Ciberdefesa e Cibersegurança

Um Olhar Brasileiro

Marcelo Malagutti

Para mais informações sobre esta publicação visite
www.vegetius.org.br/lv2022-03

ISBN: 978-65-997420-2-6

Publicado pelo Instituto Vegetius, Brasília, DF, Brasil

© Copyright 2022 Instituto Vegetius

Limitação de Direitos:
Este documento e a(s) marca(s) aqui contida(s) são protegidos por lei. Esta representação da propriedade intelectual do Instituto Vegetius é fornecida apenas para uso não comercial. Permite-se a duplicação deste documento apenas para uso pessoal, desde que inalterado e completo. É necessária a permissão do Instituto Vegetius para a reprodução ou reutilização para qualquer outro fim. Para informações sobre permissões de reimpressão ou veiculação, contate vegetius@vegetius.org.br.

Malagutti, Marcelo
Ciberdefesa e cibersegurança : um olhar brasileiro / Marcelo Malagutti. -- Brasília, DF : Instituto Vegetius, 2022.

ISBN 978-65-997420-2-6

1. Brasil. Forças armadas 2. Ciberespaço - Aspectos políticos 3. Defesa nacional
4. Informação eletrônica governamental
5. Sistemas de segurança 6. Segurança pública - Brasil 7. Tecnologia da informação - Aspectos sociais - Brasil I. Título.

22-104551 CDD-355.033081

O Instituto Vegetius é uma instituição brasileira, de caráter filantrópico, sem finalidades lucrativas e sem qualquer vinculação política ou partidária, que atua na área social mediante a realização de pesquisas, estudos, análises e ações voltadas a auxiliar na melhoria de políticas públicas e tomada de decisão e no engajamento da sociedade nos temas de defesa nacional, segurança nacional e internacional, guerra e paz, relações entre forças armadas e sociedade, ciência e tecnologia no âmbito da defesa e segurança nacionais e internacionais, geopolítica e relações internacionais, planejamento, estratégia, estudos estratégicos e ciências militares em geral.

As publicações do Instituto Vegetius não necessariamente refletem as opiniões de seus clientes e patrocinadores.

Se você gostar deste livro, apoie o Instituto Vegetius!

Faça uma doação por meio do PIX.

www.vegetius.org.br

CONVENÇÕES TIPOGRÁFICAS

As seguintes convenções tipográficas podem afetar a compreensão do texto, devendo ser percebidas da seguinte forma:

- ‘Aspas simples’ são usadas em transcrições, realces ou uma citação dentro de uma citação.
- “Aspas duplas” marcam o início e o fim de uma citação que não exceda cinco linhas inteiras; citações de texto em notas de rodapé; expressões vernaculares usadas apenas em um ambiente profissional específico; termos relativos, como gíria, apelidos ou um significado irônico; ou definições conceituais de termos.
- *Itálico* destaca títulos de livros, periódicos, peças de teatro, filmes, óperas, música, pinturas e esculturas. Nomes de espécies científicas, palavras, expressões e frases em outros idiomas (incluindo latim) citados no texto a ser enfatizado também podem estar em itálico.
- **Negrito** realça os nomes dos capítulos, seções e subseções, e letras ou palavras quando o uso de qualquer um dos métodos mencionados acima não for possível.
- <u>Sublinhado</u> indica os nomes das subseções.

Em conformidade com a norma ABNT NBR 6024, a numeração progressiva é utilizada para os trechos do nível um (seções primárias, ou capítulos) ao nível cinco (ex .: 1.1.1.1.1.).

SUMÁRIO

Convenções Tipográficas **1**

Sumário **2**

1 Prelúdio **1-1**

1.1 Sobre a Terminologia Adotada **1-2**
1.1.1 "Ciber"coisas 1-2
1.1.2 Coação ou Coerção? 1-2
1.1.3 Dissuasão x Deterrência 1-3

1.2 Introdução, Contexto e Motivação **1-4**

1.3 O Cerne do Problema **1-5**

1.4 Estrutura do Livro **1-6**

1.5 Referências **1-7**

2 Cibercapacidades Brasileiras **2-1**

2.1 Introdução **2-1**

2.2 Análise Comparada de Estruturas de Ciberdefesa **2-4**

2.3 A Peculiar Organização da Ciberdefesa Brasileira **2-6**

2.4 A necessidade de aumentar o quadro de funcionários da ComDCiber **2-10**
2.4.1 Sobre o tamanho da equipe adequada 2-10
2.4.2 Quão grande deve ser o ComDCiber e como chegar lá? 2-13
2.4.3 A Necessidade de Pessoal Civil 2-15

2.5 Onde Localizar o ComDCiber no Contexto do Ministério da Defesa? **2-21**

2.6 Relatório da OEA e Oxford sobre as capacidades cibernéticas brasileiras **2-23**

2.7 Sobre as Boas Novas 2-30

2.8 Conclusão 2-31

2.9 Referências 2-32

3 Quando 1+1 Não São 2 3-1

3.1 Introdução 3-1

3.2 Sobre Segurança e Defesa 3-3
3.2.1 A Distinção Clássica e a Fusão da Securitização 3-3
3.2.2 A Fusão da Defesa e Segurança Nacionais na Guerra Fria 3-4
3.2.3 A Institucionalização da Defesa e Segurança no Brasil 3-6
3.2.4 A Securitização pós-Guerra Fria 3-7

3.3 Impactos na Ciberdefesa e Cibersegurança Brasileiras 3-12

3.4 Uma Estratégia Cibernética "À Brasileira" 3-15
3.4.1 Quanto ao Escopo 3-16
3.4.2 Quanto à Objetividade, Tempos Verbais e Linguagem 3-19
3.4.3 Sobre a Estrutura do Documento 3-20
3.4.4 Sobre as "Referências" 3-21

3.5 Conclusão 3-23

3.6 Referências 3-24

4 A Oportunidade Estratégica 4-1

4.1 Introdução – "É a Economia, Estúpido!" ("*It's the Economy, Stupid!*") 4-1
4.1.1 Corte de Custos 4-1
4.1.2 Aumento de Receita 4-4

4.2 O Mercado Global de Software 4-4
4.2.1 Os EUA 4-4
4.2.2 Europa 4-5
4.2.3 Brasil 4-6

4.3 O Mercado de Ciberdefesa e Cibersegurança 4-12

4.4 Oportunidade Estratégica 4-14

4.5 Conclusão 4-18

4.6 Referências 4-18

5 Elevando o Software Power Brasileiro 5-1

5.1 Introdução 5-1

5.2 O Caso em Favor da Ciberdissuasão por Negação 5-1

5.3 Como Implementar Ciberdissuasão por Negação? 5-3

5.3.1 Avaliação Situacional 5-4
5.3.2 Arcabouço Legal 5-4
5.3.3 Uma Agência Nacional de Cibersegurança 5-5
5.3.4 Educação e Treinamento 5-6
5.3.5 Implementação de uma Arquitetura de Segurança 5-7
5.3.6 Preparação para Resposta e Resiliência 5-8
5.3.7 Adoção de Boas Práticas Internacionais 5-9
5.3.8 Desenvolvimento de Tecnologia Autônoma 5-10
5.3.9 Desenvolvimento de Ferramentas e Técnicas Forenses e de Atribuição 5-11

5.4 Conclusão 5-12

5.5 Referências 5-12

6 Conclusões 6-1

1 Prelúdio

Em 2010, o Brasil parecia querer alinhar-se a seus pares em segurança cibernética. Após a publicação de *Cyberwar*[1] e na esteira das primeiras revelações do Stuxnet, o Exército Brasileiro criou o núcleo de seu Centro de Defesa Cibernética, enquanto o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (GSI), criado já em 2006, publicou o Livro Verde da Segurança Cibernética[2].

Porém, foi apenas dez anos depois, em fevereiro de 2020, que o Brasil publicou sua primeira estratégia nacional para o ciberespaço, batizada de e-Ciber[3]. Foi o penúltimo país a fazê-lo entre as 15 maiores economias do mundo: Estados Unidos, China, Japão, Alemanha, Índia, Reino Unido, França, Itália, Brasil, Canadá, Rússia, Coreia do Sul, Espanha, Austrália e México[4].

Este livro analisa as cibercapacidades do Brasil, o potencial impacto da e-Ciber sobre elas, e seu potencial desenvolvimento com vistas à elevação de nossas capacidades de ciberdefesa e cibersegurança. Lança, portanto, "um olhar brasileiro" sobre esses temas tão atuais e cada vez mais relevantes.

O livro resultou de extensa pesquisa realizada a partir de 2015. Foi escrito com um enfoque didático, traduzindo conceitos de ciberdefesa e cibersegurança para "não-iniciados" e oferecendo uma visão estratégica sobre elas. Para tanto, reorganiza, atualiza e complementa informações e

---

[1] Clarke e Knake, *Cyber war: The next threat to national security and what to do about it*.

[2] Mandarino e Canongia, *Livro Verde Segurança Cibernética no Brasil*.

[3] Brasil-GSI, "Estratégia Nacional de Segurança Cibernética (e-Ciber)".

[4] IMF, "World Econ. Outlook Database".

análises desenvolvidas no Doutorado em Ciências Militares no Instituto Meira Mattos, da Escola de Comando e Estado-Maior do Exército (ECEME) e no King's College London (Reino Unido) e no Mestrado em Estudos de Guerra no mesmo King's College, bem como em cerca de uma dezena de artigos publicados em revistas acadêmicas ou especializadas, e outras tantas participações em congressos e seminários.

1.1 Sobre a Terminologia Adotada

Diversos termos usados neste livro têm semântica própria, devendo ser entendidos em seu significado específico.

1.1.1 "Ciber"coisas

Adota-se neste livro o adjetivo "cibernética", em suas flexões de gênero e número – cibernética(s) ou cibernético(s) – substituído pelo prefixo *ciber* associado ao substantivo ao qual se refere, em conformidade com as regras do Novo Acordo Ortográfico da Língua Portuguesa. Este padrão, também utilizado pelo Secretário Geral da ONU António Guterres, é adotado em Portugal e nos documentos em língua portuguesa emitidos pela União Europeia, gerando termos como: ciberespaço, cibercrime, cibersegurança, ciberdefesa, ciberdissuasão, ciber-higiene e ciber-resiliência, dentre outros[5].

1.1.2 Coação ou Coerção?

Embora em língua portuguesa as palavras 'coerção' e 'coação' sejam usualmente consideradas sinônimas, seus significados exatos denotam situações distintas: coerção

---

[5] Comissão Europeia, "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE - Comunicação Conjunta ao Parlamento Europeu e ao Conselho"; Parlamento Europeu, "RELATÓRIO sobre ciberdefesa (2018/2004(INI)) - A8-0189/2018".

representa "a força exercida pelo Estado para fazer valer o direito", o uso legal da força por autoridades para impor leis e obrigar ao seu cumprimento; coação representa o uso de "violência física ou moral imposta a alguém para que faça, deixe de fazer ou permita que se faça alguma coisa", levando-a a agir contra sua vontade ou impedi-la de agir conforme seu interesse[6].

Outrossim, o termo coação é mais adequado para traduzir o conceito proposto na *Coercion Theory* de Thomas Schelling[7].

1.1.3 Dissuasão x Deterrência

Em língua portuguesa não existe um termo específico para diferenciar os termos em língua inglesa *dissuasion* e *deterrence*, sendo comumente utilizada a palavra dissuasão em ambos os casos. Dada a relevância da diferenciação dos dois conceitos para o escopo deste trabalho, tomamos emprestado o neologismo *deterrência* usado na Estratégia Nacional de Defesa (END) para *deterrence*, enquanto usamos o clássico termo dissuasão para o sentido de *dissuasion*. Observa-se, no entanto, que a END considera deterrência e dissuasão como sinônimos[8], do que divergimos frontalmente, pelas razões expostas no Capítulo 4.

Em função da opção pelo uso do termo deterrência, foi preciso adaptarmos outros termos derivados:

- Deterrente: aquele ou aquilo que exerce deterrência;
- Deterrido: aquele que é objeto da deterrência;

---

[6] Houaiss e Villar, *Dicionário Houaiss da Língua Portuguesa*.

[7] Schelling, *Arms and influence: With a new preface and Afterword*.

[8] Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa", 76.

- Deterrer: verbo que indica a ação de exercer a deterrência. Não cabe o uso do verbo “deter”, que possui significado diverso.

1.2 Introdução, Contexto e Motivação

“Ferramentas de software” há muito são utilizadas para espionagem, sabotagem, crime ou ativismo, patrocinados ou não por estados. Entre muitos exemplos, o caso Snowden, em particular, revelou uma grande operação de espionagem estatal. Envolvia espionagem política, relacionada às comunicações pessoais da Chanceler da Alemanha, dos Presidentes de Brasil e México, de alguns de seus ministros, além de milhares de outras pessoas[9]. Fora do âmbito político, Snowden também denunciou a espionagem sistemática da Petrobras, a estatal brasileira de petróleo que havia anunciado a descoberta de gigantescas reservas de petróleo em águas jurisdicionais brasileiras alguns anos antes. Ficou bem claro que os norte-americanos realizaram operações de espionagem política e econômica tendo o Brasil com um de seus alvos.

Antes do Caso Snowden, houve um caso notavelmente diferente, denominado Stuxnet, consistindo no uso de um malware que sabotou a centrífugas nucleares iranianas, alegadamente atrasando o programa nuclear daquele país e forçando-o a aceitar a fiscalização desse programa pela Agência Internacional de Energia Atômica (AIEA). Embora não visasse atacar o Brasil em particular, o malware Stuxnet também infectou infraestruturas críticas brasileiras que utilizavam sistemas de controle industrial fornecidos pela empresa alemã Siemens[10]. Fosse o Brasil o

---

[9] Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state*.

