ESCOLA DE GUERRA NAVAL

CC (T) Maria Rejane Leite do Amaral

O MODELO DE DEFESA CIBERNÉTICA E A PROTEÇÃO DO ESPAÇO CIBERNÉTICO FRENTE A SOFISTICAÇÃO E AO SURGIMENTO DE AMEAÇAS

Rio de Janeiro

2021

CC (T) Maria Rejane Leite do Amaral

O MODELO DE DEFESA CIBERNÉTICA E A PROTEÇÃO DO ESPAÇO CIBERNÉTICO FRENTE A SOFISTICAÇÃO E AO SURGIMENTO DE AMEAÇAS

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

Orientador: Capitão de Fragata Carlos Augusto de Lima

Rio de Janeiro

Escola de Guerra Naval

2021

Dedico este trabalho integralmente ao Senhor Deus que com sua graça e misericórdias permitiu-me concluí-lo. Assim, expresso minha alegria por meio de sua Palavra que diz: “Então a nossa boca se encheu de riso e a nossa língua de cântico; então se dizia entre os gentios: Grandes coisas fez o SENHOR a estes. Grandes coisas fez o SENHOR por nós, pelas quais estamos alegres.” (BÍBLIA, Salmos 126-2:3).

AGRADECIMENTOS

Louvarei ao SENHOR em todo o tempo, porque O busquei e Ele me respondeu e me livrou dos meus temores. Na minha necessidade, clamei ao SENHOR e Ele salvou-me de todas as minhas angústias. Eu vi que o SENHOR é bom e bem-aventurado é aquele que Nele confia (BÍBLIA, Salmos 34).

Também agradeço aos instrutores do Curso Superior 2021, em especial, à equipe da disciplina Metodologia da Pesquisa e ao meu orientador, CF Carlos Lima, pelo apoio incondicional demonstrado ao longo dessa importante e desafiadora jornada de nossa carreira naval.

O entusiasmo, o esforço e a preocupação para que todos os oficiais alunos chegassem juntos ao coroamento do curso — à formatura, eram visíveis.

A esses bravos e incansáveis militares, e a toda tripulação da Escola de Guerra Naval, o meu respeito e admiração. Bravo Zulu!

RESUMO

Esta pesquisa visa analisar o modelo de defesa cibernética e a proteção do espaço cibernético diante da sofisticação e do surgimento de ameaças, propondo o seguinte problema: até que ponto esse modelo fomenta o processo contínuo de fortalecimento e a melhoria das defesas cibernéticas nacionais diante da evolução de novas ameaças? A construção da resposta inicia-se abordando a parte histórica, tal como o nascimento da cibernética e sua associação com o espaço virtual de computadores, discorrendo sobre o uso lícito e ilícito desse novo ambiente. Explica a diferença entre ameaça e vulnerabilidade; mostra os tipos de fontes de ameaças cibernéticas, suas evoluções e seus possíveis impactos. No âmbito do Brasil, o estudo descreve o despertar do país para o setor cibernético e o processo para desenvolver o Modelo de Defesa Cibernética no período de 2005 até 2020. Essa retrospectiva está dividida em três quinquênios: dos esboços; dos resultados e das atualizações e dos exercícios. Também apresenta o *modus operandi* do Modelo de Defesa Cibernética no Brasil e seus principais pontos. Durante o processo de pesquisa documental foi verificado que há um descompasso entre os atos e os fatos, contudo o trabalho das Forças Armadas, em especial do Exército Brasileiro, vem apresentando resultados positivos na busca pelo fortalecimento e pela melhoria do modelo. Este trabalho foi elaborado com base em pesquisa bibliográfica e do arcabouço legislativo brasileiro pertinente, sob uma ótica crítica entre o Modelo de Defesa Cibernética Brasileiro, a defesa cibernética nacional e as evoluções de novas ameaças. Em linhas gerais, a pesquisa conclui que, a despeito da gama documental existente e em vigor, há pontos, apresentados ao longo do capítulo quatro, que, diante da evolução de novas ameaças, enfraquecem tanto o processo contínuo de fortalecimento, quanto a melhoria das defesas cibernéticas nacionais.

Palavras-chave: Ameaças. Cibernética. Defesa Cibernética. Espaço Cibernético. Modelo de Defesa Cibernética. Segurança Cibernética. Vulnerabilidades.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AED	Ações Estratégicas de Defesa
APF	Administração Pública Federal
APT	Advanced Persistent Threat
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
CDCAER	Centro de Defesa Cibernética da Aeronáutica
CDCiber	Centro de Defesa Cibernética do Exército
CDN	Conselho de Defesa Nacional
ComDCiber	Comando de Defesa Cibernética
COVID-19	COrona VÍrus Disease 19 (porque os primeiros casos surgiram no ano de 2019)
CT&I	Ciência, Tecnologia e Inovação
CTIM	Centro de Tecnologia da Informação da Marinha
CTIR Gov	Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo
CTIR.mar	Central de Tratamento de Incidentes em Redes de Computadores da Marinha do Brasil
DDoS	Distributed Denial Of Service
DoS	Denial Of Service
E-Ciber	Estratégia Nacional de Segurança Cibernética
EB	Exército Brasileiro
ED	Estratégias de Defesa
EnaDCiber	Escola Nacional de Defesa Cibernética
END	Estratégia Nacional de Defesa
ETIR	Equipe de Tratamento e Resposta a Incidentes Cibernéticos
EUA	Estados Unidos da América
FA	Forças Armadas
FAB	Força Aérea Brasileira
FS	Forças Singulares
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ITA	Instituto Tecnológico de Aeronáutica
LBDN	Livro Branco de Defesa Nacional
MB	Marinha do Brasil
MD	Ministério da Defesa
NuCDCAER	Núcleo do Centro de Defesa Cibernética da Aeronáutica
OND	Objetivos Nacionais de Defesa
PDN	Política de Defesa Nacional
PND	Política Nacional de Defesa
PNSI	Política Nacional de Segurança da Informação
PR	Presidência da República
RECIM	Rede de Comunicações Integrada da Marinha
SIC	Segurança da Informação e Comunicações
SI	Segurança da Informação
SIMOC	Simulador Nacional de Operações Cibernéticas
SMDC	Sistema Militar de Defesa Cibernética
SWOT	Strengths, Weaknesses,Opportunities e Threats
TI	Tecnologia da Informação
URSS	União das Repúblicas Socialistas Soviéticas

SUMÁRIO

1 INTRODUÇÃO

Se você se conhece e ao inimigo, não precisa temer o resultado de uma centena de combates.
(SUN TZU).

Essa célebre frase, dita há cerca de 2.500 anos pelo filósofo e general chinês *Sun Tzu*, nunca foi tão passível de reflexão como na atualidade. As nações que, ao longo da história, têm continuamente defendido suas terras, mares e céus territoriais, agora se deparam com mais uma dimensão para proteger — o espaço cibernético, um ambiente virtual tão cheio de ameaças quanto o mundo real.

Logo, é primordial que o Brasil, para dominar esse novo espaço, esteja cônscio de quais são as suas próprias forças e fraquezas, de forma a construir um processo contínuo de fortalecimento e melhoria de suas defesas cibernéticas nacionais diante da evolução de novas ameaças.

O ininterrupto crescimento e aperfeiçoamento tecnológico tem possibilitado o acesso a diversos tipos de equipamentos com alto poder computacional e consequentemente a uma variedade de informações, contudo, paralelamente, também tem aumentado a diversidade de incidentes cibernéticos. Essas ameaças, além de serem assimétricas, amplificaram-se e sofisticaram as técnicas de ataques cibernéticos que circulam pela Internet em busca de pontos fracos passíveis de serem explorados.

Observando esse panorama e ciente da importância do espaço cibernético no cenário mundial, o Brasil tem buscado posicionar-se nesse setor, por meio de legislações e doutrinas, dentre outras medidas, para estabelecer conceitos, fundamentos e estratégias, a fim de modelar a sua defesa cibernética no âmbito nacional e internacional.

Assim, esta pesquisa justifica-se porque a cibernética é um assunto amplo, que permeia o comportamento humano, os interesses geopolíticos e a defesa nacional das grandes potências econômicas e bélicas com influência no cenário político internacional. Por esses motivos, a evolução de novas ameaças e o modelo de defesa cibernética brasileiro são pontos focais que motivam o estudo nessa área, a fim de verificar a capacidade protetiva e defensiva do Brasil em relação ao seu espaço cibernético.

Dessa forma, para responder: *até que ponto esse modelo fomenta o processo contínuo de fortalecimento e a melhoria das defesas cibernéticas nacionais diante da evolução de novas ameaças?,* este trabalho apresenta as fontes de ameaças cibernéticas e

quais podem impactar o espaço virtual brasileiro; demonstra o atual modelo de defesa cibernética brasileiro, analisando-o quanto ao processo contínuo de fortalecimento e de melhorias das defesas cibernéticas nacionais.

Para tal, as informações foram obtidas por meio de pesquisa bibliográfica e documental e organizadas de forma descritiva e qualitativa, visando, via método científico hipotético-dedutivo, responder ao problema supracitado por meio da seguinte estrutura: o segundo capítulo apresenta a história da cibernética, do espaço cibernético, identifica fontes de ameaças e suas evoluções e possíveis impactos; o terceiro capítulo demonstra o processo para desenvolver o Modelo de Defesa Cibernética Brasileiro; o quarto capítulo apresenta o modelo de defesa cibernética brasileiro e seus principais pontos e, por fim, o quinto capítulo analisa até que ponto esse modelo fomenta o processo contínuo de fortalecimento e a melhoria das defesas cibernéticas nacionais diante da evolução de novas ameaças, respondendo ao problema proposto.

Esta pesquisa apresenta sugestões para fomentar o processo contínuo de fortalecimento e a melhoria das defesas cibernéticas nacionais, podendo ser objeto de estudo por parte dos órgãos atualmente envolvidos normativamente, bem como poderá ser utilizada em trabalhos futuros.

2 O NASCIMENTO DA CIBERNÉTICA E O ESPAÇO CIBERNÉTICO

Ciberespaço[1]. Uma alucinação consensual experimentada diariamente por bilhões de operadores legítimos, em todas as nações, [...]...Uma representação gráfica dos dados extraídos dos bancos de todos os computadores do sistema humano. Complexidade impensável.
(William Gibson, tradução da autora)

Em sentido amplo, o termo cibernética é originário da palavra grega *kybernetikos* (bom em pilotar), referindo-se à arte do timoneiro – pessoa responsável pelo controle do timão – peça fundamental para direcionar o leme e conduzir a embarcação a uma trajetória segura. Este princípio – do timoneiro governar um navio – fez com que aquela palavra fosse utilizada no campo da ciência política, tanto pelo filósofo e matemático grego Platão

1 O autor de ficção científica da década de 80 William Gibson inventou a palavra ciberespaço, que, até hoje, é muito utilizada entre profissionais e acadêmicos. (OTTIS; PEETER, 2010, tradução da autora).

(428/427–348/347 a.C.), quanto pelo físico francês *André-Marie Ampère* (1775–1836), com o sentido de governar o povo.

Com o passar do tempo a palavra cibernética foi esquecida, ressurgindo com o livro Cibernética: ou controle e comunicação no animal e na máquina, publicado pelo prodigioso matemático norte-americano *Norbert Wiener* em 1948. Pelo título, observa-se que *Wiener* entendeu que cibernética significa controlar.

De fato, a simbiose que os gregos perceberam entre o timoneiro e a embarcação, por meio da comunicação homem-timão para a perfeita condução do barco, fez a cibernética – a arte de governar, de controlar, de conduzir – tornar-se interdisciplinar, sendo atualmente, e acertadamente, aplicada na teoria de controle, de automação e de programas de computadores.

Diferente de seus antecessores, Wiener (2017) coloca a cibernética como uma ciência que norteia a comunicação e o controle na máquina ou no animal. Com esse entendimento, *Wiener* consolida-se como aquele que estabeleceu a ciência da cibernética. Assim, a sua obra *Cybernetics* é considerada um marco para o renascimento da cibernética como ciência.

Tal fato foi consumado com a publicação de outro livro de Norbert *Wiener* chamado *The human use of human beings: cybernetics and society*, onde Wiener (1989) relata sobre a continuidade, pós Segunda Guerra Mundial, de seus estudos no campo da transmissão de mensagens como forma de controle máquina-sociedade e no desenvolvimento de sistemas autômatos. Ele ressalta, novamente, que a única palavra capaz de abranger todo esse complexo processo de comunicação e controle entre humanos e máquinas é a cibernética.

Embora Wiener (2017) tenha cunhado a expressão cibernética como sendo uma ciência para tratar o complexo processo de comunicação e controle, em (WIENER, 1989), ele reconhece que a palavra já havia sido usada por outras pessoas no campo da ciência política, entretanto correlacionou a definição da palavra cibernética com a comunicação e o controle entre máquinas, entre homens e as máquinas e vice-versa.

2.1 Da Cibernética para o Espaço Cibernético

Para lidar com a questão da comunicação e controle por meio da troca de mensagens entre homens e máquinas, Wiener (1989), também, atribuiu à cibernética o propósito de desenvolver linguagens e técnicas.

