível em <http://g1.globo.com/carros/noticia/2016/10/tesla-anuncia-sistema-100-autonomo-para-todos-os-seus-carros.html>. Acesso em 22 jun. 2019.

G1: 2012. *Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'*. Disponível em <https://tinyurl.com/7g9a7s9>. Acesso em 09 jun. 2019.

G1: 2013. *Entenda o caso de Edward Snowden, que revelou espionagem dos EUA*. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html> Acesso em: 16 out. 2018.

GLEICK, James. *A Informação: Uma história, uma teoria, uma enxurrada*. São Paulo: Companhia das Letras, 2013.

GNIPPER, Patrícia. CANALTECH. *Elon Musk promete carros Tesla totalmente autônomos para o final de 2019*. 2019. Disponível em <https://canaltech.com.br/carros/elon-musk-promete-carros-tesla-totalmente-autonomos-para-o-final-de-2019-131793>. Acesso em 22 jun. 2019.

GOOGLE. *Nuvem.* Disponível em: < https://tinyurl.com/ya7xxxfv>. Acesso em 13 jul. 2017.

HARARI, Yuval. *Homo Deus: Uma breve história do amanhã*. São Paulo: Companhia das Letras, 2016. Formato: eBook Kindle.

HERZOG, Stephen. *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.* Journal of Strategic Security 4, no. 2 (2011): : 49-60.

HIGA, Paulo. TECNOBLOG. *A geladeira inteligente da Samsung quer centralizar os dados da sua família.* Disponível em <https://tecnoblog.net/190121/samsung-family-hub-refrigerador>. Acesso em 22 jun 2019.

HISTÓRIA DO COMPUTADOR. *ENIAC*. Disponível em <https://grupocdd.wordpress.com/2010/10/14/eniac/>. Acesso em 22 de jul. de 2017.

IG. *Smartband ou Smartwatch? Conheça cada um e saiba qual combina mais com você*. Disponível em <https://tecnologia.ig.com.br/dicas/2018-03-27/smartband-smartwatch.html>. Acesso em 22 jun. 2019.

JESUS, Damásio de; MILAGRE, José Antonio, *Manual de Crimes Informáticos*. São Paulo: Saraiva, 2016.

KAGERMANN, Henning., W. et al. (2013) *Recommendations for implementing the strategic initiative Industrie 4.0: Final report of the Industrie 4.0 Working Group.* Disponível em <https://tinyurl.com/y2qbk4vr>. Acesso em 23 jun. 2019.

KASPERSKY. *Kaspersky Lab detectou mais de 7.000 amostras de malware em dispositivos IoT desde o começo do ano*. 2017. Disponível em <https://tinyurl.com/y5eyrnmt>. Acesso em 22 jun. 2019.

KENIN, Simon. *Mass MikroTik Router Infection – First we cryptojack Brazil, then we take the World?* Disponível em <https://tinyurl.com/y436eyk9>. Acesso em 22 jun. 2019.

KLEINA, Nilton: 2011. TECMUNDO. *Primeiro vírus de computador completa 40 anos.* Disponível em <https://www.tecmundo.com.br/virus/9184-primeiro-virus-de-computador-completa-40-anos.htm>. Acesso em 20 de nov. de 2017.

KOSELLECK, Reinhart. *Futuro passado: contribuição à semântica dos tempos históricos*. Rio de Janeiro: Contraponto: Ed. PUC-Rio, 2006.

KREPINEVICH, Andrew. *Cyber Warfare: A "Nuclear Option*"? 2012. DC: Washington.

LAGNIER, Pablo. *Introdução à História da Comunicação.* Rio de Janeiro: Ed. e-papers, 2009.

LEMOS, Alex. *Cibercultura: tecnologia e vida social na cultura contemporânea*. Porto Alegre: Ed. Editora Sulina, 2002.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 2007.

LIBICKI, Martin C. *Cyberdeterrence and Cyberwar.* Santa Mônica – Califórnia – EUA: Rand Corporation, 2009. Disponível em: <http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>. Acesso em: 17 jun 2019.