[10] Falliere, Murchu, e Chien, “W32.Stuxnet Dossier”.

alvo pretendido, sem dúvida o país teria sofrido efeitos nocivos e potencialmente catastróficos.

Num cenário de guerra ainda em desenvolvimento, desde 2014 a Rússia faz da Ucrânia um laboratório de ciberconflitos, que se intensificaram com a recente invasão da segunda pela primeira[11].

Nesse contexto geopolítico absolutamente atual, e considerando o desejo e a necessidade de inserção internacional do Brasil, um "olhar brasileiro" sobre o ciberpoder dos estados-nação e sua utilização como instrumento de coação no cenário internacional torna-se relevante para o entendimento de como esse ciberpoder pode afetar a soberania nacional. De fato, os casos recentes de ciberofensas tornados públicos demonstram que o Brasil precisa estar preparado para evitar se tornar uma presa fácil para nações interessadas no uso desses instrumentos.

1.3 O Cerne do Problema

O núcleo do livro consiste em uma avaliação das cibercapacidades brasileiras atuais, na avaliação do potencial de melhoria dessas capacidades à luz das atuais políticas públicas (como a e-Ciber) e demonstrar que o "Poder de Software" (Software Power) pode ser uma alternativa para nações com cultura institucional e tradição (ou personalidade) não-agressiva no sentido de desenvolverem suas capacidades e se inserirem no crescente mercado internacional de produtos e serviços de ciberdefesa e cibersegurança.

As fontes utilizadas para a elaboração do livro foram exclusivamente fontes abertas: documentos oficiais de várias nações e agências multilaterais, livros, relatórios, artigos acadêmicos e de notícias, vídeos, palestras e notas de conferências, em particular da Escola Superior de Guerra (ESG), do King's College London e da Escola de Comando e

---

[11] Malagutti, "Ciberofensas e a Crise da Ucrânia".

Estado-Maior do Exército (ECEME), aulas de mestrado e doutorado, seminários e debates, bem como de congressos e workshops no Brasil e no exterior. Além disso, visitas técnicas e conversas com o pessoal do Comando de Defesa Cibernética (ComDCiber) do Brasil forneceram valiosas informações não sigilosas.

1.4 Estrutura do Livro

O livro se dedica a analisar a realidade da ciberdefesa e cibersegurança no contexto brasileiro. O Capítulo 2 apresenta uma análise das atuais "Cibercapacidades Brasileiras". Seguindo, o Capítulo 3, "Quando 1+1 Não São 2", analisa o impacto da cultura estratégica brasileira na formulação da e-Ciber, a Estratégia Brasileira de Segurança Cibernética, e a não inclusão, nela, da ciberdefesa, surpreendentemente deixada para uma outra estratégia futura. Oferecendo uma perspectiva positiva, o Capítulo 4 analisa "A Oportunidade Estratégica" que se apresenta, mostrando que o Brasil, ao invés de andar a reboque dos países mais avançados, pode se beneficiar da demanda mundial de produtos e serviços de ciberdefesa e cibersegurança. A seguir, parafraseando um ícone da cultura política brasileira, o lendário Odorico Paraguaçu [12], busca-se sair da mera apresentação da problemática, para a proposição de uma "solucionática". Assim, o Capítulo 5 propõe medidas relativamente simples e de baixo custo que o país pode adotar, "Elevando o Software Power Brasileiro" e abrindo espaço para não apenas melhorar suas defesas, mas também explorar a oportunidade estratégica que se apresenta.

---

[12] Prefeito da imaginária cidade de Sucupira, personagem criado pelo dramaturgo e novelista Dias Gomes Odorico, na peça *O Bem-Amado ou Os Mistérios do Amor e da Morte*, de 1962, e adaptada pelo próprio autor como telenovela exibida de 24 de janeiro a 9 de outubro de 1973, sob a direção de Régis Cardoso.

Por fim, à guisa de “Conclusão”, o Capítulo 6 faz um apanhado dos temas abordados nos capítulos anteriores, consolidando as ideias apresentadas, as conclusões do trabalho, apontando seus pontos fortes e fracos, e possíveis desenvolvimentos futuros.

1.5 Referências

Brasil-GSI. “Estratégia Nacional de Segurança Cibernética (e-Ciber)”. *Participa.Br*. Brasília, 2020. http://www.participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber.

Brasil-MD. “Política Nacional de Defesa e Estratégia Nacional de Defesa”. Brasília, 2020.

Clarke, Richard A, e Robert K Knake. *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins Publishers, 2010.

Comissão Europeia. “Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE - Comunicação Conjunta ao Parlamento Europeu e ao Conselho”. Bruxelas, 2017.

Falliere, Nicolas, Liam O Murchu, e Eric Chien. “W32.Stuxnet Dossier”. *Symantec-Security Response*. Vol. Version 1., 2011. https://doi.org/20 September 2015.

Greenwald, Glenn. *No place to hide: Edward Snowden, the NSA and the surveillance state*. Penguin Books, 2014.

Houaiss, Antônio, e Mauro Villar. *Dicionário Houaiss da Língua Portuguesa*. Rio de Janeiro: Editora Objetiva, 2001.

IMF. “World Economic Outlook Database”. World Economic Outlook Database, 2019. https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/weorept.aspx?pr.x=57&pr.y=17&sy=2019&ey=2019&scsm=1&ssd=1&sort=country&ds=.&br=1&c=512%2C668%2C914%2C672%2C612%2C946%2C614%2C137%2C311%2C546%2C213%2C674%2C911%2C676%2C314%2C548%2C193%2C556%2C122%2C6.

Malagutti, Marcelo. “Ciberofensas e a Crise da Ucrânia”. *Observatório Militar da Praia Vermelha*. Rio de Janeiro, 7 de fevereiro de 2022. http://ompv.eceme.eb.mil.br/defesa-cibernetica/guerra-cibernetica/430-ccu.

Mandarino, Raphael, e Claudia Canongia, orgs. *Livro Verde Segurança Cibernética no Brasil*, 2010.

Parlamento Europeu. “RELATÓRIO sobre ciberdefesa (2018/2004(INI)) - A8-0189/2018”, 2018.

Schelling, Thomas. *Arms and influence: With a new preface and Afterword*. Yale University Press, 2008.

2 Cibercapacidades Brasileiras

Este capítulo analisa a necessidade de atualização do Comando Brasileiro de Defesa Cibernética (ComDCiber) para atender às necessidades do país, considerando aspectos como a inserção do órgão na estrutura organizacional do Ministério da Defesa do Brasil, sua missão e estrutura, além de fatores relacionados ao dimensionamento, aquisição e retenção de pessoal, seja militar ou civil.

2.1 Introdução

Entre a criação do Centro de Defesa Cibernética do Exército (CDCiber) em 2010 e o lançamento do e-Ciber em 2020, os "pares" do Brasil se moveram mais rápido, alocando recursos significativos para suas estruturas de ciberdefesa.

Em 2014, quatro anos após a criação do Comando Norte-Americano de Ciberdefesa (USCyberCom), os EUA anunciaram a intenção de, até 2018, criar uma Cyber Mission Force (CMF), a ser constituída por 133 Cyber Mission Teams (CMTs), distribuídas entre as diferentes forças singulares do país e constituído por um total de 6.200 profissionais, operacionalmente preparados para realizar operações cibernéticas militares ofensivas e defensivas[1]. Em agosto de 2017, o USCyberCom recebeu o status de Full Combatant Command. Assim, tornou-se independente do USStratCom (Comando Estratégico dos EUA). Portanto, mais capaz de administrar seu orçamento[2].

O Reino Unido, por sua vez, anunciou em 2015 a recriação do 77º Batalhão, com 1.500 integrantes, para

---

[1] US-ArmyCyber, "DOD FACT SHEET: Cyber Mission Force > U.S. Army Cyber Command > Fact Sheets."

[2] Marks, "At 7 Years Old, CYBERCOM Becomes a Full Combatant Command - Defense One."

combater a guerra de informação, com foco nas redes sociais[3]. Em 2016, no lançamento de sua Estratégia de Cibersegurança 2016-2021, anunciou investimentos de 1,9 bilhão de libras esterlinas (GBP), equivalente 13,5 bilhões de reais (BRL), em cibersegurança do Reino Unido nos próximos dez anos[4]. O valor corresponde a uma média de BRL 1,35 bilhões anuais. Em 2017, foi anunciada a Força Cibernética Nacional (National Cyber Force), de caráter eminentemente ofensivo, vinculada ao Ministério da Defesa e ao GCHQ (agência britânica de inteligência de sinais, ou SIGINT), com efetivo inicial de 500 profissionais das Forças Armadas, GCHQ e terceiros, que deverá ser expandido para mais de 2.000 profissionais em três anos, ao custo de GBP 250 milhões (BRL 1,78 bilhão)[5].

Já a Austrália, em agosto de 2020, publicou uma nova versão de sua Estratégia de Cibersegurança[6]. O documento prevê investimentos do governo australiano de 1,67 bilhão de dólares australianos (AUD), ou BRL 6,5 bilhões, ao longo de dez anos[7]. Ressalta ainda que sua precursora, a ciberestratégia de 2016, promoveu um investimento de AUD 230 milhões (cerca de BRL 900 milhões) em seus quatro anos de vigência[8]. Além disso, o investimento médio do governo australiano foi de BRL 225 milhões por ano entre 2016-2020 e deve subir para BRL 650 milhões entre 2020-2024. O investimento seria justificado com base em estimativas de que incidentes

---

[3] Paganini, “The British Army Creates the 77th Battalion.”

[4] United Kingdom, “Cyber Security Strategy.”

[5] Haynes, “Britain to Create 2,000-Strong Cyber Force to Tackle Russia Threat | UK News | Sky News”; Sabbagh, “UK to Launch Specialist Cyber Force Able to Target Terror Groups.”

[6] Australia, “Australia’s Cyber Security Strategy 2020.”

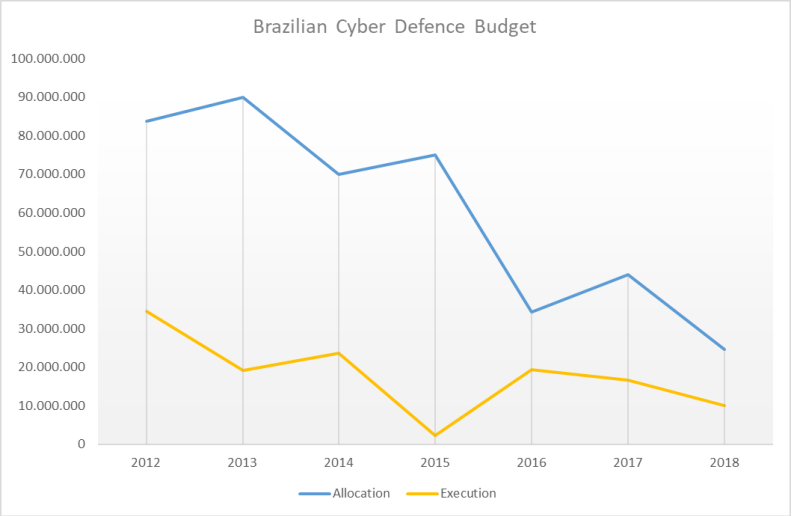
[7] Australia.

[8] Australia.

cibernéticos podem causar perdas de até AUD 29 bilhões, ou 1,9% do PIB do país, anualmente[9].

A e-Ciber brasileira não faz menção aos valores dos investimentos. Um relatório do Senado Federal apontou que o orçamento brasileiro de ciberdefesa em 2020 foi de apenas BRL 22 milhões (ou USD 4,16 milhões), dos quais apenas BRL 6,1 milhões foram destinados ao ComDCiber[10]. Além disso, como mostra a Figura 2-1, o orçamento da ciberdefesa brasileira vem diminuindo ao longo dos anos, em sentido contrário ao observado em outros países.

Figura 2-1 – Evolução do Orçamento Brasileiro de Ciberdefesa



Fonte: Compilada pelo autor com dados de Amin[11]

O relatório do Senado aponta ainda que perdas decorrentes de ciberincidentes em empresas brasileiras em

---

[9] Australia.

[10] Amin, "Relatório de Avaliação de Política Pública: A Política Nacional Sobre Defesa Cibernética."

[11] Amin.

2018 teriam sido de 20 bilhões de dólares americanos (USD)[12]. Isso equivale a AUD 28 bilhões, um valor semelhante ao das perdas australianas. No entanto, em termos comparativos, o orçamento brasileiro de cibersegurança corresponde a apenas 3% do australiano, embora o Produto Interno Bruto (PIB) australiano corresponda a cerca de 70% do brasileiro. Além disso, o relatório indica que o orçamento da ciberdefesa brasileira deve ser de BRL 60 milhões até 2020 (ou USD 11,5 milhões) e de BRL 120 milhões (USD 22,7 milhões) por ano para os três anos subsequentes[13].

2.2 Análise Comparada de Estruturas de Ciberdefesa

A Tabela 2-1 mostra dados públicos sobre estruturas de ciberdefesa em diversos países, considerando agências de inteligência e de sinais, de contrainteligência, de cibersegurança (civis) e de ciberdefesa (militares) e o ano de publicação de suas primeiras estratégias cibernéticas.

Dos países listados, Alemanha e China optaram pela criação de forças independentes, enquanto EUA, França e Reino Unido atuam com comandos que reúnem pessoal de diferentes forças individuais sob um comando unificado, subordinado ao Estado-Maior Conjunto ou um comando estratégico nacional, mantendo também equipes dedicadas à defesa das redes específicas de cada força armada singular. Tais ações visam garantir maior coesão dos esforços de ciberdefesa. Com exceção do Brasil, todas as nações integram suas forças de ciberdefesa com suas agências de inteligência de sinais (SIGINT), e em todas elas o comando da ciberdefesa militar é exercido por um general 4 estrelas, o posto militar mais alto em condições de paz.