Essas características começaram a surgir, muito timidamente, na Guerra Fria, que, segundo Mingst e Arrenguín-toft (2014), ocorreu durante o período de 1945–1989, quando as duas potências globais da época — os Estados Unidos da América (EUA) e a, então, União das Repúblicas Socialistas Soviéticas (URSS) começaram uma corrida espacial, conforme registra Calderon (2017).

Os EUA, pressionados pelo lançamento do primeiro satélite soviético *Sputnik* à órbita em 1957, criaram a agência de pesquisa tecnológica *Advanced Research Projects Agency* (ARPA) em 1958, cujo departamento *Information Processing Techniques* era responsável por fomentar pesquisas, com ênfase no meio acadêmico, em computação voltada para a comunicação com o ambiente externo, segundo explica Calderon (2017).

Após onze anos de criação da ARPA, de acordo com Calderon (2017), surgiu, em 1969, o embrião da Internet – a *The Advanced Research Projects Agency Network* (ARPANET) resultado de pesquisas que culminaram na evolução dos computadores e no modo como se comunicavam. Assim, a ARPANET era constituída por computadores interligados por cabos por onde trafegavam as informações.

Dessa forma, ao aplicar a ciência cibernética de *Norbert Wiener* à forma de funcionamento da ARPANET percebe-se que essa composição, capaz de se comunicar entre si, passou a prover um sistema autômato de comunicação, de tal forma que transcendeu o projeto inicial da ARPA, alcançando maior amplitude de uso, ou seja, pode-se inferir que a rede de computadores ARPANET deu início ao espaço cibernético de complexidade impensável, conforme afirma *William Gibson* na epígrafe que inicia este capítulo.

2.2 O uso do espaço cibernético desde a ARPANET

Desde a criação da ARPANET, a tecnologia vem crescendo vertiginosamente, validando a Lei de *Gordon Moore*[2], que, em 1965, já previa a duplicação do poder computacional a cada 18 meses.

A contar dessa lei, poderosos computadores, *smartphones*, Internet das Coisas, inteligência artificial, *wearables*[3], dentre outros tipos de tecnologias, têm surgido e ocupado espaço no dia a dia das pessoas em todo o mundo. Essa popularização tem favorecido a progressiva inclusão de muitos no mundo digital, conforme demonstrado no relatório *Digital*

2 *Gordon Moore* foi um engenheiro estadunidense que ajudou a fundar a empresa Intel, fabricante de processadores para computador. (BRITANNICA, 2021, tradução da autora).
3 Tipo de tecnologia que as pessoas "vestem", tais com relógios inteligentes, roupas, óculos, etc. os quais possuem programas embutidos para os mais variados propósitos que visam o bem-estar de seus usuários.

2020 reports, disponibilizado pelos serviços online (*WE ARE SOCIAL AND HOOTSUITE*, 2020), onde registra que, do total populacional de 7,75 bilhões, atualmente há mais de 4 bilhões de pessoas utilizando a Internet.

Paralelo ao crescimento tecnológico e ao acesso facilitado, também tem sido notado o aumento exponencial de incidentes que podem comprometer a segurança das informações digitais e das comunicações. Segundo o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), das 24.328 notificações reportadas no Brasil, em 2020, 5.565 tratavam-se de incidentes cibernéticos relacionados ou com a segurança dos sistemas de computação ou com as redes de computadores e 2.519 eram vulnerabilidades que permitiam a exploração maliciosa e acessos indesejados ou não autorizados (CTIR GOV, 2020).

Essa estatística é reforçada pelo *Security Report*, da Conteúdo Editorial, onde informa que "O Brasil sofreu mais de 3,4 bilhões de tentativas de ataques cibernéticos de janeiro a setembro, de um total de 20 bilhões em toda a América Latina e Caribe" (CONTEÚDO EDITORIAL, 2020, n.p[4].).

Assim, é inegável que a Tecnologia da Informação (TI) expandiu-se por ter se tornado parte da solução para diversos tipos de negócios, que passaram a utilizá-la, em larga escala, para realizar, de forma rápida, funcional e eficaz, várias tarefas concomitantemente. Entretanto, há situações nas quais a aplicabilidade da TI diverge do objetivo primário para a qual foi desenvolvida, desvirtuando-a para fins criminosos.

Dentre os muitos exemplos de eventos com propósito de exploração maliciosa da TI, pode-se citar a pandemia[5] de COVID-19[6] que, segundo a plataforma *Threat Intelligence Insider Latin America* da Fortinet (2020), ocasionou no aumento da dependência por recursos computacionais e no uso massivo da Internet por parte de diversas empresas, cujos funcionários passaram a exercer suas atividades laborais na modalidade *home office*.

Essa mudança do ambiente de TI, antes controlado pela governança da organização, para outro, cuja segurança das informações digitais e das comunicações não pode ser plenamente garantida, proporcionou a ampliação dos chamados cibercrimes – crimes praticados no ambiente virtual. Várias estratégias de ataques são utilizadas para explorar

4 n.p. significa não paginado.
5 Classificação dada a determinada doença de disseminação entre países. (DICIONÁRIO ONLINE *MICHAELIS* – UOL, 2021).
6 É uma doença causada por um vírus chamado popularmente de coronavírus. (UNA-SUS, 2020)

dispositivos computacionais e ativos de informação[7] de redes com o objetivo de encontrar vulnerabilidades na comunicação *home office* x Organização.

Para tal, técnicas de ataques usando força bruta[8] e *phishing*[9], que transportam vários tipos de programas maliciosos[10], tais como *ransomware*[11], vírus[12], cavalos de Troia[13], são exemplos de ameaças virtuais que se tornaram, de acordo com Fortinet (2020), mais sofisticadas e ampliadas para encontrar pontos fracos entre a Internet e a rede local de computadores das empresas.

2.3 Como identificar quando é ameaça ou vulnerabilidade

Diante dos ataques citados, faz-se importante distinguir ameaça e vulnerabilidade, pois ambas têm aplicações conceituais distintas quando da classificação da ocorrência de possíveis incidentes cibernéticos.

Para Ferreira (2003), vulnerabilidade, que pode ser lógica (hardwares ou softwares) ou física (perímetro físico de uma organização), é a presença de uma fraqueza que poderá ser explorada, por sua vez, ameaça é a probabilidade de explorar determinada vulnerabilidade e se materializa em um agente (atacante), interno ou externo, no espaço cibernético. Singer e Friedman (2017) completam, ainda, que a ameaça poderá ter vários objetivos, por exemplo, econômico, industrial, político, dentre outros.

Ainda que a norma Diretrizes para segurança cibernética (ABNT, 2015) defina ameaça como a causa de um incidente, ela somente poderá causar prejuízos a um sistema, indivíduo ou organização se o binômio vulnerabilidade + ameaça convergirem. Assim, percebe-se que, na verdade, a causa de um incidente cibernético está na vulnerabilidade, uma vez que sua ausência, em princípio, impediria a exploração por parte das ameaças. A raiz do

---

7 De forma geral, consideram-se ativos de informação equipamentos e sistemas com capacidade para armazenar, transmitir e processar informações. (BRASIL, 2019).

8 Consiste em um tipo de ataque onde se tenta “adivinhar”, por tentativa e erro, as credenciais para acessar o alvo. (CERT.br, 2021).

9 Tipo de ataque onde o atacante, para obter informações para as quais não tem acesso autorizado, geralmente, envia e-mails com conteúdo que poderá despertar o interesse do alvo para abri-lo e clicar no link ou no arquivo maliciosos. (CERT.br, 2021).

10 Também chamados de *malwares*, são códigos desenvolvidos por meio de computadores para causar prejuízos ao alvo. (CERT.br, 2021).

11 Tipo de *malware* que criptografa os arquivos existentes no ativo por ele infectado. O atacante exige um pagamento de um resgate para descriptografar as informações. (CERT.br, 2021).

12 É um tipo de *malware* que tem o objetivo de se multiplicar dentro do ativo por meio da autorreprodução. (CERT.br, 2021).

13 É um tipo de *malware* que tem aparência inofensiva, mas que traz dentro de si ações maliciosas. (CERT.br, 2021).

dano é a vulnerabilidade, pois "**uma fonte de ameaça não representa riscos quando não existe vulnerabilidade que possa ser utilizada**" (FERREIRA, 2003, p. 92, grifo da autora).

Tal afirmativa poderia levar a pensar que a solução para mitigar as ameças está em localizar e eliminar as vulnerabilidades, no entanto, de acordo com Singer e Friedman (2017), as características que definem uma ameaça são o agente, o seu objetivo e, em casos de ataques bem-sucedidos, as respectivas consequências. Dessa forma, mapear todas as possíveis vulnerabilidades tornar-se-ia uma tarefa árdua e inócua diante da evolução, do aprimoramento e do surgimento de novas ameaças.

Logo, para reduzir os prejuízos oriundos de um ataque cibernético faz-se necessário primariamente conhecer as fontes de ameaças, a fim de identificar as que possuem maior potencial danoso ao espaço cibernético que se deseja defender. Pondo em outros termos, Singer e Friedman (2017) dizem que conhecer os atacantes, estudar como trabalham e saber quais são os seus propósitos é uma forma de se estimar as ameaças.

Nesse sentido, o Quadro 1 apresenta as potenciais fontes de ameaças organizadas por Ferreira (2003), onde se pode observar, de forma macro, a divisão entre ameaças internas (Funcionários da própria organização — aqueles que não recebem treinamento adequando, negligentes, desonestos, demitidos, entre outros motivos) e externas (Hackers, crackers, Criminosos de computador, Terroristas, Espionagem industrial — companhias, países, dentre outras).

Quadro 1 – Fontes de ameaças

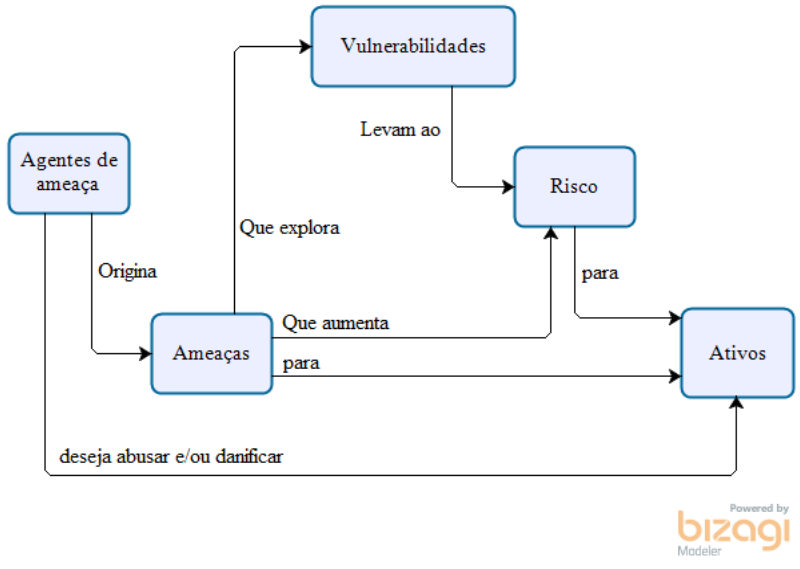
Fontes de Ameaças	Motivação	Ações Utilizadas
Hacker, cracker	– Desafio – Ego – Rebeldia	– Hacking – Engenharia Social – Invasão de sistemas – Acesso não autorizado aos sistemas
Criminoso de computador	– Destruição da informação – Divulgação e alteração não autorizada das informações – Retorno financeiro	– Crime por computador (espionagem) – Atos fraudulentos (interceptação de informações) – Suborno – Invasão de sistemas
Terrorista	– Chantagem – Destruição – Vingança – Exploração	– Bomas / terrorismo – Guerra de informação – Ataque aos sistemas (ex.: ataques DOS)

Espionagem industrial (companhias, países, etc.)	– Vantagem competitiva – Espionagem	– Exploração econômica – Roubo de informações – Engenharia social – Invasão de sistemas – Acesso às informações classificadas
Funcionários da própria organização (aqueles que não recebem treinamento adequando, negligentes, desonestos e demitidos)	– Curiosidade – Ego – Ininteligência – Retorno financeiro – Vingança – Erros não intencionais	– Abuso dos recursos de TI – Roubo e fraude – Inclusão de dados falsos – Interceptação – Inclusão de códigos maliciosos (ex.: vírus, cavalos de troia) – Venda de informações – Falhas nos sistemas – Acesso não autorizado aos sistemas

Fonte: Adaptado de FERREIRA, 2003, p. 93.

Outro ponto a observar é que cada fonte configura-se em um agente de ameaça, ou seja, conforme a (ABNT, 2015) e demonstrado na Figura 1, trata-se de uma pessoa ou grupo que executam ou apoiam um ataque, sendo, portanto, altamente recomendável que as organizações tenham atenção redobrada às ameaças relacionadas as atividades humanas, especialmente as voltadas para atos que vão na contramão da Segurança da Informação e Comunicações (SIC).