LONGO, Waldimir Pirró. O desenvolvimento científico e tecnológico do brasil e suas perspectivas frente aos desafios do mundo moderno. Coleção Brasil: 500 anos, Vol II. Belém: Editora da Universidade da Amazônia. 2000.

LONGO, Waldimir Pirró; MOREIRA; William. *Tecnologia e inovação no setor de defesa: uma perspectiva sistêmica*. Revista Escola de Guerra Naval, Rio de Janeiro, v.19, n. 2, p. 277 - 304, jul./dez. 2013.

LOPES, Nathan: 2019. *Telegram diz que não há evidência de que aplicativo foi hackeado*. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2019/06/11/telegram-celular-moro-mensagens.htm>. Acesso em: 12 jun. 2019.

MARINHA DO BRASIL. *Militares da Marinha concluem o curso de Guerra Cibernética no Exército Brasileiro*. Disponível em <https://tinyurl.com/yy8zgrgj>. Acesso em 29 mai. 2019.

MARINHA DO BRASIL. *Marinha do Brasil participa do 1º Encontro de Especialistas em Defesa Cibernética.* Disponível em <https://tinyurl.com/yyysg6lw>. Acesso em 29 mai. 2019.

MCLUHAN, Marshall: *Os meios de comunicação como extensões do homem*. 1964.

MENDONÇA, Camila; OLIVEIRA, Patrícia; COSTA, Maria. *O conceito de tecnologia na concepção de álvaro vieira pinto: contribuições para a educação a distância*. Colloquium Humanarum, vol. 13, n. Especial, Jul–Dez, 2016, p. 315-320. ISSN: 1809-8207. DOI: 10.5747/ch.2016.v13.nesp.000852

MINISTÉRIO DA DEFESA. *Centro de Análise e Sistemas Navais (CASNAV).* Disponível em <https://tinyurl.com/y3r838qu>. Acesso em 29 mai. 2019.

MILLER, Bill; ROWE, Dale, 2012, October. *A survey SCADA of and critical infrastructure incidents*. In Proceedings of the 1st Annual conference on Research in information technology ACM. Disponível em < https://tinyurl.com/y2t2r7pt>. Acesso em 21 de jun 2019.

NCA: NATIONAL CRIME AGENCY. *International hacker-for-hire jailed for cyber attacks on Liberian telecommunications provider.* 2019. Disponível em < https://tinyurl.com/y5qkh993 >. Acesso em 22 jun. 2019.

NOHE, Patrick: 2018. *What is an Air Gapped Computer?* Disponível em <https://tinyurl.com/y8dgzucx>. Acesso em: 14 jan. 2019.

NORTON. *Glossário. Trojan horse (Cavalo de Troia).* Disponível em <http://br.norton.com/security_response/glossary/define.jsp?letter=t&word=trojan-horse>. Acesso em 23 jun. 2019.

NORTON. *What is cryptojacking? How it works and how to help prevent it*. Disponível em <https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html>. Acesso em 22 jun. 2019.

NORTON. *Norton Cyber Security Insights Report 2016*. Comparação Global. Disponível em <https://tinyurl.com/ycoolxrr>. Acesso em 29 nov. 2018.

OGIE, Robert Ighodaro. *Cyber Security Incidents on Critical Infrastructure and Industrial Networks*. University of Wollongong. 2017. Disponível em <https://tinyurl.com/yyfmgote>. Acesso em 21 de jun 2019.

OLIVEIRA, Marcos; PAGLIARI, Graciela; MARQUES, Adriana; PORTELA, Lucas; FERREIRA NETO, Walfredo. *Guia de Defesa Cibernética na América do Sul*. Recife-PE, Editora UFPE, 2017.

PAGANOTTI, Ivan. *Pressão virtual e regulamentação digital brasileira: análise comparativa entre o Marco Civil da Internet e a Lei Azeredo.* Eptic (UFS), v. 16, p. 139-156, 2014.

PANDA: 2013. *The Most Famous Virus History: Melissa*. Disponível em <https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa>. Acesso em 02 dez. 2017.

PARKS, Raymond C.; DUGGAN, David P. *Principles of cyberwarfare*. IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.