---

[12] Amin.

[13] Amin.

Tabela 2-1 – Organizações de Ciberdefesa e Cibersegurança.

País	**Intel.**	**Contra Intel.**	**Segurança**	**Defesa**	**Ataque**	**1ª NCSS**	**Ativos**
USA	NSA CIA NGA	FBI	DHS NIST	NSA	USCyberCom	2003	7.000 (NSA) 6.200 (USCyberCom)
China	3rd Dep (EM-EPL)	3º Dep (EM-EPL)	3º Dep (EM-EPL)	4º Dep (EM-EPL)	4º Dep (EM-EPL)	2003	"centenas ou milhares" (Unit 61398)
França	DGSE	DGSI	ANSSI	CALID	ComCyber	2008	3.500 (CyberCom) 600 (ANSSI)
UK	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ & MoD	2009	1.900+ (NCSC) 2.000 (NCF)
Alemanha	BND BSI KSA	BfV	BSI	CIR	CIR	2011	13.600 (CIR)
Brasil	N/A	N/A	GSI/DSIC	ComDCiber	ComDCiber	2020	180~

Fonte: Compilada pelo autor com dados de diversas fontes[14]

[14] Pernik, Wojtkowiak, and Verschoor-Kirss, *National Cyber Security Organisation: UNITED STATES*; Osula, *National Cyber Security Organisation: United Kingdom*; Raud, *China and Cyber: Attitudes, Strategies, Organisation*; Schulte, "German Cyber Command Becomes Operational"; Brangetto, *National Cyber Security Organisation: France*; Brasil-CN, "Relatório Da CPI Da Espionagem Eletrônica Do Senado Federal"; Stokes, "The PLA General Staff Department Third Department Second Bureau"; Barlouet, "La France Muscle Sa Cyberdéfense"; Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*; Osborne, "Chancellor's Speech to GCHQ on Cyber Security."

2.3 A Peculiar Organização da Ciberdefesa Brasileira

Entre os países analisados, o Brasil optou por uma organização única. A atual estrutura de ciberdefesa brasileira é composta pelo Comando de Defesa Cibernética (ComDCiber), um "comando conjunto" subordinado ao Comando do Exército (Exército Brasileiro). Embora argumentos políticos possam ser usados para tentar justificar essa opção, ela constitui uma *jabuticaba*[15]. Além disso, diferentemente dos casos do programa nuclear, de responsabilidade estratégica exclusiva da Marinha do Brasil, e do programa espacial, compromisso estratégico exclusivo da Força Aérea, a ciberdefesa, embora atribuída ao Exército, constitui um comando conjunto dos três ramos singulares das forças armadas. Conceitualmente, espera-se que um comando conjunto esteja vinculado ao Estado-Maior Conjunto das Forças Armadas (EMCFA) ou diretamente ao Ministério da Defesa (MD), como é o caso dos demais países analisados, e não a uma única força.

Além da situação inusitada mencionada acima, o Brasil apresenta outra característica idiossincrática. Dentro da estrutura do Exército, o ComDCiber está subordinado ao Departamento de Ciência e Tecnologia (DCT), órgão eminentemente ligado à pesquisa e desenvolvimento tecnológico[16]. Subordinado ao ComDCiber está o CDCiber, braço operacional cibernético, tanto defensivo quanto ofensivo, do Exército. Trata-se, portanto, de um comando operacional vinculado a um órgão de ciência e tecnologia, o que constitui outra situação inusitada[17].

O ComDCiber possui, ao lado do CDCiber, um Estado-Maior Conjunto (EMC) e um Departamento de Gestão e

---

[15] Popularmente usa-se o termo "jabuticaba" para indicar algo que, como a própria fruta, só existe no Brasil.

[16] Brasil-MD, "Exército Bras. - Organograma."

[17] Brasil-MD.

Educação (DGE). O ComDCiber é comandado por um General de 3 estrelas, enquanto os comandantes do CDCiber, EMC e DGE são oficiais generais de 2 estrelas. Como o Exército tem a responsabilidade formal pela ciberdefesa, o comandante do ComDCiber vem exclusivamente das fileiras do Exército. Da mesma forma, como o CDCiber é o braço operacional do Exército, seu comandante também vem exclusivamente dessa força. Portanto, a característica "conjunta" do ComDCiber se restringe à participação da Marinha e da Aeronáutica, alternadamente, no comando do EMC e do DGE[18].

Existem alguns problemas com essa concepção brasileira. A hierarquia relativamente baixa do comandante do ComDCiber dificulta a coordenação das ações, mesmo dentro do Ministério da Defesa (MD). Um exemplo disso pode ser encontrado na Estratégia Nacional de Defesa de 2016, que, ao reafirmar que a ciberdefesa é um setor estratégico sob responsabilidade do Exército (BRASIL, 2016, p. 31) estipula o que se segue:

> Considerando que a Força Aérea se configura como uma organização altamente tecnológica, são essenciais as capacidades de proteção dos Sistemas de Comando e Controle e Estruturas Estratégicas do País, especialmente aquelas que envolvem o ciberespaço. Deve, portanto, manter o nível de segurança e defesa de seus sistemas informáticos em alto grau.[19]

Apesar de várias críticas ao trecho, inclusive minhas, a última versão do END, enviada em julho de 2020 para apreciação do Congresso, manteve essa redação[20].

---

[18] Brasil-MD.

[19] Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa," 2016.

[20] Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa," 2020.

Em segundo lugar, estando hierarquicamente em uma posição relativamente baixa no organograma do Exército, sua luta por recursos torna-se bastante desequilibrada. Somente após a divisão do orçamento de defesa entre o MD e as forças singulares, o ComDCiber terá seu orçamento definido, concorrendo com os diversos projetos prioritários dentro do Exército. Além disso, embora seja um comando operacional *de facto*, por estar sob a estrutura de P&D do Exército, a cultura brasileira o torna preterido na disputa por recursos com as áreas operacionais *de jure*. Um exemplo disso é encontrado no Relatório do Senado sobre Políticas de Defesa Cibernética, que estabelece:

> Apresentamos sugestão de alteração à Comissão de Relações Exteriores e Defesa Nacional - CRE, no valor de R$ 60 milhões para Defesa Cibernética, porém a Comissão aprovou, por opção da Força [Exército Brasileiro], o Programa relacionado à Aviação do Exército, como prioridade.[21]

Em outras palavras, o Exército Brasileiro relegou o que a END estabelece como seu setor estratégico para alocar recursos à Aviação do Exército, que teria como objetivo garantir o abastecimento dos Pelotões de Fronteira, sob o argumento de que a Força Aérea não prioriza essa atividade[22]. Fosse esta uma prioridade real de defesa nacional, seria mais sensato para o MD realocar as prioridades da Força Aérea do que instituir uma aviação de asa fixa dentro do Exército. Ressalta-se que o decreto que autorizou a recriação da Aviação do Exército foi publicado em 2 de junho de 2020, mas sob forte

---

[21] Amin, "Relatório de Avaliação de Política Pública: A Política Nacional Sobre Defesa Cibernética."

[22] DefesaNet, "Aviação Do Exército - Exército Recria Aviação de Asas Fixas e FAB Critica."

oposição da Força Aérea foi revogado em 8 de junho[23]. Portanto, a ciberdefesa, setor estratégico determinado pela Estratégia Nacional de Defesa, perdeu recursos para um projeto interno do Exército. o qual não se concretizou.

As dificuldades também podem ser percebidas no contexto administrativo de pessoal do próprio Exército Brasileiro. Como em qualquer exército, existem muitos ramos especializados (ou 'armas'): Infantaria, Cavalaria, Artilharia, Engenharia, Comunicações, Intendência e Material Bélico, para citar apenas os mais relevantes. No Exército Brasileiro, o ciberespaço historicamente foi uma atribuição 'intrínseca' da arma de Comunicações, de modo que oficiais de outras armas têm dificuldades operacionais para fazer carreira na ComDCiber. Ocorre que os planos de carreira das 'armas' exigem que seus dirigentes passem por determinados cargos ao longo de sua trajetória profissional. Assim, para que um oficial de infantaria avance na carreira, ele deve necessariamente trabalhar em unidades e funções de infantaria por longos períodos, mesmo que tenha se destacado, em determinado momento de sua carreira, com operações cibernéticas e que desejasse continuar nesse caminho. Assim, recursos humanos que seriam ativos significativos para a ciberdefesa, cujas habilidades e treinamento dificilmente seriam substituíveis em uma estrutura tão pequena, são realocados para outras áreas por exigências burocráticas.

Outra dificuldade desse vínculo histórico com a 'arma' das Comunicações diz respeito à já mencionada distribuição dos escassos recursos financeiros dentro do Exército. Até 2018 (10 anos após a primeira END designar a ciberdefesa como um setor estratégico da defesa nacional), todos os comandantes do ComDCiber eram oficiais generais da arma de comunicações. Em todo este período, não houve um único general desta arma

---

[23] DefesaNet, "Aviação Do Exército - Urgente - Revogado Decreto Sobe a Aviação Do Exército."

promovido a 4 estrelas. Assim, nunca houve um representante do ComDCiber no Alto Comando do Exército. Essa situação somente foi mitigada quando, em 2018, pela primeira vez, um general de artilharia de 3 estrelas assumiu o comando do ComDCiber, sendo promovido a 4 estrelas em 2021 e assumindo a Chefia do DCT, superior hierárquico do ComDCiber.

Adicionalmente, dentre todas as nações analisadas, apenas o Brasil não possui uma agência de Inteligência de Sinais (SIGINT), embora a criação de tal agência tenha sido recomendada pela Comissão de Investigação de Espionagem Eletrônica do Senado, instituída na esteira do Caso Snowden em 2013 (BRASIL, 2013). Consequentemente, as cibercapacidades nacionais brasileiras são ainda mais limitadas quando comparadas às de outras nações, aumentando a importância relativa do ComDCiber e exigindo maior agilidade e rapidez em sua operacionalização e eficácia.

2.4 A necessidade de aumentar o quadro de funcionários da ComDCiber

2.4.1 Sobre o tamanho da equipe adequada

De acordo com os limitados dados públicos disponíveis, a força de trabalho do ComDCiber é de aproximadamente 180 pessoas [24]. Consequentemente, um quadro menor que o de uma Companhia tradicional do Exército, mas com a responsabilidade operacional de uma Brigada, e comandado por um General de Divisão. Esse quantitativo de pessoal (efetivo) é inadequado para uma nação com as características econômicas, demográficas, geopolíticas e até militares do Brasil.

---

[24] Okamura, “Abertura Do V Seminário Internacional de Defesa Cibernética.”

É possível fazer algumas comparações relevantes, considerando os dados da Tabela 2-1 e do site Global Fire Power[25].

2.4.1.1 Poder de Paridade de Compra do PIB

As comparações baseadas no PIB fornecem *insights* considerando alguma proporcionalidade quanto às dimensões dos interesses a serem defendidos. A Tabela 2-2 apresenta uma amostra dos países cujos NCSSs são estudados neste trabalho, ordenados de acordo com seu PIB ajustado pela Paridade do Poder de Compra (PPP, da sigla em inglês). A PPP não considera o valor absoluto do PIB em dólares, mas seu valor relativo considerando os custos locais.

Tabela 2-2 – População, Militares e PIB-PPP

País	**População**	**Militares na Ativa**	**%Ativa**	**PIB-PPP (bilhões USD)**	**Def. (bilhões USD)**	**%Def**
China	1.384.688.986	2.183.000	0,16%	24.810	237	0,96%
EUA	329.256.465	1.400.000	0,43%	19.850	750	3,78%
Alemanha	80.457.737	182.650	0,23%	4.300	50	1,16%
Rússia	142.122.776	1.013.628	0,71%	4.025	48	1,19%
Brasil	208.846.892	334.500	0,16%	3.300	28	0,84%
Reino Unido	65.105.246	192.660	0,30%	2.974	55	1,85%
França	67.364.357	268.000	0,40%	2.904	42	1,43%
Itália	62.242.674	175.000	0,28%	2.344	28	1,19%

Fonte: Compilada pelo autor com dados do Global Firepower Index[26]

Como observado, a China tem um PIB-PPP de USD 24,81 trilhões, os Estados Unidos de USD 19,85 trilhões, o Brasil de USD 3,30 trilhões, e assim por diante. O PIB-PPP do

[25] GlobalFirepower.com, "2020 Military Strength Ranking."

[26] GlobalFirepower.com.

Brasil é 11% superior ao do Reino Unido e 13% superior ao da França. Portanto, presume-se que o Brasil deva defender interesses econômicos globais da mesma ordem de grandeza daqueles desses países. Isso estabelece um primeiro parâmetro para comparação da necessidade de poder.

2.4.1.2 Proporcionalidade do efetivo cibernético com o efetivo militar total

A Tabela 2-3 apresenta dados sobre o pessoal militar de alguns dos países, complementados com dados públicos sobre o respectivo pessoal de ciberdefesa. Cabe destacar que a coluna CyberCom informa apenas os militares de cada país. Portanto, os mais de 7.000 funcionários da NSA dos EUA não são considerados, pois é uma agência de inteligência de sinais, não um comando militar. No caso britânico, o Batalhão 77 não foi considerado, pois era dedicado à guerra informacional, tema diferente não tratado nesta pesquisa.

Entre os países listados na Tabela 2-3, os EUA são o país com a maior força militar ativa, com o Brasil em segundo lugar, e assim sucessivamente. Ao considerar o pessoal engajado na ciberdefesa em relação ao total de militares ativos (coluna "%Cyber"), no entanto, o Brasil aparece como um *outlier* (ponto fora da curva) absoluto.