Figura 1 - Conceitos e relações de segurança



Fonte: Fragmento adaptado da ISO/IEC 15408-1:1999 (E).

Conforme a Figura 1, a ABNT (2015) informa que as vulnerabilidades, as ameaças, os programas maliciosos e outros não existem de *per si*, antes são obras humanas. Nesse caso, Singer e Friedman (2017) pontuam que é mister reconhecer que o perigo vem das próprias pessoas, sendo que o maior encontra-se na ameaça interna a uma determinada organização, como visto nos casos *Bradley Manning*[14] e *Wikileaks*[15] e do *Edward Snowden*[16].

Há casos em que os atacantes são usuários legítimos dos recursos e serviços oferecidos pela rede local de computadores da instituição e, consequentemente, além de, possivelmente, possuírem as credenciais de acesso aos sistemas, também conhecem como funcionam os processos organizacionais. Isso facilita a construção de estratégias de ataques mais pontuais e assertivas, pois, conforme Mitnick (2003), eles sabem quais são as fraquezas da instituição e a localização de informações importantes. Esses privilégios de comporem o quadro de funcionários e possuírem credenciais dificultam a detecção de atividades maliciosas perpetradas por indivíduos mal-intencionados.

Como visto no Quadro 1, a multiplicidade das ações implementadas pelas fontes de ameaças comprovam o carácter evolutivo quanto a criação de métodos de ataques desenvolvidos para alcançar os mais diversos objetivos, que se aprimoram a cada vez que um método de defesa é implementado. Isso denota a impossibilidade de classificar qual ou quais são as principais fontes de ameaças existentes no espaço cibernético, uma vez que o trinômio ameaça + motivação + ação encontra uma pluralidade de aplicações lançadas diariamente na rede mundial de computadores buscando por vulnerabilidades que possam ser exploradas.

2.4 Ameaças: evoluções e possíveis impactos

É incontestável que o projeto inicial que resultou na ARPANET alçou voos maiores que o inicialmente planejado. A motivação original das pesquisas, realizadas com o objetivo de fazerem as máquinas comunicarem-se, alterou a forma como os dados passaram a ser manipulados pelos computadores.

Esse leque de descobertas e a extensão de possibilidades tecnológicas também estimularam o mau uso desses recursos. Entende-se por “mau uso”, por exemplo, utilizar

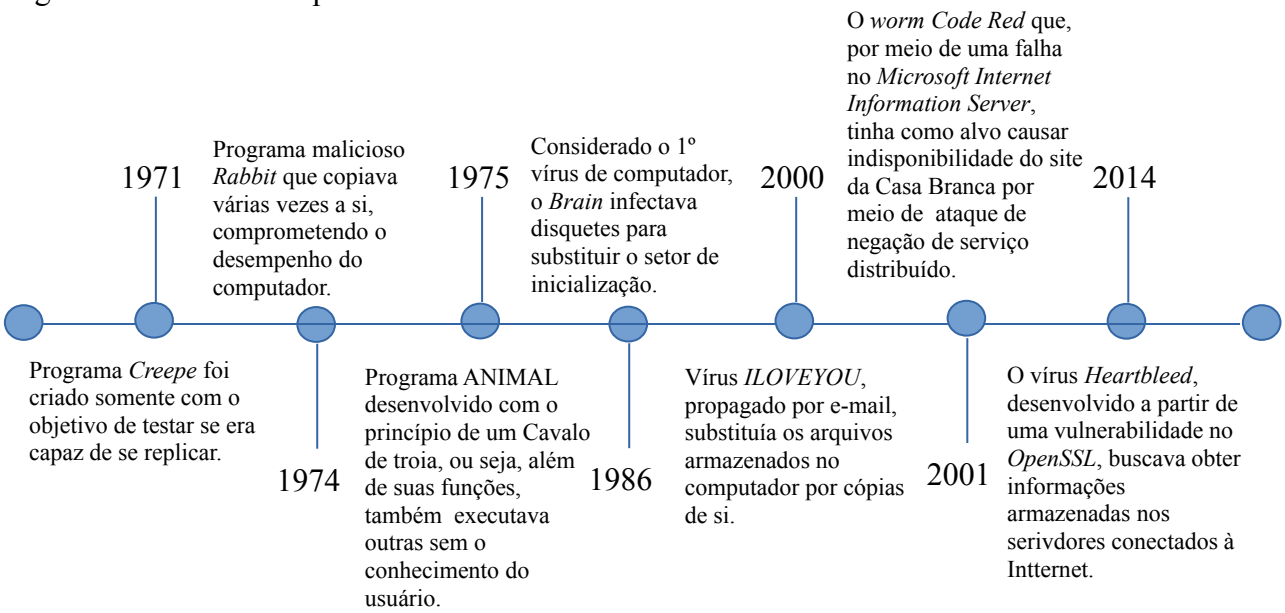
14 Ex-soldado do Exército americano que foi condenado por tornar pública as informações sigilosas daquela Força. (G1, 2013).
15 Organização fundada por *Julian Assange* com o objetivo de divulgar informações sensíveis. (WIKILEAKS, 2015).
16 Profissional de informática estadunidense que trabalhava na Agência Nacional de Segurança daquele país, mas que tornou pública as informações sigilosas da Agência. (THE GUARDIAN, 2013).

linguagens de programação[17] para desenvolver programas com objetivos maliciosos, tais como furtar informações ou causar inoperância de computadores ou, ainda, estudar determinado sistema operacional[18] com o intuito de encontrar brechas passíveis de exploração.

Como exemplo, pode-se citar o artigo *Theory of Self-Reproducing Automata*, publicado pelo matemático americano *John Von Neumann* em 1966, que tratava de um projeto comparativo entre autômatos artificiais (máquinas de computação) e naturais (o sistema nervoso humano), com o intuito era criar um sistema mecânico que, seguindo instruções, seria capaz de se autorreplicar de forma semelhante aos organismos biológicos (VON NEUMANN, 1966).

Seguindo essa mesma lógica, surgiram os vírus de computador. Programas com capacidade de se auto copiarem e se propagarem entre as máquinas. A Figura 2 apresenta uma linha do tempo com os nomes e os propósitos de alguns vírus que surgiram em paralelo ao desenvolvimento computacional.

Figura 2 - Linha do tempo dos *malwares*



Fonte: KASPERSKY, 2021, n.p.

17 São programas desenvolvidos para criar outros sistemas/aplicações por meio de sintaxes, peculiares a cada tipo de linguagem, que automatizarão as instruções que o computador deve entender e processar. Java, C++ e *Python* são exemplos de linguagens de programação. (GOTARDO, 2015).

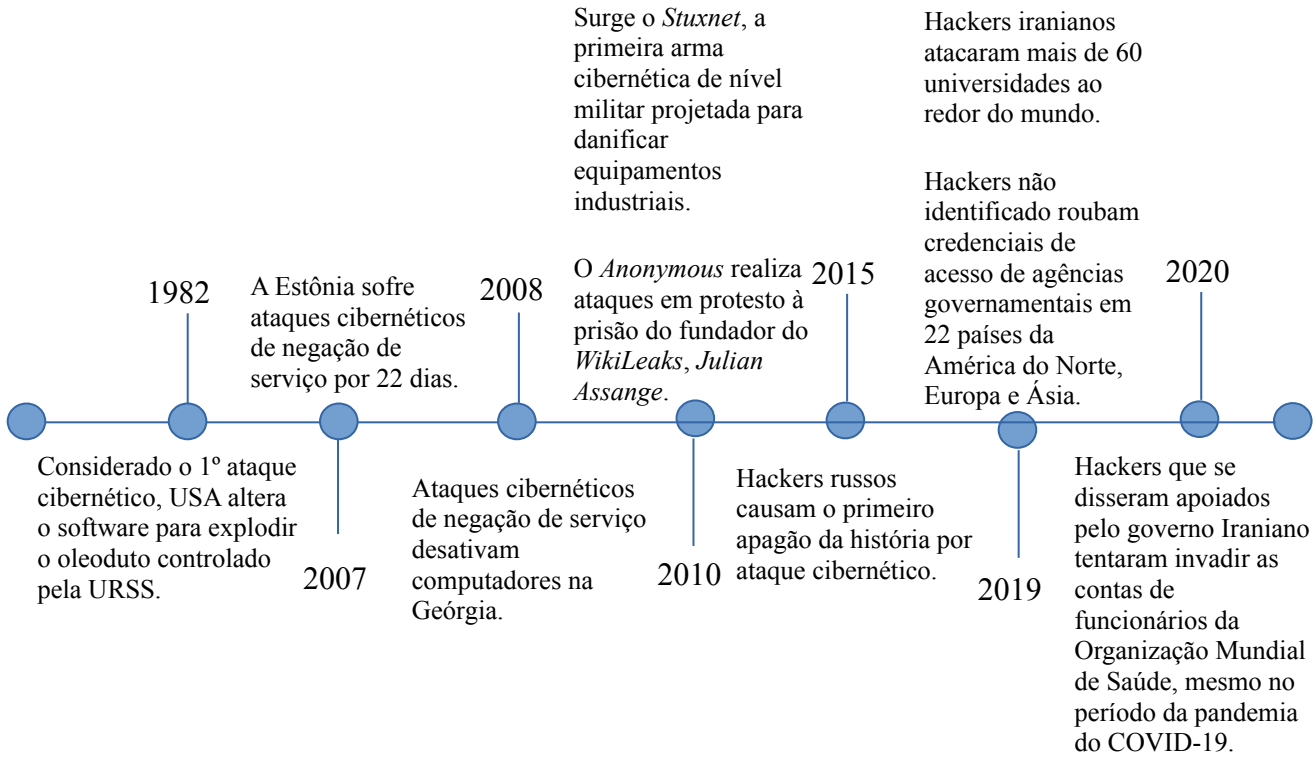
18 Programa desenvolvido para que o computador "entenda" as ações que o usuário está executando e possa responder adequadamente. (SILBERSCHATZ, 2000).

Desse modo, sob um ponto de vista maniqueísta[19], assim como a moeda tem dois lados, a cibernética apresentou seu lado benéfico e maléfico para a sociedade, demonstrados por meio da ocorrência, cada vez mais abundante, de crimes cibernéticos.

Em linhas gerais, Singer e Friedman (2017) afirmam que de um computador é possível furtar dados; utilizar credencias de acesso de terceiros e sequestrar recursos. Esses eventos também podem ocorrer em dispositivos móveis — equipamentos com alto poder computacional, que, devido às facilidades de uso e de mobilidade, têm encontrado cada vez mais maior adesão entre as pessoas.

Conforme apresentado no Quadro 1, essas ações maliciosas, causadas por fontes de ameaças que buscam encontrar vulnerabilidades para alcançar seus objetivos, têm gerado sérios problemas a nível mundial, como se pode constatar na Figura 3, que apresenta uma linha temporal de alguns dos principais ataques cibernéticos ocorridos desde o surgimento da ARPANET.

Figura 3 - Linha do tempo demonstrativa de alguns dos principais ataques cibernéticos



Fonte: COMPUGRAF, 2020, n.p.

19 Entende que somente há dois pontos de vista, por exemplo, ruim e bom, simpatia e antipatia, lado A e lado B. (DICIONÁRIO PRIBERAM DA LÍNGUA PORTUGUESA, 2021).

É inegável que os computadores trouxeram inúmeros benefícios, tais como agilidade e globalização da comunicação. Entretanto, tais vantagens também transformaram essas poderosas ferramentas — o computador e a Internet — em meios utilizados para a prática de crimes cibernéticas no mundo virtual em nível global.

De acordo com o relatório da *MCAFEE LABS* (2020), no segundo trimestre de 2020, surgiram uma média de 419 ameaças, por minuto, ao redor do mundo e a *KASPERSKY* (2020) constatou maior utilização de *trojans*[20] e *backdoors*[21] dentre as milhares de atividades maliciosas. Essas estatísticas, apresentadas pelas maiores provedoras de soluções antimalware, comprovam que os agentes de ameaças estão em contínuo processo evolutivo quanto a criação de técnicas e métodos de ataques cibernéticos.

Cabe ressaltar que as ameaças cibernéticas não se restringem somente as supramencionadas, há as *Advanced Persistent Threat* (APT), ou seja,

> […] "ameaças persistentes avançadas", um fenômeno que ganhou cada vez mais notoriedade em anos recentes […] possuem um nível de planejamento que as separa de outras ciberameaças. São o trabalho de uma equipe, o qual combina organização, inteligência, complexidade e paciência. […] Uma APT começa com um alvo específico [...] Alvos de APTs vão de projetos de jatos militares a segredos comerciais de companhias (SINGER; FRIEDMAN, 2017, p. 70),

bem como aquelas oriundas da aplicação de técnicas de engenharia social, que, por meio de persuasão e manipulação dos sentimentos humanos, tentam identificar e explorar as fraquezas das pessoas, a fim de se obter informações sensíveis.

Como visto, as numerosas atividades mal-intencionadas, que se iniciaram de forma incipiente, experimental e concentrada a uma determinada localidade, evoluíram e se expandiram além fronteiras, causando vários impactos no espaço cibernético e prejuízos em nível geopolítico, tais como o primeiro ataque cibernético dos EUA, que alterou o software para explodir o oleoduto controlado pela antiga URSS, e o roubo de credenciais de acesso de agências governamentais em 22 países da América do Norte, Europa e Ásia.