PEREIRA, A. *Navegador Mosaic, 15, desbravou a internet*. In: TecMundo. Disponível em <https://www1.folha.uol.com.br/tec/2008/12/475938-navegador-mosaic-15-desbravou-a-internet.shtml>. Acesso em 14 de jun de 2019.

POLIDO, Fabrício B.P. e ROSINA, Monica S.G, *Governança das Redes e o Marco Civil da Internet: Liberdades, Privacidade e Democracia*. Belo Horizonte: Faculdade de Direito da UFMG, 2015. Disponível em: <http://www.direito.ufmg.br/gnet/ebooks/grmcivil.pdf>. Acesso em 12 jun 2019.

RATTRAY, Greg; EVANS, Chris; HEALEY Jason. *American Security in Cyber Commons*. 2010.

ROBERTSON, Jodan; RILEY, Michael. Bloomberg Businessweek. *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. Disponível em <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>. Acesso em 24 jun. 2019.

ROGERS, Everett M. *Diffusion of Innovations*. 1983.

RUSSIA BEYOND. EGOROV, Boris. *10 monumentos de guerra soviéticos fora da Rússia de cair o queixo*. Disponível em <https://br.rbth.com/estilo-de-vida/79482-10-monumentos-sovieticos-europa>. Acesso em 17 jun. 2019.

RUST, Carlos. Defesanet. 2019. *Ponto de Vista da Segurança Cibernética no Brasil*. Disponível em <http://www.defesanet.com.br/cyberwar/noticia/32534/Carlos-Rust---Ponto-de-Vista-da-Seguranca-Cibernetica-no-Brasil>. Acesso em 14 jun. 2019.

SILVA, Rafael Pinto; ÁVILA, Rafael. *Brasil Informacional: a segurança cibernética como desafio à segurança nacional*. In: XII Encontro Nacional de Pesquisa em Ciência da Informação: Política de Informação para a Sociedade, 2011, Brasília. XII Encontro Nacional de Pesquisa em Ciência da Informação: Política de Informação para a Sociedade. Brasília: Thesaurus, 2011. p. 1514-1530.

SAKOVICH, Natallia. *What Is Internet of Everything (IoE)?* 2019. Disponível em <https://www.sam-solutions.com/blog/what-is-internet-of-everything-ioe>. Acesso em 22 jun 2019.

SANTAELLA, Lucia. *Culturas e artes do pós-humano: da cultura das mídias à cibercultura*. São Paulo: Ed. Paulus, 2004.

SHAH, Saqib. *FDA recalls close to half-a-million pacemakers over hacking fears.* 2017. Disponível em <https://www.engadget.com/2017/08/31/fda-pacemakers-abbott-hacking>. Acesso em 22 jun. 2019.

SHAKARIAN, Paulo. Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008. MILITARY REVIEW. Novembro-Dezembro 2011. Disponível em <https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20111231_art011POR.pdf>. Acesso em 20 jun. 2019.

SILVA, Júlio Cezar Barreto Leite da. *A Guerra no Quinto Domínio, Conceituação e Princípios* Revista Escola Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193 – 211, jan./jun. 2014.

SINGER, Peter W.; FRIEDMAN, Allan. *Cybersecurity: What Everyone Needs to Know.* Oxford University Press, 2014.

SIGNIFICADOS. *Significado de Hacker.* Disponível em: <https://www.significados.com.br/hacker/>. Acesso em: 14 jul. 2018.

TECH TUDO. *Dicionário de tecnologia: entenda o significado dos termos.* <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/04/dicionario-de-tecnologia-entenda-o-significado-dos-termos.html>

THOMPSON, J. *A mídia e a modernidade: uma teoria social da mídia*. Petrópolis: Ed. Vozes, 2002.

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.

VAIDHYANATHAN, Siva. *A Googlelização de Tudo (e por que devemos nos preocupar)*. São Paulo: Cultrix, 2011.