Tabela 2-3 – Equipe de Defesa e Ciberdefesa Comparada

País	**Ativo**	**Cyber Com**	**%Ciber**	**%Med**	**%RU**	**%FR**	**%EUA**
EUA	1.400.000	6.200	0,44%	14.943	14.533	18.284	6.200
Brasil	334.500	180	0,05%	3.570	3.472	4.368	1.481
França	268.000	3.500	1,31%	2.861	2.782	3.500	1.187
Reino Unido	192.660	2.000	1,04%	2.056	2.000	2.516	853
Alemanha	182.650	13.500	7,39%	1.950	1.896	2.385	809
Total	*2.377.810*	*25.380*	*1,07%*				

Fonte: Compilado pelo autor

Em termos comparativos, a Alemanha possui uma força cibernética composta por 7,39% do total de seu efetivo militar ativo (coluna %Ciber). A da França corresponde a 1,31% do efetivo total e a do Reino Unido a 1,04%, enquanto a dos EUA a 0,44% e a do Brasil a apenas 0,05%. A média geral é de 1,07%. Se a percentagem média for considerada um parâmetro adequado, o quantitativo de pessoal da 'ciberforça' nacional de cada país deve ser aquele da coluna "%Med". Por outro lado, se a taxa do efetivo britânico for considerada correta, os números seriam os da coluna "%RU". Se considerado que a taxa francesa é mais adequada, os quantitativos seriam aqueles da coluna "%FR" e para a taxa dos EUA, aqueles da coluna "%EUA". Com base nessas taxas, respectivamente, o tamanho da equipe de ciberdefesa brasileira deveria ser de 3.570, 3.472, 4.368 ou 1.481 profissionais, conforme o índice adotado, para manter certa proporcionalidade com esses países.

No entanto, como já mencionado, os interesses econômicos brasileiros são comparáveis aos dos franceses e ingleses (na verdade, mais de 10% superiores). Portanto, o tamanho adequado do efetivo da ciberdefesa brasileira, considerando militares, civis e terceirizados, deveria ser de 3.472, pelo índice britânico, ou 4.368 pelo indicador francês, considerando o equilíbrio das forças cibernéticas em proporção às demais forças. Embora os números possam parecer um tanto altos, o maior deles corresponde aproximadamente ao efetivo de uma Brigada tradicional, comando de um general de 2 estrelas.

2.4.2 Quão grande deve ser o ComDCiber e como chegar lá?

Como demonstrado na seção anterior, o quadro efetivo ComDCiber brasileiro é relativamente pequeno, considerando parâmetros usuais de comparação relativa. A justificativa para a manutenção desse estado de coisas usualmente se baseia na

falta de recursos materiais e humanos devido a restrições orçamentárias e no argumento de que a Emenda Constitucional 95 (EC95) congelou os gastos do governo federal até 2037. Ocorre que os países mencionados na comparação também enfrentam cortes orçamentários em seus gastos com defesa. As unidades da Força de Missão Cibernética dos EUA anteriormente mencionadas, anunciadas em 2014, foram concluídas em maio de 2018, quatro meses antes do previsto. No entanto, entre 2014 e 2018, o orçamento do DoD foi reduzido em cerca de 8,5%, enquanto o orçamento da USCyberCom foi aumentado em 8%. Portanto, um crescimento relativo de mais de 18% em tempos de redução geral, demonstrando que os EUA trabalham com uma priorização diferenciada para a ciberdefesa em relação às outras áreas. Da mesma forma, dados do Reino Unido e Austrália mostram priorização semelhante.

Da teoria da estratégia, sabe-se que os fins devem ser priorizados na ausência de meios. A PND e a END estipulam as áreas prioritárias pretendidas de cada força no Brasil. A Marinha do Brasil sinaliza que está priorizando o programa de submarinos de propulsão nuclear (PROSUB) sacrificando inclusive a manutenção de sua frota de superfície. Mas o domínio espacial faz pouco progresso com a Força Aérea, assim como o cibernético no Exército.

Considerando a conclusão anterior de que os interesses brasileiros são da mesma ordem de grandeza que os do Reino Unido e da França, e seguindo a lógica da relativa proporcionalidade entre militares e cibernéticos, o efetivo da ComDCiber deve ser de pelo menos 3.500 profissionais. No entanto, um crescimento dessa magnitude demanda tempo, planejamento e perseverança. Uma possibilidade ambiciosa, mas viável, seria um crescimento em oito anos, ou quatro fases de dois anos (tempo médio para troca de comando em uma unidade militar brasileira). Um total de 3.500 profissionais

seria alcançado de acordo com a escala de Tabela 2-4, com os aumentos previstos nas colunas “1º Semestre” e “2º Semestre”.

Tabela 2-4 – Proposta de Evolução do Staff do ComDCiber

Ano	Equipe Inicial	1º Semestre	2º Semestre	Equipe Final	Aumento
2023	180	0	45	225	50%
2024	225	60	90	375	67%
2025	375	120	140	635	69%
2026	635	175	200	1.010	59%
2027	1.010	225	250	1.485	47%
2028	1.485	275	300	2.060	39%
2029	2.060	325	350	2.735	33%
2030	2.735	375	390	3.500	28%

Fonte: Compilada pelo autor.

Este crescimento vertiginoso prevê o recrutamento, seleção, absorção, treinamento e operacionalização de pessoal em todos os diferentes setores da ComDCiber. Prevê ainda que, à medida que a estrutura cresça, ela será ainda mais capaz de absorver contingentes maiores em termos absolutos, mas menores em termos relativos. E também considera a necessidade de um crescimento mais acelerado nas fases iniciais para reduzir a lacuna que existe hoje.

2.4.3 A Necessidade de Pessoal Civil

É pacífico que a ciberdefesa deve envolver militares e civis, principalmente (mas não exclusivamente) devido à impossibilidade de encontrar pessoas suficientes com as qualificações necessárias apenas nas fileiras militares. Sobre esse assunto, a principal discussão nos EUA, Reino Unido, França e Alemanha é como captar e reter pessoal civil e utilizá-lo em operações militares.

Quanto à captação, alguns entendem que, a serviço da nação, e fora de uma zona de combate tradicional, há pouca diferença entre estar uniformizado ou não. Para estes, basta

contratar civis diretamente nas Forças Armadas, mesmo que por meio da contratação de empresas terceirizadas, para se chegar ao efetivo necessário, formalizando-se em seus contratos os requisitos de sigilo, hierarquia e disciplina[27]. Outros, com uma visão mais conservadora, entendem que o uniforme e o *ethos* militar também devem ser exigidos dos "ciberguerreiros". Para muitos deles, profissionais civis treinados poderiam ser admitidos, mas apenas como oficiais temporários ou em carreiras não combatentes[28].

Outra questão relevante é a existência de perspectivas de desenvolvimento de carreiras cibernéticas. Isso já foi feito pelo Exército e pelos Fuzileiros Navais dos EUA, que criaram carreiras específicas, garantindo a progressão profissional, embora saibamos que podem não ser carreiras de longo prazo[29].

2.4.3.1 Sobre o Comissionamento de Civis

No sítio da Internet do ArmyCyber dos EUA há um aplicativo online para a candidatura à contratação de pessoal treinado em programação, análise de sistemas ou hacking[30]. Outra página do mesmo sítio oferece a possibilidade de se candidatar ao comissionamento como oficiais do exército[31]. Uma vez aceitos, após um processo de "investigação social" e comprovação de competência técnica, os selecionados passam por uma breve instrução militar (6 semanas) e se tornam oficiais do Exército dos EUA. Da mesma forma, a USAF mantém uma página para o recrutamento de Oficiais de

---

[27] Paul, Porche, and Axelband, "Cyber Forces and U.S. Cyber Command"; Bracknell, "Who Says Cyber Warriors Need to Wear a Uniform?"; Schneider, "Blue Hair In The Gray Zone."

[28] Armstrong, "The US Military Can't Just 'Hire' Cyber Expertise. Here's Why."

[29] Pomerleau, "Why a Long Military Career in Cyber Feels like a Rarity."

[30] US-ArmyCyber, "Careers in Army Cyber."

[31] US-ArmyCyber, "Cyber Direct Commissioning Program."

Operações do Ciberespaço[32] e a Marinha dos EUA oferece outra para recrutar 'engenheiros de guerra cibernética'[33].

Embora o comissionamento possa não ser a forma ideal de recrutamento de civis, ela é facilmente adaptável ao caso brasileiro, onde também há previsão de ingresso regular de oficiais nas carreiras técnicas das Forças Armadas. A remuneração dos militares brasileiros em 2020 correspondia à indicada na Tabela 2-5.

Tabela 2-5 – Salários dos Oficiais Militares Brasileiros

Posto	**Vencimento (BRL)**	**Adicional de Disponibilidade**
Coronel	11.451,00	32%
Tenente-Coronel	11.250,00	26%
Major	11.088,00	20%
Capitão	9.135,00	12%
Primeiro-Tenente	8.245,00	6%
Segundo-Tenente	7.490,00	5%

Fonte: Compilada pelo autor com base na Lei 13.954/2019[34]

Observa-se que o salário constitui a remuneração base, sendo acrescido de abonos, dos quais os mais relevantes são o Adicional de Disponibilidade, "devido a disponibilidade permanente e dedicação exclusiva" e o Adicional de Habilitação, "por cursos realizados com sucesso" ao longo de suas carreiras[35]. O Adicional de Disponibilidade também é indicado na tabela.

---

[32] Apache Software Foundation, "U.S. Air Force - Career Detail - Cyberspace Operations Officer."

[33] US-Navy, "Navy Cyber Warfare Engineer Officer Program."

[34] Brasil-CN, Lei 13.954/2019.

[35] Brasil-CN.

A Tabela 2-6 apresenta o percentual de Adicional de Qualificação de acordo com os cursos realizados, com os acréscimos anuais previstos em lei.

Tabela 2-6 – Adicional de Qualificação

Qualificação/Cursos	**Desde 01/07/20**	**Desde 01/07/21**	**Desde 01/07/22**	**Desde 01/07/23**
Doutorado/Altos Estudos - Categoria I	42%	54%	66%	73%
Doutorado/Altos Estudos - Categoria II	37%	49%	61%	68%
Mestrado/Comando e Estado-Maior	27%	34%	41%	45%
Especialização	19%	22%	25%	27%
Graduação	12%	12%	12%	12%

Fonte: Compilada pelo autor com base na Lei 13.954/2019[36]

Assim, um analista de sistemas com formação em ciência da computação e mestrado, iniciando a carreira de 2º Tenente em 2021, receberia um salário de BRL 7.490,00, acrescido de um Adicional de Disponibilidade de BRL 374,50 (5%) e um Adicional de Qualificação no valor de BRL 2.022,30 (27%), totalizando um salário bruto de BRL 9.886,80. A entrada no mesmo escalão nos anos subsequentes corresponderia a um valor ainda maior, dado o aumento do Adicional de Qualificação previsto para os próximos anos.

Comparada com as condições do mercado brasileiro, essa remuneração é bastante atrativa para os profissionais de TI. O salário médio de mercado para a categoria é bem menor, como pode ser visto em Tabela 2-7.

Considerando o Exército como uma grande empresa, é evidente que não haveria dificuldade em contratar profissionais até o nível de Analista Sênior (8 anos de experiência) comparável a um Capitão, cuja remuneração

[36] Brasil-CN.

bruta seria de BRL 12.697,45. Considerando os demais benefícios proporcionados pela carreira militar (alimentação, transporte, seguro saúde e possivelmente moradia), a atratividade é muito alta.

Tabela 2-7 – Salário Médio Mensal dos Analistas de Sistemas no Brasil

Tamanho da Empresa	**Nível de Experiência**				
	Trainee	**Júnior**	**Pleno**	**Sênior**	**Master**
Experiência (anos)	**<3**	**3-4**	**5-6**	**7-8**	**>8**
Pequena (BRL)	2.492,81	3.116,01	3.895,01	4.868,76	6.085,95
Média (BRL)	3.240,65	4.050,81	5.063,51	6.329,39	7.911,74
Grande (BRL)	4.212,84	5.266,05	6.582,56	8.228,20	10.285,25

Fonte: Compilada pelo autor com dados de TrabalhaBrasil.org[37]

Além disso, o Exército tem a prerrogativa de "convocar e incorporar brasileiros de reconhecida competência técnico-profissional ou de notória cultura científica para o serviço ativo do Exército, de forma voluntária e temporária"[38]. Nessas condições, a atratividade é ainda maior. Comissionado como Major, um graduado em Ciência da Computação, com Doutorado, por exemplo, receberia um salário de BRL 11.088,00, mais um Adicional de Disponibilidade de BRL 2.217,60 (20%) e um Adicional de Qualificação de BRL 4.656,96 (42%), totalizando uma remuneração bruta de BRL 17.962,56. Tal valor é 75% superior à média dos analistas de sistemas Master (mais de oito anos de experiência) em grandes empresas do mercado brasileiro.

Além disso, a impossibilidade de extensão do efetivo do exército imposta pela EC95 não constitui uma restrição *de facto*. Um rearranjo de prioridades permitiria a realocação de Oficiais Técnicos Temporários (OTT) ou do Quadro

[37] Brasil-TrabalhaBrasil, "Salário Para Analista de Sistemas. Media Salarial Paga No Brasil."

[38] Brasil-PR, Decreto 9.637/2018.

Complementar de Oficiais (QCO) das três forças singulares para a ComDCiber. Os OTTs podem ser implantados rapidamente, e mesmo a limitação de oito anos de exercício permite um ciclo de vida razoavelmente longo no âmbito da defesa. Ao final de seu serviço, eles poderiam fortalecer as fileiras de ciberdefesa e cibersegurança no mercado privado ou no setor público civil, continuando a contribuir para a melhoria da ciberdefesa nacional.