3 O DESPERTAR DO BRASIL PARA O SETOR CIBERNÉTICO: UMA RETROSPECTIVA DE 2005 A 2020

20 O mesmo que Cavalo de Troia.
21 É um programa malicioso desenvolvido para deixar uma "brecha" no alvo de forma que o atacante pode retornar, várias vezes, ao alvo. (CERT.br, 2021).

Não obstante, é essencial que o Brasil dedique contínua atenção à sua defesa, haja vista a condição sistemática de instabilidade dos relacionamentos entre os países e a emergência de novas ameaças no cenário internacional. (PND, 2020).

Conforme destacado na epígrafe que inicia este capítulo, o Brasil, observando esse panorama, tem buscado posicionar-se no setor cibernético, por meio de legislações e doutrinas, dentre outras medidas, para estabelecer conceitos, fundamentos e estratégias, a fim de modelar a sua defesa cibernética no âmbito nacional e internacional.

Dentre as organizações de pesquisas no ramo anteriormente citadas, adiciona-se o relatório sobre atividade criminosa online no Brasil referente ao 3º trimestre da *AXUR* (2020) que informa sobre a ocorrência de 289,1 milhões de vazamentos de credenciais e a *UNYLEYA* (2020), a qual, também, registrou que o país foi alvo de 15 bilhões de tentativas de ataques em um período de três meses, destacando que técnicas antigas continuam sendo utilizadas e, por vezes, são bem-sucedidas.

A partir desses cenários, infere-se que ou há negligência ou imprudência ou imperícia por parte das empresas e instituições brasileiras no tocante a segurança de suas redes locais de computadores. Além disso, a *UNYLEYA* (2020) apontou os tipos de ataques cibernéticos mais comuns, destacando os *backdoors, phishing, DoS (Denial Of Service)*[22], *DDoS (Distributed Denial Of Service)*[23] e técnicas de engenharia social como, por exemplo, *shoulder surfing*[24].

Essas técnicas potencializam sobremaneira o impacto negativo quando aliadas as ações das APT, de engenharia social e de ameaças internas, prejudicando às atividades legítimas diariamente realizadas por milhares de pessoas e organizações no espaço cibernético.

Observa-se que as estatísticas publicadas por organizações com foco em segurança das informações demonstram a força, a evolução e o rápido crescimento, em nível global, das atividades cibernéticas de cunho ofensivo. Assim, faz-se mister que o Brasil fortaleça o setor cibernético iniciando pelo entendimento de sua importância nacional e internacional e de suas implicâncias geopolíticas, materializado em pessoas capacitadas,

22 Tipo de ataque que tem como objetivo esgotar os recursos computacionais até que o sistema fique inacessível. (CERT.br, 2021).

23 Tipo de ataque distribuído entre vários alvos e tem como objetivo esgotar os recursos computacionais de vários computadores até que os respectivos sistemas fiquem inoperantes. (CERT.br, 2021).

24 Segundo (*LONG,* 2008) surfar sobre os ombros é um ataque antigo e simples, onde o atacante olha por cima do ombro da vítima para tentar visualizar informações que possa está manipulando no dispositivo.

órgãos engajados, recursos orçamentários e contínua atualização do arcabouço documental pertinente ao tema.

3.1 2005 a 2009: o quinquênio dos esboços

Nesse sentido, a partir de 2005 percebe-se maior preocupação do Brasil com o setor cibernético, pois, nesse mesmo ano, entre os documentos de alto nível para o planejamento da defesa nacional[25], o termo "cibernético" aparece no Decreto no 5.484, da Presidência da República (PR), que aprovou a Política de Defesa Nacional (PDN) (BRASIL, 2005). Ainda que tenha tratado de forma genérica a definição de quais tipos de dispositivos seriam considerados ponto focal para a segurança e quais sistemas relacionariam-se com a defesa nacional.

Considerando que a política estabelece "o que" e a estratégia "como", em 2008 foi aprovada, pelo Decreto nº 6.703 da PR, a Estratégia Nacional de Defesa (END) (BRASIL, 2008) que classificou a cibernética como um setor estratégico decisivo para a defesa nacional.

Dada que, pela natureza e pelos fundamentos das Forças Armadas (FA), a defesa do país é atribuição principal das mesmas, o Ministério da Defesa (MD), entendendo a urgência de legislar sobre os três setores estratégicos estabelecidos pela END, definiu em sua Diretriz Ministerial nº 0014 (BRASIL, 2009), dentre outras providências, as responsabilidades das FA e atribuiu o setor cibernético ao Exército Brasileiro (EB), que, segundo (BRASIL, 2009), até aquela data, encontrava-se carente de legislação, sendo necessário criar um centro específico para os militares das três FA trabalharem em conjunto.

Também em 2008, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), em sua Instrução normativa GSI nº 1 (BRASIL, 2008a), sob a ótica da segurança, já começa a fazer menção à cibernética como sendo uma atividade da Gestão de SIC.

Assim, percebe-se que o quinquênio dos esboços foi importante para entender e estruturar os setores decisivos para a defesa nacional, dentre eles, o cibernético, que jamais poderia ser tratado com menor importância, em face da dimensão geopolítica que alcançou e, consequentemente, da necessidade de ser defendido, sendo, portanto, corretamente destinado aos cuidados das FA, especificamente ao EB, da mesma forma que coube à Marinha do Brasil (MB) o setor nuclear e à Força Aérea Brasileira (FAB), o espacial.

---

25 Ações adotadas pelo Estado para defender o país, com participação militar. (BRASIL, 2017).

3.2 2010 a 2014: o quinquênio dos resultados

Com o quinquênio dos esboços começou-se a pavimentar o caminho cibernético a ser trilhado em busca de resultados positivos para o país. Dessa forma, em 2010, por meio do Decreto nº 7.411 (BRASIL, 2010) da PR, o Governo oficializa a inclusão da segurança cibernética à Segurança da Informação (SI), esta já de responsabilidade do GSI/PR.

Ato contínuo à Diretriz Ministerial nº 0014 do MD, o EB ativa, em 2010, o Núcleo do Centro de Defesa Cibernética como o responsável pela implantação do Centro de Defesa Cibernética do Exército (CDCiber), o qual foi adicionado à estrutura regimental do EB em 2012, de acordo com o Decreto Presidencial nº 7.809 (BRASIL, 2012). O CDCiber passa a ser, então, o responsável pelas atividades de defesa cibernética no âmbito do MD.

Considerando as ações empreendidas para impulsionar a cibernética no Brasil, uma concentração de esforços materializou-se na publicação do Livro Verde: Segurança Cibernética no Brasil (BRASIL, 2010a) pelo GSI/PR em 2010, fruto de um amplo debate entre o Governo e a sociedade. O objetivo do livro era delinear diretrizes para elaborar o Livro Branco de Política Nacional de Segurança Cibernética com foco em garantir a preservação dos pilares da SIC[26] – confidencialidade, integridade e disponibilidade da informação no espaço cibernético.

Em 2012, a PDN e a END foram atualizadas, aprovadas e publicadas em um único volume, no qual a PDN passa a ser denominada Política Nacional de Defesa (PND) (BRASIL, 2012a). Em comparação à versão de 2005, destaca-se que a (BRASIL, 2012a), em observância à Diretriz Ministerial nº 0014 do MD, concorda que procedimentos de segurança voltados para a mitigação de vulnerabilidades em sistemas utilizados pelos órgãos devem ser adotados, em vez de "aperfeiçoados" — conforme constava na PDN, a qual pressupunha que tais procedimentos já existiam, e que a informação, a ser protegida de ataques cibernéticos, não se encontra somente em sistemas relacionados à defesa nacional, mas em todos os que são apoiados pela tecnologia da informação e comunicação, que trafegam no espaço cibernético.

A END (BRASIL, 2012b) apresenta maior maturidade quanto ao entendimento do setor cibernético. Dentre as prioridades estabelecidas, destacam-se: fortalecer o CDCiber para transformá-lo em Comando de Defesa Cibernética das FA; criar uma Escola Nacional de Defesa Cibernética (EnaDCiber) e capacitar, preparar e empregar o poder cibernético em operações conjuntas das FA no nível operacional.

26 Além desses três clássicos pilares da segurança das informações, pode-se também incluir autenticidades, responsabilidade, não repúdio e confiabilidade. (ABNT NBR ISO/IEC 27032, 2015).

Também em 2012, em consonância ao Decreto Presidencial nº 7.809, o MD publicou a Portaria nº 3.405 (BRASIL, 2012c) atribuindo a responsabilidade pela defesa cibernética ao CDCiber, conforme relatado em (BRASIL, 2012c citado por JUSBRASIL, 2012), ao tempo em que divulga a Portaria Normativa nº 3.389 (BRASIL, 2012d) aprovando a Política Cibernética de Defesa intitulada MD31-P-02 (1ª Edição/2012), segundo (BRASIL, 2012d citado por DEFESANET, 2012).

Em consonância com a PND e a END, destaca-se que a Política Cibernética de Defesa apresenta-se com a finalidade de nortear tanto a defesa quanto a guerra cibernética no âmbito militar de poder nacional, extensivos aos órgãos interessados em participar de tais ações. Alerta, ainda, que é condição *sine qua non* a colaboração de setores da sociedade para alcançar seu propósito e que a eficácia da defesa dependerá do nível de maturidade quanto ao valor da informação, pois entende que a defesa cibernética está para garantir a SIC.

Ainda em 2012, seguindo a linha de raciocínio apresentada no Livro Verde, foi aprovado o Livro Branco, não de Política Nacional de Segurança Cibernética, mas de Defesa Nacional (LBDN) (BRASIL, 2012e). Entregue pelo MD, o LBDN é, segundo (DEFESANET, 2013), uma espécie de enciclopédia para a defesa nacional que atende a demanda internacional, pois os países registram nesse tipo de publicação as suas visões e estratégias no campo da defesa, sendo, portanto, importante para solidificar a confiança entre as nações e elevar o nível de segurança do país.

Em linhas gerais, o (BRASIL, 2012e) apresenta a importância de envidar esforços para defender o setor cibernético, em virtude, dentre outros aspectos, do seu carácter multidisciplinar, por interagir com diferentes organizações e por ser fonte dos mais diversos tipos de dados, sendo, portanto, fundamental garantir os fundamentos de SIC, acima mencionados. Reforça sobre o fortalecimento do CDCiber com recursos humanos capacitados, equipamentos e *softwares* capazes de responder aos diferentes tipos de ameaças cibernéticas, bem como estipula prazo e destina recursos financeiros para o projeto Defesa cibernética, definido pelo EB como prioritário.

Em 2014, o MD publica a Doutrina Militar de Defesa Cibernética (BRASIL, 2014) com o objetivo de fixar fundamentos, unificar o entendimento sobre o assunto na esfera do MD e contribuir para o preparo das FA na defesa do país quando atuando no espaço cibernético.

A Doutrina Militar de Defesa Cibernética reconhece que a defesa cibernética é essencial para a proteção dos ativos de informação, ao considerar a volatilidade e a mutabilidade das ameaças externas e a possibilidade de aumento de ataques perpetrados por atores externos, por exemplo, os Estados.

Assim, no quinquênio dos resultados observa-se um amadurecimento e melhor entendimento conceitual do que é a cibernética para o Brasil. Esse quinquênio foi marcado pela quantidade de normas regulamentares e pela definição e segmentação de responsabilidades quanto ao setor cibernético, ou seja, a defesa foi delegada para o CDCiber e a segurança para o GSI/PR.

Essa importância também pode ser notada com a aprovação da Política Cibernética de Defesa e da Doutrina Militar de Defesa Cibernética, pilares que apoiarão a segurança e a defesa dos ativos de informação no espaço cibernético e promoverão a conscientização das pessoas da Administração Pública Federal (APF) e demais instituições.

3.2.1 A concretização dos resultados

Até aqui muito se fez pela consolidação de um arcabouço documental capaz de informar quais são as diretrizes do Governo e o que este espera dos órgãos que compõem a APF, bem como da sociedade quanto a condução do setor cibernético brasileiro.

Desde a Diretriz Ministerial nº 0014 do MD, muitos foram os sucessos alcançados pelo EB no tocante ao desenvolvimento de um modelo de defesa cibernética. Além das normas apresentadas, o EB efetivamente estruturou o CDCiber, conforme estabelecido no Decreto nº 8.491 da PR (BRASIL, 2015a), que, de acordo com a Doutrina Militar de Defesa Cibernética, foi classificado, enquanto órgão central do Sistema Militar de Defesa Cibernética (SMDC), como elemento do nível decisório estratégico, integrando o setor cibernético nas FA e mantendo a comunicação com seus órgãos de inteligência e entidades envolvidas com a defesa cibernética.