WAKKA. Wagner. *Anonymous hackeia Ministério da Defesa e expõe dados de Villas Boas e Mourão.* Disponível em: <https://canaltech.com.br/hacker/anonymous-hackeia-ministerio-da-defesa-e-expoe-dados-de-villas-boas-e-mourao-123398/>. Acesso em: 11 jul. 2019.
ZETTER, Kim. *Contagem Regressiva até Zero Day.* Brasport, 2017.

ZUCCARO, Paulo Martino. *Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço*. In: BARROS, O. S. R.; GOMES, U. M.; FREITAS, W. L. (org.). Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 49.

ANEXO A

A seguir, estão destacadas todas as menções relacionadas à cibernética que integram a Estratégia Nacional de Defesa. As menções sobre o setor cibernético tangem sobre o fomento de saber e estruturação do setor no Brasil, com fito em parcerias estratégicas e ações necessárias para a autonomia nacional.

1) "Independência nacional alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa, como para o desenvolvimento." (END: 2012, p. 44).

2) "Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear. Esse fortalecimento assegurará o atendimento ao conceito de flexibilidade. Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar". (END: 2012, p. 49).

3) "Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio País não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço". (END: 2012, p. 49).

> 4) Ao lado da destinação constitucional, das atribuições, da cultura, dos costumes e das competências próprias de cada Força e da maneira de sistematizá-las em uma estratégia de defesa integrada, aborda-se o papel de três setores decisivos para a defesa nacional: o espacial, o cibernético e o nuclear. (END: 2012, p. 65).
>
> 5) Para assegurar a tarefa de negação do uso do mar, o Brasil contará com força naval submarina de envergadura, composta de submarinos convencionais e de submarinos de propulsão nuclear. O Brasil manterá e desenvolverá sua capacidade de projetar e de fabricar tanto submarinos de propulsão convencional, como de propulsão nuclear. Acelerará os investimentos e as parcerias necessários para executar o projeto do submarino de propulsão nuclear. Armará os submarinos com mísseis e desenvolverá capacitações para projetá-los e fabricá-los. Cuidará de ganhar autonomia nas tecnologias cibernéticas que guiem os submarinos e seus sistemas de armas, e que lhes possibilitem atuar em rede com as outras forças navais, terrestres e aéreas. (END: 2012, p. 70).
>
> 6) O monitoramento/controle, como componente do imperativo de flexibilidade, exigirá que, entre os recursos espaciais, haja um vetor sob integral domínio nacional, ainda que parceiros estrangeiros participem do seu projeto e da sua implementação,

incluindo: (...) (e) as capacitações e os instrumentos cibernéticos necessários para assegurar comunicações entre os monitores espaciais e aéreos e a força terrestre. (END: 2012, p. 80).

7) 1. Três setores estratégicos – o espacial, o cibernético e o nuclear – são essenciais para a defesa nacional. (...) 3. No setor cibernético, as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades são as seguintes: (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas; (...)
(c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética; (d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual; (e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais; (f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas; (g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e (h) Estruturar a produção de conhecimento oriundo da fonte cibernética. (END: 2012, p. 93, 94).

8) O futuro das capacitações tecnológicas nacionais de defesa depende tanto do desenvolvimento de aparato tecnológico, quanto da formação de recursos humanos. Daí a importância de se desenvolver uma política de formação de cientistas, em ciência aplicada e básica, já abordada no tratamento dos setores espacial, cibernético e nuclear, privilegiando a aproximação da produção científica com as atividades relativas ao desenvolvimento tecnológico da BID. (END: 2012, p. 101).

9) Inteligência de Defesa: aperfeiçoar o Sistema de Inteligência de Defesa. O Sistema deverá receber recursos necessários à formulação de diagnóstico conjuntural dos cenários vigentes em prospectiva político-estratégica, nos campos nacional e internacional. Os recursos humanos serão capacitados em análise e técnicas nos campos científico, tecnológico, cibernético, espacial e nuclear, com ênfase para o monitoramento/controle, à mobilidade estratégica e à capacidade logística. (END: 2012, p. 133, 134).

10) Segurança Nacional: Contribuir para o incremento do nível de Segurança Nacional. Todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase sobre: (...) o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos ministérios da Defesa, das Comunicações e da Ciência, Tecnologia e Inovação, e do Gabinete de Segurança Institucional da Presidência da República; (END: 2012, p. 134, 135).