2.4.3.2 Cargos Civis

O comissionamento de civis é uma espécie de "conversão rápida" de civis em militares. Mas não interessará a um determinado grupo de profissionais, que prefeririam servir à ciberdefesa permanecendo civis, fugindo das peculiaridades da vida militar, como marchas, formações, testes de aptidão física, e uso de uniformes, dentre outras. Além de ampliar o leque de profissionais disponíveis, a contratação de civis permitiria uma maior continuidade e retenção dos conhecimentos associados à função, dado que os militares, por suas exigências de carreira, são frequentemente deslocados para realizar cursos e missões de comando. Os civis, isentos dessas obrigações, poderiam garantir a estabilidade e continuidade dos processos.

No entanto, há a necessidade de um plano de carreira que permita aos civis ascender na tomada de decisões e posições estratégicas na estrutura de ciberdefesa. Em termos técnicos, isso não é um problema. Entretanto, na prática, essa convivência de militares e civis em funções equivalentes exigirá uma adaptação normativa (e principalmente cultural) nas Forças Armadas. A possível criação da 'Carreira de Estado' de Especialista em Defesa que agora aparece na proposta de END 2020 pode ajudar a preencher essa lacuna[39]. Essa integração civil-militar na ciberdefesa já começou em

[39] Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa," 2020.

outros países, e o ComDCiber pode se beneficiar das experiências de “nações amigas” nesse processo.

2.4.3.3 Criando uma cibercarreira militar

A médio prazo, é preciso criar uma força cibernética, com regras específicas e uma nova cultura. Entretanto, a curto prazo, urge desenvolver cibercarreiras que permitam aos militares de diferentes ramos das diversas forças ascender profissionalmente, evitando que sejam afastados para servir em cargos e funções específicas como requisito dos seus ramos de origem. Uma vez inserido nesta “carreira” (ou quadro), um militar apenas se afastaria temporariamente para cursos técnicos, de estado-maior, de política e de estratégia, como foi feito pelo Exército, Marinha, Corpo de Fuzileiros Navais e Força Aérea dos EUA.

2.5 Onde Localizar o ComDCiber no Contexto do Ministério da Defesa?

Há também a necessidade de considerar o posicionamento do ComDCiber dentro da estrutura do MD. Duas alternativas são mais adequadas do que a atual subordinação ao DCT do Exército.

2.5.1.1 Alternativa 1 – Sob o Estado-Maior Conjunto (EMCFA)

A proposta mais consistente, considerando as experiências dos países do “Arco do Conhecimento” militar, seria a alocação do ComDCiber no Estado-Maior Conjunto (EMCFA), no MD. Essa opção elevaria o status de ciberdefesa, já que não estaria mais vinculada a uma única força, mesmo que o comando continuasse sendo dado permanentemente ao Exército. Isso, em tese, facilitaria a obtenção de recursos, incluindo a realocação de posições de OTT e QCO das forças singulares, além de reduzir dois “níveis” (entre forças e ‘armas’ do Exército) na disputa por recursos. Em termos práticos, não deve representar um

problema para o Exército. Da mesma forma que "perderia" a dotação orçamentária equivalente, também "perderia" a despesa correspondente, sem perder prestígio, pois permaneceria no comando conforme estabelecido pela END.

No entanto, essa opção enfrentará dificuldades de natureza política, dada a incipiente atuação conjunta do MD em seus pouco mais de 20 anos de existência. Embora, mais cedo ou mais tarde, essa ação conjunta tenha que se tornar efetiva. Quanto antes melhor! Além disso, a crescente importância da cibernética no contexto militar internacional pode, inclusive, alavancar o desenvolvimento dessa capacidade de ação conjunta.

2.5.1.2 Alternativa 2 - Adoção do Modelo do Comando de Operações Especiais (COpEsp)

Na impossibilidade momentânea de se ter uma estrutura diretamente ligada ao EMCFA, uma alternativa dentro do próprio Exército seria dotar o ComDCiber de condição semelhante à do COpEsp. De fato, a natureza das operações cibernéticas é, em boa medida, "semelhante" à das operações especiais[40]. São essencialmente dois comandos operacionais. Ambos envolvem o desenvolvimento de doutrinas e técnicas específicas, distintas e complementares às do restante do Exército, o que justifica que tenham "tratamento administrativo" semelhante.

Embora a solução adotada para o COpEsp possa parecer outra jabuticaba, ao menos haveria dois comandos que fariam uso da mesma exceção, e não duas exceções diferentes, uma para cada comando.

[40] Paul, Porche, and Axelband, "Cyber Forces and U.S. Cyber Command."

2.6 Relatório da OEA e Oxford sobre as capacidades cibernéticas brasileiras

Em agosto de 2020, a Organização dos Estados Americanos, o Governo Brasileiro e a Universidade de Oxford publicaram o Cybersecurity Capabilities Review of Brazil[41].

Modelos de maturidade de capacidade são relativamente comuns no contexto cibernético. O mais famoso deles é o CMM/CMMI, desenvolvido pelo renomado Instituto de Engenharia de Software da Carnegie-Melon University (SEI/CMU), que avalia a maturidade do desenvolvimento de software das instituições[42]. Após alguns anos o Brasil adotou um modelo de maturidade próprio, denominado MPS-BR (Melhoria dos Processos do Software Brasileiro), criado em 2003 pela Associação para a Promoção da Excelência do Software Brasileiro (Softex). A opção pelo MPS-BR pareceu mais adequada à realidade nacional, principalmente no que diz respeito aos custos das certificações internacionais[43]. Esses modelos geralmente consideram que quando uma única área-chave de processo (KPA) exigida para um nível não é atingida, esse nível não é totalmente alcançado, com a classificação final sendo aquela para a qual todas as KPAs foram certificadas. Assim, se algum dos requisitos (KPAs) do nível 4 não for atendido, o relatório indica a organização como sendo de nível 3.

Uma leitura cuidadosa do relatório da OEA/Oxford mostra, apesar da linguagem cuidadosamente adotada pelos autores, que o Brasil está em um estágio muito primário em suas capacidades cibernéticas.

---

[41] Oxford GCSCC, “Cybersecurity Capacity Review of Brazil.”

[42] CMMI Institute, “CMMI Institute.”

[43] Softex, “MPS-BR.”

O modelo Oxford prevê 5 “estágios” de capacidade (Start-up, Formative, Established, Strategic, Dynamic). O estágio “Start-up”, no entanto, tem a seguinte descrição:

> neste estágio, **não existe maturidade de segurança cibernética** ou [ela] é de **natureza muito embrionária**. Pode haver discussões iniciais sobre o fortalecimento da capacidade de segurança cibernética, mas **nenhuma ação concreta foi tomada**. Há uma ausência de evidências observáveis de capacidade de segurança cibernética nesta fase.[44]

Consequentemente, os estágios que de fato demonstram alguma capacidade são os quatro seguintes. Para simplificar a análise, neste capítulo, cada etapa será considerada como correspondendo a um número, sendo “Formativo” equivalente a 1, “Estabelecido” correspondendo a 2, “Estratégico” correspondendo a 3 e “Dinâmico” equivalendo a 4, a maior “pontuação” possível.

O modelo considera cinco dimensões, totalizando 24 KPAs (áreas), conforme a Tabela 2-8.

Tabela 2-8 – Dimensões e KPAs do Modelo de Maturidade Oxford GCSCC

Dimensão	Área	Descrição
Estratégia e Política de Cibersegurança	D1.1	Estratégia Nacional de Segurança Cibernética
	D1.2	Resposta a incidentes
	D1.3	Proteção da infraestrutura crítica (IC)
	D1.4	Gerenciamento de crises
	D1.5	Defesa cibernética
	D1.6	Redundância nas comunicações
	D2.1	Mentalidade de segurança cibernética
	D2.2	Confiança na Internet

[44] Oxford GCSCC, “Cybersecurity Capacity Review of Brazil.”

Dimensão	**Área**	**Descrição**
Cultura e Sociedade de Cibersegurança	D2.3	Entendimento do usuário sobre a proteção de informações pessoais on-line
	D2.4	Mecanismos de informação
	D2.5	Mídia e mídia social
Educação, Treinamento e Habilidades em Cibersegurança	D3.1	Conscientização
	D3.2	Estrutura para a educação
	D3.3	Estrutura para a formação profissional
Estruturas Jurídicas e Regulamentares	D4.1	Estruturas jurídicas
	D4.2	Sistema de justiça criminal
	D4.3	Estruturas formais e informais de cooperação para combater o crime cibernético
Padrões, Organizações e Tecnologias	D5.1	Adesão às normas
	D5.2	Resiliência da infraestrutura da Internet
	D5.3	Qualidade do software
	D5.4	Controles técnicos de segurança
	D5.5	Controles criptográficos
	D5.6	Mercado de segurança cibernética
	D5.7	Divulgação responsável

Fonte: Compilada pelo autor com dados do Cybersecurity Capabilities Review of Brazil [45]

Na Avaliação do Brasil, diferentemente do modelo tradicional, há estágios intermediários. Por exemplo, na área D1.1, onde o Brasil foi classificado como “Formativo-Estabelecido”, e não como “Formativo”, como ocorreria numa avaliação usual. Note-se que a avaliação realizada em 2015, com a mesma metodologia, sobre as cibercapacidades do Reino Unido, não contém estes níveis intermédios. No entanto, o gráfico do relatório correspondente indicou níveis

[45] Oxford GCSCC.

intermediários nesse caso também[46]. Trata-se, portanto, de um "ajuste" feito ao modelo após a avaliação realizada no Reino Unido.

A comparação do Brasil com o Reino Unido é justificável, como demonstrado na Seção 2.4.1, considerando a defesa de interesses econômicos de similar magnitude. A avaliação das capacidades brasileiras no relatório da OEA indica que, considerando os estágios "híbridos" ou "intermediários", o Brasil apresenta a situação apresentada em Tabela 2-9.

Tabela 2-9 – Áreas por Estágio nas Capacidades Brasileiras

Estágio	Qtd	%
Formativo	10	42%
Formativo-Estabelecido	7	29%
Estabelecido	6	25%
Estabelecido-Estratégico	1	4%
Estratégico	0	0%
Estratégico-Dinâmico	0	0%
Dinâmico	0	0%

Fonte: Compilada pelo autor com dados do Cybersecurity Capabilities Review of Brazil [47]

Se aplicado o mesmo rigor utilizado na avaliação das capacidades do Reino Unido em 2015, no entanto, os cenários brasileiro e britânico seriam os mostrados na Tabela 2-10.

Tabela 2-10 – Áreas por Estágio nas Capacidades Brasileiras e Britânicas (sem Estágios Híbridos)

Estágio	Qtd	BR	UK
Formativo	17	71%	14%

[46] Oxford GCSCC, "Cybersecurity Capacity Review of the United Kingdom."

[47] Oxford GCSCC, "Cybersecurity Capacity Review of Brazil."

Estabelecido	7	29%	62%
Estratégico	0	0%	14%
Dinâmico	0	0%	10%

Fonte: Compilada pelo autor com dados do Cybersecurity Capabilities Review of Brazil[48] e do Cyber Capabilities Review of the UK[49]

Uma comparação mais fácil é possível utilizando-se os valores numéricos atribuídos como correspondentes aos estágios identificados, e considerando que os estágios híbridos corresponderiam a um aumento de 0,5 ("a virtude está no meio", como afirma um dito popular brasileiro). Usando esse processo, as capacidades brasileiras seriam "pontuadas" conforme apresentado na Tabela 2-11.

Tabela 2-11 – Pontuação de Cada Área das Capacidades Brasileiras

Área	Descrição	Estágio	Pontos
D1.1	Estratégia Nacional de Segurança Cibernética	Formativo-Estabelecido	1.5
D1.2	Resposta a incidentes	Estabelecido-Estratégico	2.5
D1.3	Proteção da infraestrutura crítica (IC)	Estabelecido	2.0
D1.4	Gerenciamento de crises	Estabelecido	2.0
D1.5	Defesa cibernética	Formativo-Estabelecido	1.5
D1.6	Redundância nas comunicações	Formativo	1.0
D2.1	Mentalidade de segurança cibernética	Formativo	1.0
D2.2	Confiança na Internet	Formativo-Estabelecido	1.5
D2.3	Entendimento do usuário sobre a proteção de informações pessoais on-line	Formativo	1.0
D2.4	Mecanismos de informação	Formativo	1.0
D2.5	Mídia e mídia social	Formativo	1.0

[48] Oxford GCSCC.

[49] Oxford GCSCC, "Cybersecurity Capacity Review of the United Kingdom."

Área	Descrição	Estágio	Pontos
D3.1	Conscientização	Formativo-Estabelecido	1.5
D3.2	Estrutura para a educação	Formativo	1.0
D3.3	Estrutura para a formação profissional	Formativo	1.0
D4.1	Estruturas jurídicas	Estabelecido	2.0
D4.2	Sistema de justiça criminal	Formativo	1.0
D4.3	Estruturas formais e informais de cooperação para combater o crime cibernético	Formativo	1.0
D5.1	Adesão às normas	Formativo-Estabelecido	1.5
D5.2	Resiliência da infraestrutura da Internet	Estabelecido	2.0
D5.3	Qualidade do software	Formativo	1.0
D5.4	Controles técnicos de segurança	Estabelecido	2.0
D5.5	Controles criptográficos	Estabelecido	2.0
D5.6	Mercado de segurança cibernética	Formativo-Estabelecido	1.5
D5.7	Divulgação responsável	Formativo-Estabelecido	1.5

Fonte: Compilada pelo autor com dados do Cybersecurity Capabilities Review of Brazil[50]

Disso resulta uma média de 1,5 pontos, ou o equivalente ao estágio híbrido “Formativo-Estabelecido” ou, no caso do rigor original, o estágio “Formativo”. Além disso, sem as etapas “híbridas”, no rigor da metodologia original, a média brasileira corresponderia a 1,3.