Em 2013, em cumprimento à ação estratégica Ciência, Tecnologia e Inovação (CT&I) da (BRASIL, 2012b), o EB apresentou o

> […] Simulador Nacional de Operações Cibernéticas (SIMOC) – software que cria e planeja treinamentos em um ambiente de rede. A ferramenta está inserida nos pilares da Estratégia Nacional de Defesa no que diz respeito ao desenvolvimento de equipamentos e plataformas de defesa cibernética. (BRASIL, 2013, n.p.)

e o MD emitiu a Portaria Normativa nº 2.777 (BRASIL, 2014a) com diretrizes para potencializar a defesa cibernética nacional, dentre as quais se encontravam a criação tanto do Comando de Defesa Cibernética (ComDCiber), ativado em 2016, com a responsabilidade, segundo (BRASIL, 2020b), de planejar e coordenar as atividades no SMDC; quanto da ENaDCiber, ativada em 2019, para capacitar os recursos humanos na área de defesa cibernética, em cumprimento à END, ambos sob o Comando do EB. Com a ativação do ComDCiber, o CDCiber passou a ser subordinada àquele Comando.

Toda essa diligência do EB foi posta à prova em grandes eventos. O primeiro deles foi a Conferência das Nações Unidas sobre Desenvolvimento Sustentável, que ocorreu em 2012 no Rio de Janeiro, quando o CDCiber monitorou toda a rede de computadores do evento, conforme anunciado pelo EB em (BRASIL, 2012f). Em 2013, ocorreram a Copa das Confederações e a Jornada Mundial da Juventude, cabendo ao MD prover segurança e defesa cibernética, segundo o MD em (BRASIL, 2013). Em (BRASIL, 2014b) foi a vez da Copa do Mundo, em que o CDCiber apoiou no fortalecimento da segurança; na proteção contra ataques cibernéticos; na resposta aos possíveis incidentes na rede de computadores e na proteção das infraestruturas consideradas estratégicas, tais como água e energia elétrica, conforme estabelecido na END.

3.3 2015 a 2020: o quinquênio das atualizações e dos exercícios

Após, aproximadamente, uma década de esforços empreendidos e lições aprendidas no setor cibernético, chega o momento de atualizar as normas regulatórias e buscar formas de manter o aprendizado até então conquistados.

Assim, em decorrência da Instrução Normativa GSI/PR nº 01/2008, o Conselho de Defesa Nacional[27] publicou, em 2015, a Portaria CDN nº 14 (BRASIL, 2015b) que trata da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF, delineando objetivos e metas estratégicos para o fortalecimento nessas áreas.

Passados oito anos desde a última revisão da PND, da END e do LBDN em 2012, o MD encaminhou novas versões para aprovação do Congresso Nacional em 2020, contudo, segundo a Lei complementar nº 136 (BRASIL, 2010b) da PR, esse conjunto de normas deveria ser encaminhado para o Congresso Nacional a cada quadriênio.

27 Órgão que assessora o PR em assuntos de soberania e de defesa nacional. (CF, art. 91).

Ao estabelecer um mapa comparativo sobre a evolução da unidade do pensamento e do nível de maturidade alcançados pela APF, desde 2005, para desenvolver um modelo de segurança e de defesa cibernéticas, percebe-se que a PND 2020 (BRASIL, 2020) somente contextualiza a segurança e a defesa do espaço cibernético no âmbito nacional, apesar de reconhecer a inconstância e o advento de novas ameaças no cenário internacional.

Quanto à END 2020 (BRASIL, 2020a), observa-se maior especificidade das Estratégias de Defesa (ED), que, por sua vez, têm Ações Estratégicas de Defesa (AED), que terão os Objetivos Nacionais de Defesa (OND). Nesta lógica, a ED, reconhecendo a capacidade dissuasória do setor cibernético, autoriza a ampliação das habilidades de defesa e de exploração do espaço cibernético, já fazendo uma notória menção as ações cibernéticas: atacar, proteger e explorar apresentadas em (BRASIL, 2014).

O LBDN 2020 (BRASIL, 2020b) apresenta a preocupação com a possibilidade de possíveis guerras cibernéticas serem um desafio para a defesa nacional e segurança internacional, em virtude da dificuldade de se identificar a autoria dos ataques dessa natureza e dos prejuízos que podem causar. Reconhece, ainda, o êxito alcançado pelo EB quanto a qualificação de pessoal especializado e a implementação de soluções tecnológicas de qualidade e, por fim, em atendimento a END 2020, apresenta a defesa cibernética como um projeto estratégico do EB como capacidade transformacional, sendo o Sistema de Proteção Cibernética selecionado como prioritário para transformar a Força Terrestre.

O SMDC, mencionado na Política Cibernética de Defesa e na END 2020, foi materializado pela Portaria nº 3.781 (BRASIL, 2020c) do MD, que o apresenta com um conglomerado dotado de pessoas, normas, equipamentos, acomodações, dentre outros. O SMDC deve ser utilizado, no contexto da defesa nacional, para garantir o efetivo uso do espaço cibernético pelas FA, bem com impedir ou dificultar seu uso malicioso. Com a criação do SMDC, o ComDCiber passa a ser o seu órgão central, em lugar do CDCiber.

Diante de todas essas ações e busca por manter o alinhamento com a PND, a END e o LBDN quanto ao fortalecimento e ao envolvimento da sociedade nos assuntos pertencentes à defesa nacional, conforme expresso na Política Cibernética de Defesa, e para elevar o grau de conscientização sobre a importância do setor cibernético para a defesa do país, o EB tem promovido exercícios chamados de Guardião Cibernético.

Esse exercício Cibernético envolve a participação de vários segmentos da sociedade civil e militar, incluindo órgãos de infraestruturas nacionais consideras críticas,

para, em conjunto, realizarem treinamentos de ações de proteção cibernética contra problemas cibernéticos simulados pelo SIMOC. A primeira versão desse exercício ocorreu em 2018 e a segunda em 2019. Em 2021, de acordo com (DEFESANET, 2018, 2019, 2021), foi aberto um edital de chamamento público para a terceira versão desse exercício.

Esse tipo de iniciativa tem se mostrado de grande relevância para apresentar aos participantes os tipos de vulnerabilidades existentes em *softwares* e *hardwares*, as variedades de ameaças que podem explorar tais fraquezas e as ações que podem ser adotadas no sentido de defender e proteger aquele espaço cibernético simulado dos ataques maliciosos.

3.4 Enquanto a defesa galopa, a segurança coxeia[28]

No tocante à defesa cibernética, percebe-se que, desde a Diretriz Ministerial nº 0014 do MD, este segmento, sob o comando do EB, apresentou relevantes e rápidos resultados.

Por outro lado, no que se refere à segurança cibernética, atribuída ao GSI/PR pelo Decreto nº 7.411 da PR, observa-se uma lentidão quanto a tomada de ações efetivas para a promoção da segurança cibernética como atividade da gestão de SIC.

Os passos em direção a segurança cibernética nacional ainda estão no campo documental, dentre os quais, destacam-se o Livro Verde Segurança Cibernética no Brasil, em 2010, e a Política Nacional de Segurança da Informação (PNSI), pelo Decreto nº 9.637 (BRASIL, 2018). Este Decreto ratifica a Instrução normativa GSI nº 1/2008, acrescentando que a defesa cibernética também está contida na SI, conforme previsto na Política Cibernética de Defesa.

Entre seus instrumentos, a Política Nacional de Segurança da Informação apresenta a Estratégia Nacional de Segurança da Informação a ser elaborada em módulos, dentre os quais estarão os de segurança e de defesa cibernética, bem como registra que cabe ao MD apoiar o GSI/PR nos assuntos atinentes à segurança cibernética, algo, também, previsto na Política Cibernética de Defesa.

Contudo, foi em 2020 que o GSI/PR resolveu atualizar suas normas, iniciando pela antiga Instrução Normativa nº 1 de 2008. Diferente de sua primeira versão que mencionava a cibernética circunstancialmente, destaca-se que a Instrução normativa nº 1 GSI (BRASIL, 2020d) exorta aos órgãos da APF a observarem algumas legislações, dentre elas, o

28 Neste contexto, coxeia significa segue com dificuldade. (DICIONÁRIO ONLINE MICHAELIS – UOL, 2021, n.p.).

Decreto nº 10.222 (BRASIL, 2020e), que trata sobre a Estratégia Nacional de Segurança Cibernética; obriga aos órgãos a criarem as Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), sob a tutela do CTIR Gov e cria a função de gestor de SI, a ser designado dentro de cada órgão, para, dentre outras atribuições, supervisionar as atividades da ETIR.

No tocante às ETIR, a (BRASIL, 2020d) apresentou um ponto interessante. Considerando o conceito de dividir para conquistar, ela encoraja a participação de diversos setores do Estado brasileiro no processo de defesa nacional. Assim, cada órgão que pertence à APF deve ter uma ETIR e um gestor de SI com o fito de promover a segurança cibernética localmente.

Entretanto, o GSI/PR percebeu que somente tratar e responder significava uma ação reativa a algum incidente cibernético já ocorrido, ou seja, as ETIR de cada órgão trabalhariam reativamente em invés de proativamente. Para garantir efetivamente a segurança cibernética na APF não bastava distribuir vários pontos de apoio ao CTIR Gov, espelhando o mesmo trabalho. Se o objetivo era colaborar para a segurança cibernética em nível nacional, as ETIR deveriam realizar primariamente ações preventivas em suas infraestruturas de rede local de computadores.

Como esse intuito, o GSI/PR retifica a Instrução normativa nº 1 GSI/2020 por meio da Instrução Normativa nº 2 GSI (BRASIL, 2020f), adicionando a palavra “prevenção” à nomenclatura ETIR, que passa de Equipe de Tratamento e Resposta a Incidentes Cibernéticos para Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, em sintonia com a PNSI.

Ainda em 2020, é publicada a Estratégia Nacional de Segurança Cibernética (BRASIL, 2020e) aprovando o primeiro módulo da Estratégia Nacional de Segurança da Informação chamado de E-Ciber. Com validade até 2023, a E-Ciber apresenta ações e objetivos estratégicos, no âmbito nacional e internacional, os quais devem ser observados tanto pelos órgãos da APF, quanto pela sociedade brasileira.

Diante do exposto, observa-se que, embora a APF tenha decidido dividir a cibernética em dois segmentos – segurança e defesa – e delegado as respectivas competências a órgãos diferentes, os documentos normativos apresentados tratam do espaço cibernético tanto sob a ótica da defesa, quanto da segurança porque ambas têm como alvo proteger sistemas, informações, infraestruturas e tudo o mais que influenciar na defesa nacional.

Logo, apesar da defesa encontrar-se sob a competência militar e a segurança sob a civil; de a defesa ser um conjunto de ações temporárias em níveis estratégico, operacional e tático e da segurança ser um conjunto de atividades contínuas e permanentes, ambas estão interligadas e são profundamente correlatas pelo fato da defesa está contida na segurança. Assim, ainda que, por questões normativas, a segurança e a defesa estejam sob égides diferentes, seus órgãos responsáveis devem trabalhar em uníssono para evitar que uma se sobressaia a outra, o que resultaria em fraquezas tanto na segurança, quanto na defesa do setor cibernético brasileiro.

4 O *MODUS OPERANDI* DO MODELO DE DEFESA CIBERNÉTICA BRASILEIRO

> *[...] requerem especial atenção a segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional.*
> *(PND, 2020).*

O capítulo anterior apresentou o longo caminho percorrido pelo Governo-Estado para desenvolver a construção de um modelo de defesa cibernética brasileiro. A retrospectiva apresentada demonstrou que o intenso trabalho iniciado com esboços, seguido de resultados iniciais, atualizações e exercícios apresentou progressos, delineou o modelo e definiu as responsabilidades de atuação nos campos da segurança e da defesa cibernéticas do país.

O EB, principal ator do setor cibernético, desde que recebeu a missão, tem alcançado, conforme relatado, grandes conquistas no transcorrer do processo para estruturar e consolidar o modelo de defesa cibernética no Brasil, culminando na criação do SMDC, um sistema completo que engloba, dentre outros aspectos, o doutrinamento, as instalações físicas, o pessoal e os equipamentos.

A aprovação da Política Nacional de Defesa, da Estratégia Nacional de Defesa, do Livro Branco de Defesa Nacional, da Política Cibernética de Defesa e da Doutrina Militar de Defesa Cibernética são alguns exemplos da direção a ser seguida. Esses são documentos basilares para nortear os segmentos da sociedade quanto a postura a ser adotada tanto no caminho para a defesa, quanto para a segurança do espaço cibernético brasileiro.

Quanto as instalações físicas, em atendimento a END de 2012, o EB concretizou com a criação e proveu os insumos necessários para o adequado funcionamento do Comando

de Defesa Cibernética, o qual foi mencionado no Livro Branco de Defesa Nacional 2020 como um suporte positivo aos órgão da APF no que diz respeito ao gerenciamento das atividades de defesa do Setor Cibernético. O CDCiber, capacitado com um Centro de Operações, é qualificado para monitorar as atividades de defesa cibernética e passou a ser o braço operacional do ComDCiber, adicionado à ENaDCiber responsável pela capacitação em cibernética.