11) “O Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nas áreas cibernética, espacial e nuclear e o intercâmbio militar com as Forças Armadas das nações

amigas, neste caso particularmente com a América do Sul e países lindeiros ao Atlântico Sul" (END: 2012, p. 136).

> 12) 6. No setor cibernético, o Ministério da Defesa e o Ministério da Ciência Tecnologia e Inovação, por intermédio do Departamento de Ciência e Tecnologia do Exército, promoverão ações que contemplem a multidisciplinaridade e a dualidade das aplicações; o fomento da Base Industrial de Defesa com duplo viés:
> aquisição de conhecimento e geração de empregos; e a proteção das infraestruturas estratégicas, com ênfase para o desenvolvimento de soluções nacionais inovadoras, dentre elas:
>
> • sistema integrado de proteção de ambientes computacionais;
> • simulador de defesa cibernética;
> • ferramentas de conteúdo web;
> • ferramentas de inteligência artificial;
> • algoritmos criptográficos e autenticação próprios;
> • sistema de chaves-públicas da Defesa;
> • sistema de análise de artefatos maliciosos;
> • ferramentas de análise de interesse para o setor cibernético (voz, vídeo, idioma e protocolos);
> • sistema de certificação de Tecnologias da Informação;
> • sistema de apoio à tomada de decisão;
> • sistema de restabelecimento do negócio;
> • sistemas de gestão de riscos;
> • sistema de consciência situacional;
> • computação de alto desempenho;
> • rádio definido por software; e
> • pesquisa científica por meio da Escola Nacional de Defesa Cibernética, de instituições acadêmicas no âmbito do Ministério da Defesa e demais instituições de ensino superior nacionais e internacionais. (END: 2012, p. 142, 143).

A END tem cento e cinquenta e cinco páginas e cita diretamente o setor cibernético usando os seguintes termos: *cibernético, cibernéticos cibernética, cibernéticas.* O total de menções de todas as ocorrências relacionadas ao setor cibernético são trinta no total, o que denota a importância do setor para a implementação da Estratégia Nacional de Defesa.

ANEXO B

Escola de Guerra Naval – Programa de Pós-graduação em Estudos Marítimos

Pesquisa para dissertação de Sara Martins, mestranda.

Título: **"Tecnologia e Inovação na Arte da Guerra: reflexões para a Defesa Cibernética Brasileira a Partir do Estudo de Casos Internacionais"**

Esta pesquisa busca conhecer sua opinião sobre **que reflexões podem ser obtidas para a segurança cibernética brasileira a partir de casos de ataques cibernéticos** de União Soviética (1982), Estônia (2007), Síria (2007), Geórgia (2008) e Irã (2009/10) (sumariados a seguir), **considerando o contexto brasileiro vigente** e tomando como referencial teórico os três tipos de ações cibernéticas que a Doutrina Militar de Defesa Cibernética MD31-M-07 conceitua: a) ataque cibernético; b) proteção cibernética; c) exploração cibernética (o texto com os conceitos e as principais referências desta pesquisa estão depois do questionário).

QUESTIONÁRIO:

1) Quais funções exerceu na área de segurança/defesa cibernética ao longo da carreira? (A resposta não será exposta no texto da dissertação).

2) O ataque sofrido pela União Soviética ocorreu em 1982, quando o uso da Internet ainda não estava difundido. Os soviéticos não detinham o conhecimento tecnológico necessário para construir o gasoduto e tiveram que usar a tecnologia e equipamentos do Canadá. Houve uma sabotagem no sistema SCADA que controlava as válvulas do gasoduto, culminando na maior explosão não nuclear já registrada.

2.1) O desenvolvimento brasileiro em ciência, tecnologia e inovação é capaz de mitigar ataques na cadeia de suprimentos (*supply chain*)?

2.2) A proteção cibernética passa necessariamente pelo desenvolvimento de CT&I em geral?

2.3) Quais ações/políticas capazes de mitigar este tipo de ataque já foram adotadas no Brasil?