O Reino Unido, por sua vez, em 2015, seria “pontuado” como mostrado na Tabela 2-12

Tabela 2-12 – Pontos de Cada Área das Capacidades do Reino Unido

Área	Descrição	Estágio	Pontos
D1.1	Estratégia Nacional de Segurança Cibernética	Estratégico	3.0
D1.2	Resposta a incidentes	Estabelecido	2.0

[50] Oxford GCSCC, “Cybersecurity Capacity Review of Brazil.”

Área	Descrição	Estágio	Pontos
D1.3	Proteção da infraestrutura crítica (IC)	Estabelecido	2.0
D1.4	Gerenciamento de crises	Estabelecido	2.0
D1.5	Defesa cibernética	Estabelecido	2.0
D1.6	Redundância nas comunicações	Estabelecido	2.0
D2.1	Mentalidade de segurança cibernética	Formativo	1.0
D2.2	Confiança na Internet	Estabelecido	2.0
D2.3	Entendimento do usuário sobre a proteção de informações pessoais on-line	Formativo	1.0
D2.4	Mecanismos de informação	Estabelecido	2.0
D2.5	Mídia e mídia social	N/A	N/A
D3.1	Conscientização	Estabelecido	2.0
D3.2	Estrutura para a educação	Estabelecido	2.0
D3.3	Estrutura para a formação profissional	Estabelecido	2.0
D4.1	Estruturas jurídicas	Dinâmico	4.0
D4.2	Sistema de justiça criminal	Estratégico	3.0
D4.3	Estruturas formais e informais de cooperação para combater o crime cibernético	Formativo	1.0
D5.1	Adesão às normas	Estabelecido	2.0
D5.2	Resiliência da infraestrutura da Internet	Estabelecido	2.0
D5.3	Qualidade do software	Estabelecido	2.0
D5.4	Controles técnicos de segurança	Dinâmico	4.0
D5.5	Controles criptográficos	Estratégico	3.0
D5.6	Mercado de segurança cibernética	N/A	N/A
D5.7	Divulgação responsável	N/A	N/A

Nota: N/A indica que a área não foi avaliada nessa versão da metodologia, ou que fazia parte de outra área.

Fonte: Compilada pelo autor com dados do Cybersecurity Capabilities Review of the United Kingdom[51]

[51] Oxford GCSCC, "Cybersecurity Capacity Review of the United Kingdom."

O “score” britânico, então, correspondeu a uma média de 2,2 (mesmo sem o “incremento” proporcionado pelas etapas híbridas).

Em outras palavras, em 2015 o Reino Unido já tinha cibercapacidades muito melhores do que as do Brasil em 2020. E, como visto, nesses cinco anos eles investiram em média BRL 1,35 bilhões anualmente, enquanto a média brasileira no mesmo período foi de apenas BRL 15 milhões. Uma taxa nominal de 90:1, mas se considerado que o PIB-PPP brasileiro é 11% maior que o britânico, a razão real entre os investimentos pode ser arredondada para 100:1.

Por parte do Reino Unido, pode-se supor que os significativos investimentos realizados por aquele país nos últimos anos, em sentido contrário ao que ocorre no Brasil, acentuou ainda mais a lacuna tecnológica que o separa do Brasil. E como se sabe, não se coloca alarme no carro para evitar que ele seja roubado; se o ladrão quiser levá-lo, ele o fará; há um efeito dissuasor no alarme, mas é o de fazer com que o ladrão, motivado pela “lei do menor esforço”, procure um carro semelhante mais fácil de roubar.

2.7 Sobre as Boas Novas

Há algumas boas notícias, também. A legislação brasileira exige autorização do Comandante Supremo para a implantação de capacidades militares em nome do Estado. Isso geralmente é autorizado por um decreto presidencial dentro de um período limitado. Comandos conjuntos específicos, no entanto, podem ter uma autorização “permanente” para o engajamento. Há décadas esse é o caso do Comando de Defesa Aérea do Brasil (COMAE). Em novembro de 2020, uma portaria do MD abriu caminho para que o ComDCiber também se tornasse “permanentemente ativado”. O MD agora aguarda por uma consideração presidencial, possivelmente resultando no necessário decreto.

Além disso, conversas com o ComDCiber em 2020 indicaram que a parte conjunta do orçamento do comando seria multiplicada por um fator de dez vezes, elevando o orçamento total de cerca de BRL 21 milhões para cerca de BRL 74 milhões, de acordo com proposta orçamentária em discussão no Governo e Congresso.

Essas duas mudanças constituem passos muito significativos na direção certa para a evolução da ciberdefesa brasileira. No entanto, comparativamente, elas ainda são bastante tímidas.

2.8 Conclusão

O ciberespaço, inequivocamente, constitui-se como um novo espaço de coação interestatal e de política. Mesmo países com cultura e tradição não-agressivas, que favorecem a solução pacífica de controvérsias, e que estão dispostos a renunciar às vantagens competitivas oferecidas pelo potencial ofensivo do ciberespaço, não podem alimentar a expectativa de que seus pares façam o mesmo.

A ação de Estados no ciberespaço é real, acontece diariamente, envolve significativos interesses econômicos, estratégicos e geopolíticos, é global, ignora o tradicional campo de batalha e está crescendo. Muitas nações já operam no dia a dia, ao mesmo tempo em que ampliam seus conhecimentos, arsenais e respaldo jurídico.

O Brasil precisa estar adequadamente preparado o quanto antes, e os resultados das pesquisas realizadas mostram que o progresso do Brasil nessa área é muito lento quando comparado ao de nações com interesses econômicos e geopolíticos semelhantes, e até mesmo de “potências menores” como Austrália, Israel, Irã e Coréia do Norte.

As conclusões e proposições deste Capítulo apontam para um caminho coerente, baseado em dados e conceitos sólidos, coletados em ampla pesquisa sobre as práticas de diferentes países, para proporcionar uma abordagem científica

sobre um tema tão controverso quanto contemporâneo.

2.9 Referências

Amin, Espiridião. “Relatório de Avaliação de Política Pública: A Política Nacional Sobre Defesa Cibernética.” Brasília, 2019.

Apache Software Foundation. “U.S. Air Force - Career Detail - Cyberspace Operations Officer.” airforce.com, n.d. https://www.airforce.com/careers/detail/cyberspace-operations-officer.

Armstrong, James. “The US Military Can’t Just ‘Hire’ Cyber Expertise. Here’s Why.” Modern War institute, 2018. https://mwi.usma.edu/us-military-cant-just-hire-cyber-expertise-heres/.

Australia. “Australia’s Cyber Security Strategy 2020,” 2020.

Barlouet, Alain. “La France Muscle Sa Cyberdéfense.” *Le Figaro*. 2016.

Bracknell, Butch. “Who Says Cyber Warriors Need to Wear a Uniform?” Modern War Institute, 2018. https://mwi.usma.edu/says-cyber-warriors-need-wear-uniform/.

Brangetto, Pascal. *National Cyber Security Organisation: France*, 2015.

Brasil-CN. Lei 13.954/2019 (2019). http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13954.htm.

———. “Relatório Da CPI Da Espionagem Eletrônica Do Senado Federal.” Brasília, 2014.

Brasil-MD. “Exército Brasileiro - Organograma.” Exército Brasileiro - Organograma, 2020. http://www.eb.mil.br/organograma.

———. “Política Nacional de Defesa e Estratégia Nacional de Defesa.” Brasília, 2016.

———. “Política Nacional de Defesa e Estratégia Nacional de Defesa.” Brasília, 2020.

Brasil-PR. Decreto 9.637/2018 (2018).

Brasil-TrabalhaBrasil. “Salário Para Analista de Sistemas. Media Salarial Paga No Brasil.” TrabalhaBrasil.com.br, 2020. https://www.trabalhabrasil.com.br/media-salarial-para-analista-de-sistemas.

CMMI Institute. “CMMI Institute.” CMMI Institute website, n.d. https://cmmiinstitute.com/.

DefesaNet. “Aviação Do Exército - Exército Recria Aviação de Asas Fixas e FAB Critica.” *DefesaNet*. 2020. https://www.defesanet.com.br/avex/noticia/37078/Exercito-recria-aviacao-de-asas-fixas-e-FAB-critica/.

———. “Aviação Do Exército - Urgente - Revogado Decreto Sobe a Aviação Do Exército.” *DefesaNet*. 2020. https://www.defesanet.com.br/avex/noticia/37089/Urgente---Revogado-Decreto-sobe-a-Aviacao-do-Exercito/.

GlobalFirepower.com. “2020 Military Strength Ranking.” Global Firepower Index, 2020. https://www.globalfirepower.com/countries-listing.asp.

Hayden, Michael. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: The Penguin Press, 2016.

Haynes, Deborah. “Britain to Create 2,000-Strong Cyber Force to Tackle Russia Threat | UK News | Sky News.” *SkyNews*, 2018. https://news.sky.com/story/britain-to-create-2-000-strong-cyber-force-to-tackle-russia-threat-11503653.

Marks, Joseph. “At 7 Years Old, CYBERCOM Becomes a Full Combatant Command - Defense One.” *Defense One*, 2017.

Okamura, Ângelo. “Abertura Do V Seminário Internacional de Defesa Cibernética.” Brasília, 2017. https://cryptoid.com.br/eventos/v-seminario-internacional-de-defesa-cibernetica/.

Osborne, George. “Chancellor’s Speech to GCHQ on Cyber Security.” *Gov.Uk*, 2015, 1–12. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

Osula, Anna-Maria. *National Cyber Security Organisation: United Kingdom*, 2015.

Oxford GCSCC. “Cybersecurity Capacity Review of Brazil,” 2020.

———. “Cybersecurity Capacity Review of the United Kingdom,” 2016. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity Capacity Review of the United Kingdom.pdf.

Paganini, Pierluigi. “The British Army Creates the 77th Battalion.” *Security Affairs*, 2015.

Paul, Christopher, Isaac Porche, and Elliot Axelband. “Cyber Forces and U.S. Cyber Command.” In *The Other Quiet Professionals*. RAND Corporation, 2014. https://doi.org/10.4135/9781452229300.n1568.

Pernik, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss. *National Cyber Security Organisation: UNITED STATES*, 2016.

Pomerleau, Mark. “Why a Long Military Career in Cyber Feels like a Rarity.” *FifthDomain*, 2018.

Raud, Mikk. *China and Cyber: Attitudes, Strategies, Organisation*. NATO CCDCOE, 2016.

Sabbagh, Dan. “UK to Launch Specialist Cyber Force Able to Target Terror Groups.” *The Guardian*, 2020.

Schneider, Jacquelyn. “Blue Hair In The Gray Zone.” *War On The Rocks*, 2018.

Schulte, Sebastian. “German Cyber Command Becomes Operational.” *Jane’s*, no. 06 abr. (2017).

Softex. “MPS-BR.” MPS-BR Website, n.d. https://softex.br/mpsbr/.

Stokes, Mark. “The PLA General Staff Department Third Department Second Bureau,” 2015.

United Kingdom. “Cyber Security Strategy,” 2016. http://www.gov.uk/government/publications/cyber-security-strategy.

US-ArmyCyber. “Careers in Army Cyber.” goarmy.com, n.d. https://www.goarmy.com/army-cyber/careers-in-army-cyber.html.

———. “Cyber Direct Commissioning Program.” goarmy.com, n.d. https://www.goarmy.com/army-cyber/cyber-direct-commissioning-program.html.

———. “DOD FACT SHEET: Cyber Mission Force > U.S. Army Cyber Command > Fact Sheets.” U.S. Army Cyber Command, 2020. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

US-Navy. “Navy Cyber Warfare Engineer Officer Program.” NavyCyberSpace (navycs.com), n.d. https://www.navycs.com/officer/cyberwarfareengineer.html.

3 Quando 1+1 Não São 2

Foi somente em fevereiro de 2020 que o Brasil publicou sua primeira estratégia nacional de cibersegurança (e-Ciber). Foi a penúltima entre as 15 maiores economias. Além de atrasada, a e-Ciber trouxe uma peculiaridade: é a única estratégia que trata apenas de cibersegurança, explicitamente excluindo a ciberdefesa. Utilizando as lentes da cultura estratégica brasileira, este capítulo analisa peculiaridades do documento brasileiro. Mostra-se que essas idiossincrasias, ao invés de derivarem de um processo de securitização, como muitas vezes se afirma, têm suas raízes na forma como a sociedade brasileira percebe as questões de segurança e defesa nacional, refletindo nas escolhas políticas e estratégicas dos tomadores de decisão, com impactos sobre as capacidades nacionais a médio e longo prazos. A análise também mostra que, apesar de abordar vários temas importantes e apontar objetivos e possíveis linhas de ação, a e-Ciber é pouco determinista na alocação de recursos e responsabilidades para a execução dessas ações. Isso indica que o Brasil deve permanecer por algum tempo sem capacidades de ciberdefesa e cibersegurança compatíveis com as de seus pares.

3.1 Introdução

O Brasil tem o quinto maior território, a sexta população, a oitava economia (cerca de 11% que a do Reino Unido e 14% maior que a francesa, comparando a Paridade de Poder de Compra) e a nona força militar mais poderosa do mundo[1]. E, segundo a e-Ciber, é a segunda maior vítima de crimes cibernéticos no mundo. Não obstante, a cibersegurança do país é frequentemente negligenciada na literatura internacional.

---

[1] GlobalFirepower.com, “2021 Military Strength Ranking.”