Referente ao pessoal, em consonância com a END de 2012, o EB tem estabelecido parcerias, dentro e fora do país, para promover a qualificação de militares e civis, dente elas, com Israel, com a Organização dos Estados Americanos, com o Instituto Tecnológico de Aeronáutica (ITA), além da própria ENaDCiber. O ComDCiber também provê anualmente o curso de Guerra Cibernética, que compõe o programa de capacitação em cibernética dos militares das FA.

No que diz respeito aos equipamentos, tecnologias e serviços, o EB, em atenção a ação estratégica CT&I da END de 2012, adquiriu o SIMOC, contribuindo também para a emancipação da base industrial de defesa. O SIMOC tem sido utilizado nos exercícios Guardião Cibernético que visam preparar vários setores da sociedade em treinamentos voltados para a defesa cibernética por meio de ações ofensivas, defensivas e exploratórias realizadas em um ambiente virtual simulado.

4.1 Da segurança para a defesa: um modelo de quando agir

A Doutrina Militar de Defesa Cibernética classifica em níveis a decisão de quando iniciar, no espaço cibernético, as atividades e as ações cibernéticas, quais sejam, estratégico, operacional e tático.

Assim, tendo em vista que a segurança cibernética é uma atividade que deve ocorrer rotineiramente para garantir a proteção da informação, dos ativos e das infraestruturas críticas que utilizam o espaço cibernético e que a PNSI a coloca como um elemento da SI, as atuações relacionadas a esta área encontram-se no nível político.

Quanto à defesa cibernética, descrita pela (BRASIL, 2014) como ações ofensivas, defensivas e exploratórias executadas no espaço cibernético, a decisão de iniciá-la encontra-se no nível estratégico sob o comando do MD e das FA. Percebe-se que as ações de defesa cibernética serão empreendidas em operações ou em casos de eventos reais que possam

comprometer a proteção dos sistemas de informação de interesse da defesa nacional no espaço cibernético.

Dependendo da intensidade das ameaças cibernéticas, essas ações poderão ensejar em uma guerra cibernética nos níveis operacional e tático, de âmbito restrito às FA. Essas intensidades são medidas pelo nível de alerta cibernético que é uma "[…] classificação dada ao estado em que se encontra o Espaço Cibernético de interesse do MD e das FA, no tocante à possibilidade de concretização de ameaças cibernéticas.", de acordo com (BRASIL, 2014, p. 26).

Apesar de restrita ao âmbito do MD, a ideia do alerta cibernético é muito interessante, pois permite, por meio de monitoramento ininterrupto, saber ou identificar em qual risco cibernético[29] encontra-se o espaço cibernético. Assim, ações de defesa cibernética poderão ser autorizadas, dependendo do nível e dos tipos de ameaças, para proteger os sistemas de informação de interesse da Defesa Nacional (BRASIL, 2014).

Em face do apresentado, percebe-se que a defesa cibernética Brasileira vigente apresenta elementos e ferramentas com condições para gerenciar e mitigar as ameaças cibernéticas atualmente existentes no espaço cibernético. Além disso, as estratégias, até o momento, estruturadas para a executá-la apresentam-se bem organizadas, contendo princípios, características, possibilidades, planejamento, objetivos, meios disponíveis, limites e situações de ação importantes para evitar dúvidas sobre as competências, a sua aplicabilidade e os campos de atuação quando se fizerem necessárias.

4.2 Defesa x preparo: um modelo de quando os atos não correspondem aos fatos

Conforme a PND e a END, para que os objetivos do setor cibernético sejam alcançados faz-se necessária a interoperabilidade entre órgãos militares e civis. Assim, de acordo com a Doutrina Militar de Defesa Cibernética, a forma de atuação cibernética com maior probabilidade de emprego será por meio de operações em ambiente interagências[30] com coordenação nos níveis estratégico, operacional e tático, sendo necessário, portanto, empregar um Destacamento[31] Conjunto de Defesa Cibernética para atuar em nível estratégico.

---

29 A probabilidade de um incidente cibernético ocorrer e o grau do prejuízo que causará. (BRASIL, 2014).

30 Intercâmbio e colaboração entre instituições governamentais e não governamentais, nacionais e/ ou internacionais. (BRASIL, 2017).

31 Grupo de militares designados para execução de uma tarefa específica e temporária. (BRASIL, 2017).

Essa visão interoperável para promover a defesa do setor cibernético se dá pela consolidação do entendimento de que o Estado, em conjunto com as ações das agências[32], apresenta-se com uma das medidas protetivas contra ameaças, como uma resposta aos ataques, bem como um meio para gerenciar crises (BRASIL, 2017).

Contudo, muitos ataques cibernéticos vêm ocorrendo em grande quantidade, alta velocidade e complexidade, cujos alvos são tanto os órgãos privados, quanto públicos. Assim, tomando como base as características da defesa acima citadas, percebe-se que os atos não correspondem aos fatos quando se trata de agilidade na implementação tempestiva de medidas proativas em resposta as atividades maliciosas hostis previamente monitoradas. Essa demora foi observada em 2020, quando vários eventos cibernéticos hostis foram perpetrados contra diversos órgãos da APF.

Segundo VEJA (2020), a Receita Federal, o Superior Tribunal de Justiça, o Ministério da Saúde e o Distrito Federal foram alvos de ataques cibernéticos que resultaram em inoperância de seus sistemas. Também foram atacados ciberneticamente o Conselho Nacional de Justiça e a Controladoria-Geral da União, bem como órgãos públicos de alguns Estados brasileiros, tais como, a Prefeitura de Vitória, o Tribunal de Justiça de Santa Catarina, o Tribunal de Justiça de Pernambuco e o Tribunal de Justiça Militar do Estado de São Paulo.

O próprio EB foi alvo de hackers, conforme divulgado em G1 (2015), que divulgaram os números de CPF de centenas de militares em fóruns hackers na Internet. A CNN BRASIL (2020) também informou sobre a divulgação de supostos exames do Presidente da República por hackers que obtiveram acesso não autorizado ao site do Hospital das Forças Armadas.

Assim, diante da quantidade e dos tipos de ataques orquestrados de uma só vez aos mais diversos órgãos, constata-se que houve um planejamento, por parte dos atacantes, de quando, onde e como desferir tais ataques, denunciando, consequentemente, a ausência ou deficiência no monitoramento, que se adequadamente realizado e interpretado resultaria em ações preventivas de resposta àquelas ameaças insurgentes. O êxito dos ataques demonstrou que o amplo arcabouço documental, apresentado ao longo desta pesquisa, ou é de difícil implementação ou não está sendo observado.

Os ataques citados não foram os primeiros e nem serão os últimos. Tais casos, adicionados aos do *Edward Snowden*, envolvendo espionagem cibernética, ocorrido em 2013,

32 São instituições legalmente reconhecidas, com competências definidas, públicas ou privadas, nacionais ou internacionais, civis ou militares. (BRASIL, 2017).

as invasões aos celulares de autoridades como os presidentes da Câmara e do Senado, do ministro do Superior Tribunal de Justiça, da Procuradora-Geral da República, como relatado em G1 (2019) e do ex-Ministro da Justiça Sergio Moro, também em 2019, têm mostrado inobservância das normas regulamentares expedidas pelo GSI/PR; falhas na gestão contínua das atividades de segurança, nas ações de defesa do espaço cibernético de interesse, nos treinamentos contínuos entre as interagências, bem como em suas capacidades de atuarem colaborativamente, preventivamente e tempestivamente.

4.3 Órgãos de defesa cibernética das Forças Singulares: um modelo de atuação colaborativa

Em apoio às amplas, notórias e efetivas realizações do EB em relação a construção do modelo de defesa do setor cibernético brasileiro; a contribuição para a segurança Cibernética[33] dos ativos de informação da APF e sendo o SMDC, também, composto pelas estruturas de Defesa Cibernética das Forças Singulares (FS), segundo (BRASIL, 2020c), essas FS têm envidado esforços para agirem como órgãos de Defesa Cibernética das FA.

Nesse sentido, a FAB, além de possuir uma ETIR, conforme consta na Portaria nº 3.781/2020, também, segundo (DEFESANET, 2020), implantou, em 2020, um Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER) e, em 2023, ativará o Centro de Defesa Cibernética da Aeronáutica (CDCAER) com o objetivo de amplificar a atuação qualificada para prover segurança ao setor espacial atribuído àquela FS.

Da mesma forma, de acordo com as Normas de Tecnologia da Informação da Marinha (BRASIL, 2019), a MB, por meio de sua diretoria especializada – a Diretoria de Comunicações e Tecnologia da Informação da Marinha, doutrina e normatiza a área de defesa cibernética no âmbito da MB, cujas atividades são gerenciadas e executadas por seu órgão operacional — o Centro de Tecnologia da Informação da Marinha (CTIM).

Em consonância com a Estratégia Nacional de Segurança Cibernética, o CTIM possui uma ETIR, chamada Central de Tratamento de Incidentes em Redes de Computadores da Marinha do Brasil (CTIR.mar), bem como uma divisão voltada, dentre outas atividades, para analisar a existência de possíveis vulnerabilidades tanto nos ativos que compõem a rede local de computadores da MB, chamada Rede de Comunicações Integrada da Marinha (RECIM), quanto em sistemas e sites em uso na RECIM e na Internet.

33 São atividades contínuas que visam manter a segurança das informações que trafegam no espaço cibernético e todos que dele usufruem. (BRASIL, 2014).

A MB, em seus documentos estratégicos — a Política Naval e o Plano Estratégico da Marinha — apresenta preocupação com a cibernética ao incluir em sua Política Naval (BRASIL, 2020g) a necessidade de desenvolver a capacidade cibernética na MB. Em seu Plano Estratégico (BRASIL, 2020h), dentre outros pontos, considera o espaço virtual um teatro de operações militares por envolver os setores marítimo, terrestre e espacial, tornando-se, portanto, um alvo a ser protegido, pois a sua vulnerabilidade pode ser uma ameaça àqueles setores.

Desse modo, a MB e as demais FS estão inseridas no modelo de defesa cibernética, contribuindo colaborativamente e proativamente para promover a segurança e a defesa cibernéticas dos ativos de informação contidos em suas Intranet, as quais fazem parte do espaço cibernético nacional, colaborando, portanto, para mitigar os riscos cibernéticos e garantir o funcionamento desse espaço em nível adequado de segurança.

4.4 Fortalecimento e a melhoria contínuos da defesa cibernética: até que ponto podem ser ameaçados?

Diante do relatado até agora, fica evidente que, apesar de todos os acontecimentos apresentados na retrospectiva 2005-2020, não há como vislumbrar comparar o modelo de defesa cibernética brasileiro com o de outros países, ainda que aliados, como os EUA, China e Israel, uma vez que fatos como os relatados no tópico **Defesa x preparo: um modelo de quando os atos não correspondem aos fatos** demonstram a urgente necessidade de rever e de promover o engajamento entre os vários órgãos envolvidos normativamente no processo de defesa cibernética.

É claro que a defesa do espaço cibernético e todos os interesses que o envolvem torna árdua e rapidamente obsoleta a tarefa de proteção, especialmente porque se trata de um ambiente puramente tecnológico, onde, dentre outras características, a obsolência e a evolução, embora tenham significados opostos, andam na mesma velocidade e, por conseguinte, representam desafios para os responsáveis pela defesa desse espaço.

Dessa forma, poder-se-ia elencar uma infinidade de pontos a serem analisados, revisados e aprimorados, porém, dada a complexidade do assunto e a existência de múltiplas vertentes, foram selecionados alguns que podem ameaçar o fortalecimento e a melhoria contínua da defesa cibernética do espaço virtual brasileiro. Para tal, o Quadro 2 apresenta a

ferramenta de análise SWOT[34] com o objetivo de demonstrar as forças; as fraquezas; as oportunidades e as ameças que o atual modelo de defesa cibernética brasileiro possui em relação a proteção de seu espaço cibernético.

Quadro 2 - Análise SWOT do modelo de defesa cibernética brasileiro

	Contribuem para a defesa cibernética	Dificultam a defesa cibernética
Aspectos internos	***Strengths*** Quais são os pontos fortes do atual modelo de defesa cibernética brasileiro? – Arcabouço documental sólido com políticas, estratégias e doutrinas; e – Delegação de competências.	***Weaknesses*** Quais são os pontos fracos do atual modelo de defesa cibernética brasileiro? – Ausência de indicadores para aferir o grau de fortalecimento da E-Ciber, por parte das ETIR e dos setores privados que aderiram à E-Ciber; e – Despreparo quanto ao enfrentamento das ameaças cibernéticas reais que circulam no espaço cibernético.
Aspectos externos	***Opportunities*** Quais são as oportunidades para o atual modelo de defesa cibernética brasileiro? – Apresentar-se no panorama geopolítico como um país que sabe da importância da defesa cibernética para a preservação da soberania nacional; e – Desenvolver a autonomia tecnológica cibernética.	***Threats*** Quais são as ameaças para o atual modelo de defesa cibernética brasileiro? – Ininterrupta evolução tecnológica; e – A guerra cibernética.

Fonte: Adaptado de NAKAGAWA, 2021, p. 2.