2.4) Quais ações/políticas ainda não tomadas poderiam ser implementadas?

3) A Estônia é um dos países mais conectados à Internet no mundo. Tal fato contribuiu para que os serviços básicos do país fossem afetados em 2007 por ataques de negação de serviço DDoS. Durante o ataque, os estonianos ficaram sem acesso aos serviços eletrônicos essenciais como bancos, páginas do governo, serviços de comunicação e de comércio.

3.1) É possível minimizar o risco de o Brasil sofrer esse tipo de ataque?

3.2) Se for possível, de qual(is) forma(s)?

4) Em 2008 a Geórgia sofreu um ataque conjunto: ao território do país e ao ambiente cibernético. Similar ao ataque contra a Estônia, a população ficou sem acesso aos sites de notícias internacionais, houve paralisação dos bancos, sites do governo foram ridicularizados e a Geórgia perdeu o controle de seus domínios ".ge".

4.1) Caso o Brasil sofra um ataque similar contra os sites oficiais do governo, sistema bancário e de comunicação, existe um plano de contingência que seja capaz de evitar que, assim como na Geórgia, a população fique sem acesso às fontes oficiais de informação e aos serviços essenciais?

4.2) Caso o plano não exista, é exequível criar ações nesse sentido? Quais?

5) Em 2007 a Síria sofreu ataque aéreo em uma instalação nuclear por duas brechas nos sistemas: 1) os radares sírios tiveram interferência israelense, para não apontar a ameaça. 2) as informações sobre a construção do reator foram obtidas por uma invasão no computador de um alto funcionário do governo da Síria.

5.1) Os sistemas do governo e seus agentes têm proteção cibernética necessária para evitar ataques via trojan?

5.2) Se não têm, quais seriam as etapas necessárias para assegurar a proteção e detecção de uma possível espionagem?

6) O Irã experimentou os efeitos da chamada "primeira arma cibernética" na destruição de centrífugas nucleares, em 2009/2010. Através de ação feita no mundo virtual, usando o *worm* chamado de *Stuxnet*, foi provado que um código virtual pode causar danos em objetos físicos.

6.1) Que estrutura(s) crítica(s) do Brasil poderiam eventualmente sofrer um ataque similar, com execução no mundo virtual, causando danos físicos significativos?

6.2) Como proteger tais estruturas?

7) Que outras lições envolvendo **ataques cibernéticos** podem ser tiradas dos casos internacionais aqui citados para **proteção cibernética** brasileira no contexto atual?

DEFINIÇÕES:

Conforme a Doutrina Militar de Defesa Cibernética MD31-M-07, a proteção cibernética: "abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente." (BRASIL: 2014, p. 23).

O mesmo documento conceitua **Ataque Cibernético** como "ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente." (BRASIL: 2014, p. 23).

CASOS SELECIONADOS PARA ESTUDO:

Os casos selecionados para o estudo se enquadram no conceito de ataque cibernético: União Soviética (1982), Estônia (2007), Síria (2007), Geórgia (2008) e Irã (2009/10), conforme quadros abaixo:

ATAQUE CONTRA A UNIÃO SOVIÉTICA	
País atacado	União Soviética.
Países atacantes	EUA. (CLARKE; KNAKE: 2015).
Quando foi o ataque	1982.
Tipo de artefato	Tojan.
Alvo	Gasoduto da União Soviética.
Motivação para o ataque	Impedir o avanço tecnológico, econômico (e possivelmente militar) da União Soviética.
Como foi o ataque	Sabotagem no sistema SCADA que controlava as válvulas do gasoduto.
Forma de ação	Bomba-lógica.
Dano causado	Destruição do gasoduto, provocando a maior explosão não nuclear já ocorrida.