Em 2010, o Brasil parecia estar no mesmo ritmo de muitos de seus pares em cibersegurança. Após a publicação de *Cyberwar*[2] e na esteira das primeiras revelações do Stuxnet, o Exército Brasileiro criou o núcleo de seu Centro de Defesa Cibernética, enquanto o Gabinete de Segurança Institucional da Presidência da República (GSI) publicou o Livro Verde de Segurança Cibernética[3].

Mesmo neste estágio inicial de desenvolvimento de capacidades cibernéticas, no entanto, alguns acadêmicos afirmavam que o Brasil estava securitizando o ciberespaço[4].

No entanto, foi apenas dez anos depois que o Brasil publicou sua primeira estratégia nacional para o cibernético, batizada de e-Ciber. Foi o penúltimo país a fazê-lo entre as 15 maiores economias: Estados Unidos, China, Japão, Alemanha, Índia, Reino Unido, França, Itália, Brasil, Canadá, Rússia, Coreia do Sul, Espanha, Austrália e México[5].

Os brasileiros costumam usar a palavra *jabuticaba* (ou *jaboticaba*), nome de uma fruta só encontrada ali, para indicar algo único, peculiar do país. A e-Ciber trouxe uma enorme jabuticaba em seu escopo: excluiu explicitamente a ciberdefesa, supostamente focando na cibersegurança. Mas essa não é a única idiossincrasia presente nas medidas cibernéticas brasileiras, como será demonstrado. Mostraremos também que muitas delas se relacionam com aspectos particulares da cultura nacional.

---

[2] Clarke and Knake, *Cyber War: The next Threat to National Security and What to Do about It*.

[3] Mandarino and Canongia, *Livro Verde Segurança Cibernética No Brasil*.

[4] Lobato and Kenkel, “Discourses of Cyberspace Securitization in Brazil and in the United States”; Vales, “Is There a Way to Desecuritise Cyberspace? How Brazil’s Legal Framework for the Internet Could Have Done That”; Hurel and Lobato, “Uma Estratégia Para a Governança Da Segurança Cibernética No Brasil.”

[5] IMF, “World Econ. Outlook Database.”

Por que demorou tanto para o Brasil lançar sua primeira Estratégia Nacional de Segurança Cibernética (e-Ciber) e por que ela se concentrou na cibersegurança e deliberadamente ignorou a ciberdefesa? Para responder a essa pergunta, este capítulo defende que a e-Ciber, mais do que resultar de um processo de securitização do ciberespaço, como muitas vezes se afirma, resulta de uma cultura estratégica muito brasileira em questões de defesa e segurança, que evita o desenvolvimento do 'poder duro' (*hard power*) e sua utilização como um instrumento de estadismo (statecraft). Para demonstrá-la, a primeira seção aborda os fundamentos do conceito de cultura estratégica. Uma segunda seção apresenta brevemente as origens da cultura estratégica (e do "institucionalismo histórico") que moldou o "jeitinho brasileiro" do poder militar. Uma terceira explora a evolução doutrinária e jurídica nacional dos conceitos de segurança e defesa. A quarta analisa os impactos da cultura estratégica brasileira na ciberdefesa e na cibersegurança. A quinta seção explora as características da e-Ciber. O capítulo mostra que, como preconizado pelos teóricos da cultura estratégica, nem mesmo novas tecnologias como as do ciberespaço podem escapar da cultura e tradição de uma sociedade.

3.2 Sobre Segurança e Defesa

Esta seção analisa a argumentada securitização do ciberespaço no Brasil. Antes, porém, examina os princípios da teoria da securitização e a visão histórica e doutrinária brasileira sobre segurança e defesa.

3.2.1 A Distinção Clássica e a Fusão da Securitização

Tradicionalmente, os Estados ofereciam duas maneiras diferentes de proteger seus cidadãos e interesses. A proteção contra ameaças externas constituía defesa, dever das Forças Armadas, enquanto a proteção contra ameaças internas constituía segurança, atribuída às polícias. Recentemente, no

entanto, é cada vez mais difícil distinguir entre defesa e segurança. O processo de *securitização* fez com que questões tradicionalmente alheias à defesa ou segurança passassem a receber atenção especial dos Estados-nação, com uma politização ampliada de temas específicos e a alocação de recursos e meios extraordinários para sua mitigação, em nome da *segurança nacional*[6].

A maioria dos arranjos feitos pelas potências médias estaria subordinada a temas internacionais securitizados por aqueles que estão no centro do sistema[7]. As Cruzadas e a Guerra Global ao Terror seriam exemplos de "macrossecuritização", processo de securitização em larga escala no sistema internacional, promovido por atores centrais do sistema e envolvendo outros atores regionais[8].

3.2.2 A Fusão da Defesa e Segurança Nacionais na Guerra Fria

Em consonância com a macrossecuritização, os arranjos de securitização durante a Guerra Fria são enquadrados pelo confronto entre Oriente e Ocidente, principalmente um embate entre o capitalismo, defendido pelo Ocidente (EUA, Europa Ocidental e Japão), e o comunismo, apoiado pelo Oriente (URSS e a República Popular da China)[9].

Nesse processo, argumenta-se, as grandes potências intensificaram sua interferência nos assuntos internos das potências menores. A URSS expôs claramente seu interesse em levar "a revolução" a todos os cantos do globo, no início

---

[6] Buzan, Wæver, and Wilde, *Security: A New Framework for Analysis*.

[7] Buzan and Wæver, "Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory."

[8] Buzan and Hansen, *The Evolution of International Security Studies*.

[9] Buzan and Wæver, "Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory."

abertamente (iniciativas Komintern e Kominform), e depois de forma mais discreta, mas permanente.

O Ocidente capitalista, ao seu lado (principalmente os EUA), sentiu-se no direito de intervir diretamente onde quer que a ameaça comunista estivesse presente. Henry Kissinger, Conselheiro de Segurança Nacional do Presidente Nixon, referindo-se à eleição de Salvador Allende no Chile em 1971, materializou claramente esta premissa:

> "As questões são muito importantes para que os eleitores chilenos decidam por si mesmos… veja, por que precisamos ficar parados e ver um país se tornar comunista devido à irresponsabilidade de seu povo?"[10].

A interferência externa levou várias nações a fazer da luta contra o comunismo uma questão de "segurança nacional". Muitas vezes envolvendo suas forças armadas. No Brasil, Argentina, Chile, Paraguai e Uruguai, para citar alguns, governos eleitos foram depostos e substituídos por regimes militares. Suas forças armadas foram amplamente utilizadas para conter a ameaça comunista, perseguindo, prendendo, torturando e até executando "elementos subversivos", terroristas ou guerrilheiros. Isso teria profundas repercussões na cultura desses países, de modo que ainda hoje há uma grande dificuldade em dotar suas Forças Armadas dos meios necessários para a defesa devido à falta de uma percepção clara de quem seria o inimigo a ser combatido[11]. Essa situação persiste nos últimos anos, pois a maioria das elites políticas desses países foi, em maior ou menor grau ou proximidade, afetada pela repressão naquele momento.

---

[10] Fagen, "The United States and Chile: Roots and Branches"; Lewys, "The Kissinger Doctrine."

[11] Saint-Pierre, "'Defesa' Ou 'Segurança'?: Reflexões Em Torno de Conceitos e Ideologias."

3.2.3 A Institucionalização da Defesa e Segurança no Brasil

Coincidência ou não, a doutrina militar brasileira, expressa pela Escola Superior de Guerra (ESG), não define segurança e defesa em termos de ameaças externas ou internas. A ESG, *think tank* do Ministério da Defesa criado em 1950, foi muito influente durante o regime militar do Brasil. Três dos cinco presidentes militares passaram por ela. A doutrina da ESG estabelece que a segurança "é a garantia necessária e indispensável de uma sociedade e de cada um dos seus membros, contra ameaças *de qualquer natureza*"[12]. Também afirma que "Segurança é uma sensação, enquanto Defesa é ação"[13].

Significativamente, estabelece que a insegurança pode "assumir formas muito sutis, como aquelas decorrentes da intrusão indevida de culturas externas que atacam a identidade cultural nacional".[14]. A defesa é a mitigação dessas ameaças, que podem vir de fatores sociais, políticos ou culturais, internos e externos. Emblematicamente, afirma que "Defesa Nacional é o conjunto de atitudes, medidas e ações do Estado [...] contra ameaças **predominantemente externas**, potenciais ou manifestas"[15].

A fusão doutrinária de segurança e defesa é ainda mais explícita:

> Tendo em vista a origem das ameaças, a Segurança Nacional deve ser analisada em duas vertentes: Externa e Interna.
>
> Quando advindas de ameaças de qualquer origem, forma ou natureza, localizadas no ambiente das relações internacionais, a

---

[12] Brasil-MD, *Manual Básico Vol. 1*.

[13] Brasil-MD.

[14] Brasil-MD.

[15] Brasil-MD.

> Segurança Nacional será buscada por meio de ações de Defesa Externa. Diante de ameaças que possam se manifestar ou produzir efeitos dentro do país, esta é a Defesa Interna.[16]

Portanto, dentro da Segurança Nacional, pode haver Defesa Externa e Defesa Interna. Assim, doutrinariamente, o Brasil não diferencia defesa e segurança no contexto de ameaças externas ou internas.

A Constituição brasileira, em seu artigo 144, estabelece que a segurança pública é exercida pelas polícias federal e estadual. No entanto, o artigo 142 afirma que as Forças Armadas "são destinadas a defender a Pátria, garantir os poderes constitucionais e, por iniciativa de qualquer desses poderes, garantir a lei e a ordem"[17]. Assim, as forças armadas podem ser empregadas para garantir a lei e a ordem por iniciativa de qualquer poder constitucional.

3.2.4 A Securitização pós-Guerra Fria

Desde o fim da Guerra Fria, Europa e América do Sul são, respectivamente, as duas áreas mais pacíficas do planeta, sem a ocorrência de grandes conflitos interestatais[18]. Na União Europeia, a ausência (pelo menos momentânea) de um inimigo externo percebido e a lógica da securitização foram argumentos para justificar o uso das Forças Armadas e agências nacionais de inteligência, juntamente com as forças de segurança pública, para controlar atividades como o terrorismo , crimes transnacionais, ou mesmo migrações humanas: dois tornam-se um [19].

---

[16] Brasil-MD.

[17] Brasil-CN, Constituição Federal de 1988.

[18] Herz, "Concepts of Security in South America"; Franchi, Migon, and Villarreal, "Taxonomy of Interstate Conflicts: Is South America a Peaceful Region?"

[19] Bigo, "When Two Become One: Internal and External Securitisations in Europe."

Processo semelhante ocorreu no Brasil. Desde 2010 (com a ocupação do Complexo do Alemão), as Forças Armadas brasileiras têm se engajado ostensivamente e cada vez mais na segurança pública, culminando com a Intervenção Federal no Estado do Rio de Janeiro em 2018. O prestígio das Forças Armadas, a sensação de insegurança da população, o fracasso de outros mecanismos de segurança interna, bem como a necessidade de apresentar respostas de apelo público no curto prazo, também pesaram, levando os governantes à decisão de utilizar os militares regularmente nas ações de segurança[20].

Durante anos, a relutância militar em se engajar na segurança pública se concentrou na falta de respaldo legal em caso de acusação: se um militar, envolvido em combate de rua, ferisse ou matasse cidadãos civis, criminosos ou não, ele enfrentaria a justiça comum. Uma lei[21] aprovada em outubro de 2017 determinou que esses casos passassem a ser julgados pela justiça militar. Proposta ao Congresso no início de 2016, essa lei pretendia dar suporte legal aos militares envolvidos na segurança das Olimpíadas do Rio, em julho daquele ano. Ainda assim, só foi aprovada mais de um ano após o encerramento dos jogos, exemplificando a falta de atenção do Congresso às questões militares, mesmo quando envolvem a segurança de eventos internacionais.

As próprias forças armadas brasileiras aparentemente buscam justificar investimentos participando de ações de segurança, como visto em dois programas estratégicos do Exército. A Escritório de Gestão de Projetos do Exército Brasileiro (EPEX) descreve a principal diretriz do Sistema Integrado de Monitoramento de Fronteiras (SISFRON) como "a atuação integrada dos órgãos de segurança pública, Forças

---

[20] Saint-Pierre, "'Defesa' Ou 'Segurança'?: Reflexões Em Torno de Conceitos e Ideologias."

[21] Law 13,491/2017.

Armadas e Receita Federal, além de outros órgãos de segurança federais, estaduais e municipais"[22]. Na mesma linha, em relação ao programa de Defesa Cibernética, afirma:

> O programa também contribuirá para aumentar a capacidade nacional de combate ao **cibercrime**, vinculado a ameaças transnacionais, por meio da integração das ações do MD [Ministério da Defesa], das Forças Armadas e dos órgãos governamentais envolvidos nessas atividades.[23]

Em meio a essa névoa conceitual entre segurança e defesa, o Brasil vive hoje um cenário paradoxal. Como herança do regime militar, tem as forças armadas mais potentes da América do Sul[24]. No entanto, devido à ausência de uma ameaça externa concreta e perceptível, a sociedade brasileira não entende claramente a necessidade de investimentos nas Forças Armadas, tornando-as gradativamente obsoletas e subequipadas.

Além disso, há uma desconfiança histórica em relação às intervenções militares no ambiente político, particularmente o regime militar. Muitos daqueles então considerados "elementos subversivos" hoje em dia estão em posições políticas ou midiáticas proeminentes. Isso dificulta muito a negociação de orçamentos e de questões legais afetas aos militares. Sintomática, talvez até emblemática, é a tentativa de "escapar" da terminologia daquele período. Enquanto antes haveria uma Estratégia de Defesa Nacional, onde 'nacional' era a defesa, hoje existe a Estratégia Nacional de Defesa, onde 'nacional' é a estratégia. Mesmo a Política Nacional de Defesa, que, segundo a legislação, deveria se chamar Política de

---

[22] Brasil-MD-EPEX, "Integrando Capacidades Na Vigilância e Na Atuação Em Nossas Fronteiras."