34 SWOT é uma ferramenta, cujo acrônimo origina-se de ***S**trengths* (forças), ***W**eaknesses* (fraquezas), ***O**pportunities* (oportunidades) e ***T**hreats* (ameaças), utilizada para descobrir os pontos fortes/fracos dentro do ambiente interno organizacional e as oportunidades/ameaças existentes no âmbito externo à organização. (SEBRAE, 2021).

Por meio dessa análise SWOT é possível verificar que, no âmbito nacional (aspectos internos), os pontos que fortalecem esse modelo são demonstrados pela construção, ao longo de dezesseis anos, de um modelo de defesa cibernética com sólido arcabouço documental e com competências bem definidas entre os órgãos da APF. Por outro lado, os pontos que enfraquecem esse modelo são demonstrados pela ausência de indicadores para aferir o grau de fortalecimento da E-Ciber, por parte das ETIR e dos setores privados que aderiram à E-Ciber e pelo despreparo quanto ao enfrentamento das ameaças cibernéticas reais que circulam pelo espaço virtual, uma vez que, na prática, percebe-se incapacidade dos atores em responder e tratar, em tempo hábil e proativamente, os incidentes cibernéticos.

Quanto ao âmbito internacional (aspectos externos), os pontos de oportunidades para o Brasil são que, pelo fato de ter esse modelo, posiciona-o no panorama geopolítico como ciente da importância da defesa cibernética para a preservação de sua soberania nacional e alavanca a autonomia tecnológica cibernética. Contudo, essas oportunidades estão sob constante ameaça devido a ininterrupta evolução tecnológica e a iminência de uma guerra cibernética.

Dessa forma, percebe-se que a trajetória percorrida pela APF para construção do atual modelo de defesa cibernética gerou um amplo conjunto de diretrizes para a proteção do espaço cibernético brasileiro, cuja prática foram postas a prova nos ataques cibernéticos ocorridos em 2020 a vários órgãos públicos, denunciando a fragilidade na segurança de seus ativos, a ineficiência na proteção contra os ataques e a lentidão em responder efetivamente aos incidentes.

5 CONCLUSÃO

Como visto no tópico **Da Cibernética para o Espaço Cibernético**, desde o embrião da Internet, a tecnologia vem crescendo vertiginosamente motivada, dentre outras qualidades, pela facilidade, comodidade e mobilidade que os dispositivos tecnológicos proporcionam aos seres humanos. Assim, em um mundo cada vez mais digital, o espaço cibernético vem, progressivamente, integrando-se ao cotidiano das pessoas.

Dessa forma, Governos, conduzidos pelo curso normal da modernização e da globalização, estão conectando uma quantidade, sempre crescente, de serviços, por vezes críticos, à Internet. Nesse contexto, nações, em maior ou menor grau, tem participado dessa

corrida para o mundo virtual sem observar os cuidados cibernéticos preventivos para que seus ativos, dados e pessoas trafeguem no espaço cibernético de forma segura e protegida.

Nesse sentido, essa pesquisa apontou que o Brasil, em consonância com os demais países e ciente de suas responsabilidades na conjuntura nacional e internacional, apresenta-se no panorama mundial como consciente sobre a importância da defesa cibernética e que o seu espaço virtual é um fator relevante para a preservação de sua soberania nacional e para o desenvolvimento de sua autonomia tecnológica.

Nessa perspectiva, conforme demonstrado na pesquisa documental apresentada a partir do capítulo **O despertar do Brasil para o setor cibernético: uma retrospectiva de 2005 a 2020**, o país iniciou um longo trabalho de preparo na área cibernética que resultou no atual modelo de defesa do espaço cibernético brasileiro, por meio de um conjunto de normas que são diretrizes para nortear a APF e a sociedade sobre o que e como deve ser realizada a segurança e a defesa desse espaço.

Entretanto, os recentes eventos hostis cibernéticos perpetrados contra o espaço cibernético brasileiro, relatados no tópico **Defesa x preparo: um modelo de quando os atos não correspondem aos fatos**, demonstraram o despreparo dos órgãos quanto ao enfrentamento de ameaças cibernéticas reais que circulam pelo espaço cibernético e falhas no processo de preservação da SIC dos ativos de informação conectados nesse espaço e no tratamento e resposta, de forma tempestiva, dos incidentes cibernéticos que degradaram alguns serviços como os do Superior Tribunal de Justiça, ferindo a disponibilidade, um dos pilares de SIC, que deveria ser garantida pela segurança cibernética.

Assim, de acordo com a pesquisa ora apresentada, ao demonstrar e analisar o Modelo de Defesa Cibernética Brasileiro, a resposta ao problema: *até que ponto o modelo de defesa cibernética brasileiro fomenta o processo contínuo de fortalecimento e a melhoria das defesas cibernéticas nacionais diante da evolução de novas ameaças* é que, no tocante as diretrizes, esse modelo fomenta o processo contínuo de fortalecimento até o ponto do arcabouço documental gerado ao longo de quinze anos, junto com a criação de organizações cibernéticas. Entretanto, no tocante a provar a exequibilidade e a antifragilidade dessas normas, faz-se necessário que as interagências realizem exercícios, de forma contínua e periódica, para testar o atual modelo de defesa cibernética brasileiro com o intuito de validá-lo e aprimorá-lo, visando sempre a melhoria das defesas cibernéticas nacionais diante da evolução de novas ameaças.

Para o Brasil manter-se em condições de enfrentar, em tempo hábil, as ameaças cibernéticas será necessário, a exemplo do Guardião Cibernético, realizar exercícios rotineiros de segurança e de defesa cibernéticas entre as interagências, relacionadas na E-Ciber, para colocar em prática e validar a ampla documentação normativa existente com o objetivo de manter suas equipes aptas a detectar, antecipadamente, quais ameaças poderão impactar o espaço cibernético brasileiro, de modo a, proativamente, adotarem ações efetivas e tempestivas para mitigá-las, reduzindo, ao máximo, possíveis prejuízos a SIC do espaço cibernético.

Conforme mencionado no tópico **Órgãos de defesa cibernética das Forças Singulares: um modelo de atuação colaborativa**, assim como a MB e o EB promovem exercícios cibernéticos para testarem as suas capacidades preventivas e reativas, também a APF e as interagências deveriam envidar esforços para implementar tais treinamentos na rotina da administração pública, a fim de promover a melhoria contínua das ações empreendidas para garantir a segurança e a defesa do espaço cibernético brasileiro.

Somente assim, mesmo diante da ininterrupta evolução tecnológica, do aprimoramento e da complexidade das ameaças cibernéticas, a APF e as interagências poderão, de forma contínua, fortalecer e melhorar as defesas cibernéticas nacionais e manter o preparo adequado para enfrentar outro tipo de guerra, a maior das ameaças do mundo contemporâneo digital e que já é real no ciberespaço — a guerra cibernética.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27032: Tecnologia da Informação – Técnicas de segurança – Diretrizes para segurança cibernética**. Rio de Janeiro, 2015. 72 p.

AXUR. **RELATÓRIO Atividade criminosa online no Brasil 3º trimestre / 2020**. Disponível em: https://conteudo.axur.com/atividade-criminosa-online-brasil-q3-2020. Acesso em: 24 jan. 2021.

BRASIL. Ministério da Defesa. Exército Brasileiro. Secretaria-Geral do Exército. **Boletim do Exército nº 52/2012, de 28 de dezembro de 2012**. Atribui ao Centro de Defesa Cibernética (CDCiber) a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa. Brasília, DF, 2012. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/1/1700/1/be52-12.pdf. Acesso em: 15 jun. 2021.

BRASIL. Ministério da Defesa. Exército Brasileiro. Secretaria-Geral Do Exército. **Boletim do Exército nº 47/2014, de 21 de novembro de 2014**. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética nacional e dá outras providências. Brasília, DF, 2014. Disponível em: https://www.resdal.org/caeef-resdal/assets/brasil----ordenanza-normativa-n---2.777---ministerio-de-defensa,-de-27-de-octubre-de-2014.pdf Acesso em: 14 jun. 2021.

BRASIL. Marinha do Brasil. **Comando de Defesa Cibernética realiza Cerimônia de Transmissão de Cargos**. Brasília, DF, 2021. Disponível em: https://www.marinha.mil.br/noticias/comando-de-defesa-cibernetica-realiza-cerimonia-de-transmissao-de-cargos. Acesso em: 24 jan. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília: Senado Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 jan. 2021.

BRASIL. Ministério da Defesa. **Decreto nº 3.405, de 21 de setembro de 2012**. Atribuir ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa (MD), consoante o disposto no Decreto nº 6.703, de 18 de dezembro de 2008, que aprova a Estratégia Nacional de Defesa (END). Brasília, DF, 21 dez. 2012. Disponível em: https://www.jusbrasil.com.br/diarios/44573976/dou-secao-2-24-12-2012-pg-6. Acesso em: 12 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 5.484, de 30 de junho de 2005**. Aprova a Política de Defesa Nacional, e dá outras providências. Brasília, DF, 30 jun. 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm. Acesso em: 6 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 5 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 7.411, de 29 de dezembro de 2010**. Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores – DAS, aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República; altera o Anexo II do Decreto no 7.063, de 13 de janeiro de 2010, e dá outras providências. Brasília, DF, 29 dez. 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7411.htm. Acesso em: 13 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 7.809, de 20 de setembro de 2012**. Altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009, que aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas dos Comandos da Marinha, do Exército e da Aeronáutica, do Ministério da Defesa. Brasília, DF, 20 set. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7809.htm. Acesso em: 12 jun. 2021.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Decreto nº 8.491, de 13 de julho de 2015**. Altera o Anexo I ao Decreto nº 5.751, de 12 de abril de 2006, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores – DAS e das Funções Gratificadas do Comando do Exército do Ministério da Defesa. Brasília, DF, 13 jul. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/D8491.htm. Acesso em: 16 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF, 26 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art22. Acesso em: 13 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 9.668, de 2 de janeiro de 2019**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares - RMP. Brasília, DF, 30 jan. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9668.htm#art7. Acesso em: 13 jun. 2021.

BRASIL. Presidência da República. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 17 jun. 2021.

BRASIL. Ministério da Defesa. **Defesa discute planejamentos operacionais para a Copa das Confederações**. Rio de Janeiro, RJ, 2013. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/06-03-2013-defesa-militares-tem-ate-o-fim-do-mes-para-definir-estruturas-estrategicas-da-copa-das-confederacoes. Acesso em: 16 jun. 2021.

BRASIL. Ministério da Defesa. **DEFESA - Exército apresenta Simulador Nacional de Operações Cibernéticas. Brasília: MD, 2013**. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/22-01-2013-defesa-exercito-apresenta-simulador-nacional-de-guerra-eletronica. Acesso em: 16 jun. 2021.

BRASIL. Ministério da Defesa. **Diretriz Ministerial nº 0014, de 9 de novembro de 2009**. Integração e coordenação dos setores estratégicos da Defesa. Brasília, DF, 9 jun. 2009. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/portarias/0014a_2009.pdf. Acesso em: 12 jun. 2021.

BRASIL. Marinha do Brasil. Diretoria-Geral do Material da Marinha. **DGMM-0540**: Normas de Tecnologia da Informação da Marinha. Rev.3. Brasília, 2019.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **EMA-135**: Manual de Direito Internacional Aplicado às Operações Navais. Brasília, 2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0**. Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília: Presidência da República, 2015. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf. Acesso em: 17 jan. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei complementar nº 136, de 25 de agosto de 2010**. Altera a Lei Complementar no 97, de 9 de junho de 1999, que "dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas", para criar o Estado-Maior Conjunto das Forças Armadas e disciplinar as atribuições do Ministro de Estado da Defesa. Brasília, DF, 25 ago. 2010. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp136.htm#art1. Acesso em: 14 jun. 2021.

BRASIL. Exército Brasileiro. **Exército Coordena Segurança Da Rio+20. Rio de Janeiro, RJ, 2012**. Disponível em: http://www.eb.mil.br/web/noticias/noticiario-do-exercito?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher %2Fview_content&_101_assetEntryId=1814555&_101_type=content&_101_groupId=16541

&_101_urlTitle=exercito-coordena-seguranca-da-rio-20&inheritRedirect=true. Acesso em: 16 jun. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.341, de 29 de setembro de 2016**. Altera as Leis n º 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios, e 11.890, de 24 de dezembro de 2008, e revoga a Medida Provisória nº 717, de 16 de março de 2016. Brasília, DF, 29 set. 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13341.htm. Acesso em: 14 jun. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa GSI Nº 1, de 13 de junho de 2008**. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/06/2008&jornal=1&pagina=6&totalArquivos=120. Acesso em: 12 jun. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução normativa nº 1, de 27 de maio de 2020**. Brasília: GSIPR, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 13 jun. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução normativa nº 2, de 24 de julho de 2020**. Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700. Acesso em: 13 jun. 2021.