ATAQUE CONTRA A ESTÔNIA	
País atacado	Estônia.
Países atacantes	Provavelmente a Rússia. (LIBICKI: 2009; CLARKE; KNAKE: 2015).
Quando foi o ataque	2007.
Tipo de artefato	DDoS (Distributed Denial of Services).
Alvo	Serviços básicos usados pelos estonianos na Internet.
Motivação para o ataque	Retirada da estátua do Soldado de bronze de Tallinn, que homenageava o extinto bloco comunista por sua participação na Segunda Guerra Mundial.
Como foi o ataque	Sobrecarga intencional nos servidores que hospedam as páginas mais usadas na Estônia.
Forma de ação	*Botnets.*
Dano causado	Derrubada de vários serviços básicos como bancos, páginas do governo, serviços de comunicação e de comércio.

ATAQUE CONTRA A SÍRIA	
País atacado	Síria.
Países atacantes	Israel. (CLARKE; KNAKE: 2015; DIPERT: 2013)
Quando foi o ataque	2007.
Tipo de artefato	Bomba lógica.
Alvo	Usina nuclear de Al Kibar.
Motivação para o ataque	Impedir o desenvolvimento tecnológico e militar da Síria, destruindo a possibilidade de um ataque nuclear.
Como foi o ataque	Envio de pulsos eletromagnéticos que transmitiam uma sequência binária específica para controlar os radares da defesa aérea da Síria. Essa ação foi feita com objetivo de apoiar a operação aérea, que promoveu ataque contra a usina nuclear de Al Kibar.
Forma de ação	Ataques eletrônicos.
Dano causado	Destruição da usina nuclear de Al Kibar.

ATAQUE CONTRA A GEÓRGIA	
País atacado	Geórgia.
Países atacantes	Provavelmente a Rússia. (CLARKE; KNAKE: 2015; LIBICKI: 2009; KREPINEVICH: 2012).
Quando foi o ataque	2008.
Tipo de artefato	DDoS (Distributed Denial of Services).
Alvo	Meios de comunicação e sites governamentais georgianos.
Motivação para o ataque	Rebeldes da Ossétia do Sul atacaram as aldeias da Geórgia, com a utilização de mísseis. Em resposta, o exército georgiano bombardeou e invadiu a Ossétia do Sul. O exército da Rússia expulsou os georgianos de Ossétia do Sul. Há a probabilidade de o governo russo ter usado as ações cibernéticas em apoio às ações cinéticas contra a Geórgia.
Como foi o ataque	Negação de serviço em sites do governo georgiano. Posteriormente, os hackers assumiram o controle dos roteadores que suportavam o tráfego para a Geórgia.
Forma de ação	*Botnets.*
Dano causado	Os georgianos perderam acesso às fontes externas de notícias. O envio de e-mails para destinatários fora da Geórgia foi bloqueado. Houve a paralisação dos sistemas de cartões de crédito e operações bancárias. O país perdeu o controle de seus domínios ".ge".

ATAQUE CONTRA O IRÃ	
País atacado	Irã.
Países atacantes	Possivelmente EUA e Israel. (ZETTER: 2017)
Quando foi o ataque	2009/2010.
Tipo de artefato	*Worm.*
Alvo	Centrífugas de enriquecimento de urânio da usina de Natanz.
Motivação para o ataque	Sabotar o desenvolvimento do programa de enriquecimento de urânio do Irã.
Como foi o ataque	Uso de "Zero day" exploits para ganhar o controle de centrífugas de enriquecimento de urânio, aproveitando uma falha desconhecida no sistema SCADA.
Forma de ação	Propagação em rede e através de Pen-drives infectados. Injeção de código malicioso em Controladores Lógicos Programáveis (CLP).
Dano causado	Quase mil centrífugas para enriquecimento de urânio foram quebradas, atrasando o programa nuclear iraniano por vários meses.

ATAQUE CONTRA SETORES PÚBLICO E PRIVADO NORTE-AMERICANOS	
País atacado	Estados Unidos (através de empresas e entidades).
Países atacantes	China. (ROBERTSON; RILEY: 2018).
Quando foi o ataque	2015.
Tipo de artefato	Microchip instalado em placas-mãe de servidores.
Alvo	Empresas e órgãos do governo.
Motivação para o ataque	Espionagem.
Como foi o ataque	Implantação de microchips em placas de servidores com o objetivo de controlar os dispositivos.
Forma de ação	Infiltração na cadeia de suprimentos.
Dano causado	Vazamento de informações.