BRASIL. Ministério da Defesa. **JMJ 2013: A participação da Defesa na Jornada Mundial da Juventude. Brasília**, DF, 2013. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/15-07-2013-defesa-a-participacao-da-defesa-na-jornada-mundial-da-juventude. Acesso em: 16 jun. 2021.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, DF, 2012. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/livro_branco/livrobranco.pdf. Acesso em: 13 jun. 2021.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional Brasil 2020**. Brasília, DF, 2012. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 13 jun. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil**. Brasília: GSIPR/SE/DSIC, 2010. Disponível em: http://livroaberto.ibict.br/bitstream/1/639/4/Livro%20verde%20seguran%c3%a7a%20cibern%c3%a9tica%20no%20Brasil.pdf. Acesso em: 12 jun. 2021.

BRASIL. Ministério da Defesa. **MD31-M-07**: Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014. 38 p. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 13 jan. 2021.

BRASIL. Ministério da Defesa. **MD33-M-02**: Manual de abreviaturas, siglas, símbolos e convenções cartográficas das forças armadas. Brasília, DF, 2008. 338 p. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/publicacoes/md33a_ma_02a_mnla_abreva_siglaa_sblcnvca_crtgrffaa_3aed2008.pdf. Acesso em: 13 jan. 2021.

BRASIL. Ministério da Defesa. **MD33-M-12**: Operações Interagências. 2 Ed. Brasília, DF, 2017.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. 2 Ed. Brasília, DF, 2015.

BRASIL. Ministério da Defesa. **MD52-N-01**: Doutrina de Inteligência de Defesa. Brasília, DF, 2005. Desclassificado.

BRASIL. Ministério da Defesa. **Ministro acompanha trabalho de Defesa Cibernética na Copa do Mundo**. Brasília, DF, 2014. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/ministro-acompanha-trabalho-de-defesa-cibernetica-na-copa-do-mundo. Acesso em: 16 jun. 2021.

BRASIL. Marinha do Brasil. **Plano Estratégico da Marinha (PEM 2040)**. Brasília, DF, 2020. Disponível em: https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/book.html. Acesso em: 2 jul. 2021.

BRASIL. Ministério da Defesa. **Política e a Estratégia Nacional de Defesa**. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf. Acesso em: 12 jun. 2021.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF, 2020. 41 p. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 24 jan. 2021.

BRASIL. Marinha do Brasil. **Política Naval**. Brasília, DF, 2020. Disponível em: https://www.marinha.mil.br/sites/all/modules/politica_naval/book.html. Acesso em: 2 jul. 2021.

BRASIL. Presidência da República. Conselho de Defesa Nacional. **Portaria nº 14, de 11 de maio de 2015**. Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0",

desdobramento da Instrução Normativa GSI/PR nº 01/2008. Disponível em: https://www.gov.br/gsi/pt-br/arquivos/portaria-dsic.pdf. Acesso em: 17 jan. 2021.

BRASIL. Ministério da Defesa. Gabinete do Ministro. **Portaria nº 3.781/GM-MD, de 17 de novembro de 2020**. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 14 jun. 2021.

CALDERON, Barbara. **DEEP & DARK WEB**. Rio de Janeiro: Alta Books,2017.

CERT.br. Cartilha de Segurança para Internet 3. **Ataques na Internet**. Disponível em: https://cartilha.cert.br/ataques/. Acesso em: 30 mai. 2021.

CERT.br. Cartilha de Segurança para Internet 4. **Códigos maliciosos (Malware)**. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 30 mai. 2021.

CERT.br. Cartilha de Segurança para Internet 2. **Golpes na Internet**. Disponível em: https://cartilha.cert.br/golpes/. Acesso em: 30 mai. 2021.

CERT.br. Cartilha de Segurança para Internet. **Ransomware**. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 30 mai. 2021.

CNNBRASIL. **Hackers invadem site do Exército e divulgam supostos exames de Bolsonaro**. Disponível em: https://www.cnnbrasil.com.br/politica/2020/05/15/hackers-invadem-site-do-exercito-e-divulgam-supostos-exames-de-bolsonaro. Acesso em: 1 jul. 2021.

COMPUGRAF. **As Principais Guerras Cibernéticas ao Longo da História**. Disponível em: https://www.compugraf.com.br/guerras-ciberneticas-ao-longo-da-historia/. Acesso em: 3 jun. 2021.

CONTEÚDO EDITORIAL. Security Report. **Mais de 3,4 bilhões de tentativas de ataques cibernéticos já atingiram o país em 2020**. Disponível em: https://www.securityreport.com.br/overview/mais-de-34-bilhoes-de-tentativas-de-ataques-ciberneticos-ja-atingiram-o-pais-em-2020/#.X_-E5VjQ-Ul. Acesso em: 13 jan. 2021.

CTIR Gov. **Notificações Reportadas e Incidentes/Vulnerabilidades Confirmados pelo CTIR Gov ao longo do tempo**. Brasília, DF, 2020. Disponível em: https://emnumeros.ctir.gov.br/. Acesso em: 26 jan. 2021.

DEFESANET. **DEFESA – Câmara aprova Política Nacional de Defesa, Estratégia Nacional de Defesa e Livro Branco**. Disponível em: https://www.defesanet.com.br/defesa/noticia/12227/DEFESA---Camara-aprova-Politica-Nacional-de-Defesa--Estrategia-Nacional-de-Defesa-e-Livro-Branco/. Acesso em: 13 jun. 2021.

DEFESANET. **ComDCiber - 1º Exercício Guardião Cibernético**. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/29755/ComDCiber---1--Exercicio-Guardiao-Cibernetico-/. Acesso em: 17 jun. 2021.

DEFESANET. **ComDCiber - Exercício Guardião Cibernético 2.0 (EGC 2.0)**. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/33427/ComDCiber---Exercicio-Guardiao-Cibernetico-2-0-%28EGC-2-0%29/. Acesso em: 17 jun. 2021.

DEFESANET. **Exercício Guardião Cibernético 3.0 - Edital de Chamamento Público**. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/39840/Exercicio-Guardiao-Cibernetico-3-0---Edital-de-Chamamento-Publico/. Acesso em: 17 jun. 2021.

DEFESANET. **FAB implanta Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER)**. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/38958/FAB-implanta-Nucleo-do-Centro-de-Defesa-Cibernetica-da-Aeronautica-%28NuCDCAER%29/. Acesso em: 2 jul. 2021.

DEFESANET. MD – **Política Cibernética de Defesa**. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa/#:~:text=PORTARIA%20NORMATIVA%20No-%203.389%2FMD%2C%20DE%2021%20DE%20DEZEMBRO,2012%20Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20Cibern%C3%A9tica%20de%20Defesa. Acesso em: 13 jun. 2021.

DICIONÁRIO PRIBERAM DA LÍNGUA PORTUGUESA. **Maniqueísta**. 2021. Disponível em: https://dicionario.priberam.org/manique%C3%ADsta. Acesso em: 3 jun. 2021.

ENCYCLOPAEDIA BRITANNICA'S. **Gordon Moore**. Disponível em: https://www.britannica.com/biography/Gordon-Moore. Acesso em: 30 mai. 2021.

ENCYCLOPAEDIA BRITANNICA'S. **William Gibson**. Disponível em: https://www.britannica.com/biography/William-Gibson-American-Canadian-author. Acesso em: 30 mai. 2021.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2003.

FORTINET. **Threat Intelligence Insider Latin America, [3º quadrimestre Q3-2020]**. Disponível em: https://www.fortinetthreatinsiderlat.com/pt/current/landing. Acesso em: 13 jan. 2021.

G1. **Hackers invadem servidores do Exército e vazam CPFs de militares**. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/11/hackers-invadem-servidores-do-exercito-e-vazam-cpfs-de-militares.html. Acesso em: 1 jul. 2021.

G1. **Entenda o caso de Bradley Manning, condenado por vazar segredos**. Disponível em: http://g1.globo.com/mundo/noticia/2013/08/entenda-o-caso-de-bradley-manning-condenado-por-vazar-segredos.html. Acesso em: 3 jun. 2021.

G1. **PF identifica invasão nos celulares de presidentes de STJ, Câmara e Senado; PGR também foi alvo**. Disponível em:

https://g1.globo.com/politica/noticia/2019/07/25/investigacao-da-pf-identifica-invasao-no-celular-de-rodrigo-maia.ghtml. Acesso em: 1 jul. 2021.

GOTARDO, Reginaldo. **Linguagem de programação I**. Rio de Janeiro: SESES, 2015.

INSTITUTO TECNOLÓGICO DE AERONÁUTICA. **ITA firma acordo com Comando de Defesa Cibernética**. Disponível em: http://www.ita.br/noticias/itafirmaacordocomcomandodedefesacibernticadoexrcito. Acesso em: 17 jun. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 15408-1:1999(E)** Information technology — Security techniques — Evaluation criteria for IT security —Part 1: Introduction and general model. 1999. Disponível em: http://comsec.spb.ru/matherials/is/iso15408-1.pdf. Acesso em: 30 jan. 2021.

KASPERSKY. **Mais de 360 mil ameaças foram criadas por dia em 2020**. Disponível em: https://www.kaspersky.com.br/blog/360-mil-ameacas-dia-2020/16750/. Acesso em: 24 jan. 2021.

KASPERSKY. Security Bulletin 2020. **Statistics, 2020**. Disponível em: https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/. Acesso em: 24 jan. 2021.

KASPERSKY. **Um breve histórico dos vírus de computador e qual será seu futuro**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds. Acesso em: 30 jan. 2021.

LONG, Johnny. **No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing**. Burlington:Elsevier, 2008.

MCAFEE, Labs. **Relatório do McAfee Labs sobre ameaças Novembro de 2020**. Disponível em: https://www.mcafee.com/enterprise/pt-br/assets/reports/rp-quarterly-threats-nov-2020.pdf. Acesso em: 24 jan. 2021.

MICHAELIS DICIONÁRIO BRASILEIRO DA LÍNGUA PORTUGUESA. **Coxear**. 2021. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=COXEar. Acesso em: 13 jun. 2021.

MICHAELIS DICIONÁRIO BRASILEIRO DA LÍNGUA PORTUGUESA. **Pandemia**. 2021. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=pandemia. Acesso em: 30 mai. 2021.

MINGST, Karen A.; ARRENGUÍN-TOFT, Ivan M. **Princípios de Relações Internacionais**. Tradução da 6. ed. Rio de Janeiro: Elsevier, 2014.

MITNICK, Kevin D.; SIMON, William l.. **A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson Makron Books, 2003.

NAKAGAWA, Marcelo. **FERRAMENTA: ANÁLISE SWOT (CLÁSSICO)**. Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/ME_Analise-Swot.PDF. Acesso em: 3 jul. 2021.

OTTIS, Rain; Lorents, PEETER. **Cyberspace: Definition and Implications**. 2010. Disponível em: https://www.proquest.com/openview/11c3f4f3a7ca044eeb3a18a4929dc5ff/1?pq-origsite=gscholar&cbl=396500. Acesso em: 30 mai. 2021.

SILBERSCHATZ, A.; GALVIN, Peter; GAGNE, Greg. **Sistemas operacionais: conceitos e aplicações**. Rio de Janeiro: Campus, 2000.

SINGER, Peter W.; FRIEDMAN, Allan. **Segurança e Guerra Cibernética: o que todos precisam saber**. Rio de Janeiro: Biblioteca do Exército, 2017.

THE GUARDIAN. **Edward Snowden: the whistleblower behind the NSA surveillance revelations**. Disponível em: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Acesso em: 3 jun. 2021.

TZU, Sun, com adaptação e prefácio de James Clavell. **A arte da guerra** / Sun Tzu. Rio de Janeiro: Record, 2000.

UNA-SUS. **Organização Mundial de Saúde declara pandemia do novo Coronavírus**. 2020. Disponível em: https://www.unasus.gov.br/noticia/organizacao-mundial-de-saude-declara-pandemia-de-coronavirus. Acesso em: 30 jan. 2021.

UNYLEYA. **Conheça os 10 principais ataques cibernéticos da atualidade**. 2020. Disponível em: https://blog.unyleya.edu.br/bitbyte/ataques-ciberneticos/. Acesso em: 30 jan. 2021.

VEJA. **Brasil sofre seu maior ataque hacker da história**. Disponível em: https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/. Acesso em: 1 jul. 2021.

VON NEUMANN, JOHN. **Theory of Self-Reproducing Automata**. University of lllinois Press URBANA AND LONDON, 1966. Disponível em: http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf. Acesso em: 31 mai. 2021.

WE ARE SOCIAL INC. **Digital 2020: 3.8 billion people use social media**. 2020. Disponível em: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media. Acesso em: 08 mai. 2021.

WIENER, Norbert. **Cibernética: ou Controle de Comunicação no Animal e na Máquina**. São Paulo: Perspectiva, 2017.

WIENER, Norbert. **The human use of human beings: cybernetics and society**. 2. ed. London: Free Association Books, 1989.

WIKILEAKS. **What is WikiLeaks**. Disponível em: https://wikileaks.org/What-is-WikiLeaks.html. Acesso em: 3 jun. 2021.

WILLIAM, Gibson. **Neuromancer**. New York:Berkley Publishing Group. 1984. ISBN: 0-441-56958-7