[23] Brasil-MD-EPEX, "Programa Da Defesa Cibernética Na Defesa Nacional."

[24] GlobalFirepower.com, "2021 Military Strength Ranking."

Defesa Nacional, adota um 'nome artístico' menos associado ao período[25].

Nesse contexto, os chamados "documentos de defesa" – Política Nacional de Defesa (PND), Estratégia Nacional de Defesa (END) e Livro Branco de Defesa Nacional (LBDN) – são legalmente obrigados a serem submetidos ao Congresso a cada quatro anos[26]. O Ministério da Defesa os apresentou em 2008-2009, 2012 e 2016. A versão de 2012 nunca foi discutida pelo Congresso, enquanto a de 2016 só foi aprovada em dezembro de 2018[27]. A versão 2020 enviada ao Congresso em 22 de julho ainda não foi apreciada.

Nem mesmo os projetos dos setores estratégicos determinados desde 2008 pela END para cada força armada avançam adequadamente. Para a Força Aérea, o programa espacial brasileiro enfrenta sucessivos atrasos e cortes. A Base de Lançamento de Alcântara não lança foguetes desde o acidente com o Veículo Lançador de Satélites VLS-3 em 2003[28].

Para a Marinha, o Programa Submarino Nuclear (PROSUB) avança lentamente. Ainda assim, para isso, a Marinha sacrifica a manutenção de sua frota de superfície. Com mais de 9.000 quilômetros de costa, o Brasil tem apenas sete fragatas e duas corvetas, a maioria com mais de 30 anos, e algumas atracadas por falta de peças de reposição. Como sua vida útil é limitada a meados desta década, as fragatas serão

---

[25] Brasil-CN, Lei Complementar 97; Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa."

[26] Brasil-CN, Lei Complementar 97.

[27] Notícias, "Aprovadas Em Plenário Novas Política e Estratégia Nacional de Defesa."

[28] D'Alama, "Tragédia Em Alcântara Faz Dez Anos e Brasil Ainda Sonha Em Lançar Foguete"; Maltchiik, "Brasil Deve Lançar Foguete No Espaço Em 2019."

substituídas por corvetas, menores, mais baratas e com menor poder de fogo[29].

Para o Exército, o programa cibernético ainda está engatinhando. O Comando de Defesa Cibernética (ComDCiber), criado em 2015, conta com cerca de 180 militares. A França, por exemplo, com uma economia de porte semelhante, um contingente menor em suas Forças Armadas e uma população inferior a um terço da brasileira, tem um efetivo de mais de 3.600 integrantes em ciberdefesa[30]. A Escola Nacional de Defesa Cibernética do Brasil (ENaDCiber), prevista para entrar em operação em 2017, só teve início em 2019[31].

Assim, aqueles que reivindicavam uma possível mudança na cultura estratégica brasileira a partir de uma aparente intenção de aumentar o 'poder duro'(*hard power*) nacional, como Degaut[32], agora observam a prevalência da antiga cultura. Desde 2018, de fato, o Brasil reduziu significativamente até mesmo sua participação em operações de consolidação e manutenção da paz, por muito tempo consideradas parte importante da tentativa de inserção internacional do país[33].

---

[29] US-Navy, "Marinha Vai Substituir Fragatas Por Corvetas, Revela Alm. Ivan Taveira"; GlobalFirepower.com, "2021 Military Strength Ranking."

[30] Malagutti, "Estruturas de Ciberdefesa Em Diferentes Países."

[31] Okamura, "Abertura Do V Seminário Internacional de Defesa Cibernética"; Brasil-MD, "Escola Nacional de Defesa Cibernética é Inaugurada Em Brasília."

[32] Degaut, "Brazil's Military Modernization: Is a New Strategic Culture Emerging?"

[33] Brasil-MD, "Missões de Paz."

3.3 Impactos na Ciberdefesa e Cibersegurança Brasileiras

EUA, China, França, Reino Unido e Alemanha são comumente citados como superpotências cibernéticas. Para sua ciberdefesa, a Alemanha optou por um novo ramo de suas forças armadas. A China por um comando estratégico. Os EUA, o Reino Unido e a França[34] criaram comandos conjuntos reunindo pessoal de seus diversos serviços militares, subordinados ao Estado-Maior Conjunto ou similar. Conceitualmente, um comando conjunto é subordinado ao Chefe de Governo, ao Ministério da Defesa, ou pelo menos ao Estado-Maior Conjunto, alternando os comandantes entre os ramos e garantindo maior coesão dos esforços de defesa. Em todos esses países, o comando da ciberdefesa é exercido por um general de quatro estrelas. Além disso, todos eles integram suas forças cibernéticas com suas agências de Inteligência de Sinais (SIGINT)[35].

O Brasil, diferentemente, optou por um 'comando conjunto' sob uma única Força, o Exército. Além disso, dentro do Exército, o ComDCiber está subordinado à Diretoria de Ciência e Tecnologia (DCT), órgão de pesquisa e desenvolvimento, e não a um dos comandos operacionais da Instituição[36]. Finalmente, o ComDCiber é um comando de General de Divisão (três estrelas). Possivelmente devido ao seu quadro de funcionários relativamente minúsculo em relação aos dos países mencionados. Uma discussão detalhada do tamanho relativo adequado pode ser encontrada no Capítulo 2 e alhures[37]. Ali, uma comparação com países com interesses

---

[34] Em abril de 2018, a França anunciou sua intenção de criar uma "quarta força".

[35] Malagutti, "Estruturas de Ciberdefesa Em Diferentes Países."

[36] Brasil-MD, "Exército Bras. - Organograma."

[37] Malagutti, "O Necessário Upgrade Na Ciberdefesa Brasileira."

nacionais comparáveis, como Reino Unido, França, Austrália e Itália, com base em parâmetros diversos aponta que o Brasil deveria dispor de mais de 3.000 integrantes em seu Comando de Defesa Cibernética.

Apesar dessas (graves) limitações, os críticos argumentaram que a alocação de recursos do Brasil deveria se concentrar na cibersegurança, não na ciberdefesa, já que o país sofre o segundo maior número de crimes cibernéticos do mundo[38]. Não obstante o fato já mencionado de que o próprio Exército Brasileiro indica que o ComDCiber ajudará no combate ao cibercrime, a história de sucesso do Comando comumente se refere à 'proteção de grandes eventos', como a Conferência do Clima Rio+20 2012, a Copa do Mundo FIFA 2014 e os Jogos Olímpicos do Rio 2016, só para citar alguns[39].

Mais uma vez, a maior visibilidade dos aspectos de segurança aduz a percepções de maior urgência do que questões de defesa. A despeito dos três episódios mais midiáticos envolvendo o ciberespaço (WikiLeaks, Stuxnet e Snowden) se refiram a ciberofensas patrocinadas por Estado. O WikiLeaks mostrou milhares de mensagens diplomáticas dos EUA sobre vários países, incluindo o Brasil. O Stuxnet, apesar de infectar instalações brasileiras, não causou danos (mas muitas preocupações!), já que visava especificamente a instalação nuclear iraniana de Natanz. No caso Snowden, a espionagem dos EUA envolvendo a presidente brasileira e a maior empresa do país, a Petrobras, ficou evidente[40].

---

[38] Diniz, Muggah, and Glenny, "Deconstructing Cyber Security in Brazil: Threats and Responses"; Muggah and Thompson, "Brazil Must Rebalance Its Approach to Cybersecurity."

[39] Caiafa, "10 Perguntas Para o General Okamura, Comandante Da Defesa Cibernética Do Exército Brasileiro."

[40] Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*.

Na esteira do caso Snowden, em 2013, uma Comissão Parlamentar de Inquérito (CPI) investigou a espionagem eletrônica estrangeira no Brasil. Desdobrou-se outra consequência nefasta da desconfiança histórica da classe política nas forças armadas. A utilização do Serviço Nacional de Informações (SNI), incluindo a intercepção de comunicações telefônicas pelo aparato estatal de segurança, durante o regime militar, colocou sob suspeita a atividade de inteligência. A legislação posterior ao regime militar restringiu significativamente essas capacidades. O próprio SNI foi extinto em 1990, e somente em 1999 foi criada a Agência Brasileira de Inteligência (ABIN), sem capacidade de SIGINT. O relatório da referida CPI sugeriu a criação de tal agência, o que ainda não foi feito[41].

Da mesma forma, o arcabouço jurídico cibernético brasileiro vem evoluindo rapidamente no que diz respeito à proteção das garantias individuais e na classificação dos crimes praticados com meios cibernéticos. Exemplos são a Lei Carolina Dieckmann (2012), o Marco Civil da Internet (2014) e a LGPD (2018), a versão brasileira da GDPR europeia[42]. Nenhuma legislação, no entanto, concede ao Estado capacidades de inteligência cibernética.

Outra crítica comum é a falta de participação da sociedade civil organizada, academia e setor privado na formulação de políticas relacionadas ao ciberespaço [43]. Ainda assim, a e-Ciber expressa, em seu texto, um processo bastante participativo envolvendo centenas de participantes do

---

[41] Brasil-CN, "Relatório Da CPI Da Espionagem Eletrônica Do Senado Federal."

[42] Union, "What Is the LGPD? Brazil's Version of the GDPR."

[43] Beer, "Cyber Security in Brazil: Can a Grassroots Campaign Help Protect a Country"; Diniz, Muggah, and Glenny, "Deconstructing Cyber Security in Brazil: Threats and Responses"; Hurel and Lobato, "Uma Estratégia Para a Governança Da Segurança Cibernética No Brasil."

governo, da iniciativa privada e da academia. De fato, a estratégia se assemelha em muitos aspectos a um texto acadêmico, principalmente nas referências bibliográficas.

A essência de um processo de securitização é aumentar a percepção do público sobre a importância do objeto securitizado, permitindo assim uma excepcional alocação de recursos a ele. O volume de recursos aplicados pelo Brasil em ciberdefesa e cibersegurança, comparado ao investido por países com interesses semelhantes, mostra que é difícil argumentar a favor da securitização do ciberespaço no Brasil. É perceptível que alguns insistem que essa securitização ocorre mesmo quando reconhecem que o Marco Civil da Internet evitou especificamente quaisquer termos que pudessem se relacionar com essa suposta securitização, para facilitar sua aprovação pelo Congresso.

> Enquanto o Brasil desecuritiza o ciberespaço por meio do Marco Civil da Internet, respondendo a preocupações sobre os papéis dos diferentes atores que lidam com o ciberespaço, ao mesmo tempo o Marco Legal pode contribuir para uma ressecuritização do ciberespaço, não limitando claramente a ação estatal neste campo. [44]

A rigor, essa "dessecuritização" reflete a cultura estratégica brasileira e institucionaliza mais uma instância do ato de evitar formas de *hard power* ou de estadismo.

3.4 Uma Estratégia Cibernética "À Brasileira"

Em outubro de 2019, o GSI divulgou uma consulta pública sobre o texto preliminar da futura e-Ciber brasileira, consolidada e publicada em fevereiro de 2020. Como esperado, ela reflete muito da cultura brasileira, memória

---

[44] Vales, "Is There a Way to Desecuritise Cyberspace? How Brazil's Legal Framework for the Internet Could Have Done That."

social, tradição, institucionalismo histórico e *cara* (*face*) do Brasil, como mostrado adiante.

3.4.1 Quanto ao Escopo

Considerando os 15 países com as maiores economias citados no início deste capítulo, apenas a Índia ainda não publicou sua Estratégia Nacional de Segurança Cibernética. Dentre os outros 14, a e-Ciber brasileira é a única que exclui explicitamente a ciberdefesa de seu escopo, não obstante a já mencionada fusão doutrinária brasileira de questões de segurança e defesa e a orgulhosa participação do ComDCiber brasileiro nas atividades de cibersegurança. Ela explicita que a ciberdefesa deverá constar de um documento futuro separado, sob a responsabilidade do Ministério da Defesa. A justificativa, retórica, argumentou que a Política Nacional de Segurança da Informação (PNSI) afirma que a Estratégia Nacional de Segurança da Informação (ENSI) "será dividida nos seguintes módulos, **entre outros**:

> I – segurança cibernética;
>
> II – defesa cibernética;
>
> III – segurança de infraestruturas críticas;
>
> IV – segurança de informações sensíveis; e
>
> V – proteção contra vazamento de dados" [45]

A separação baseada nesses tópicos, porém, gera um paradoxo em relação às infraestruturas críticas (ICs). De fato, a "segurança de infraestruturas críticas", conforme estipulado no item III, é mais abrangente do que cibersegurança das ICs, segurança de informações confidenciais e proteção contra vazamento de dados. Assim, não deveria haver qualquer referência à cibersegurança das ICs na e-Ciber, pois essas deveriam

[45] Brasil-GSI, Política Nacional de Segurança da Informação.

estar no módulo específico das ICs (previsto no item III). Mas existem algumas.

Se, no sentido contrário, se entender que a cibersegurança é um item que engloba a cibersegurança dos ICs, pode-se deduzir que o mesmo princípio se aplica à ciberdefesa dos ICs, segurança de informações sensíveis e proteção contra vazamento de dados. Cada um deve, portanto, ser incluído em seu módulo correspondente. Nesse caso, sobraria muito pouco, em segurança da informação, para um módulo relacionado à proteção de ICs.

Ambas as alternativas soam logicamente absurdas. Assim, verifica-se que o legislador (o próprio GSI), entendeu que a Estratégia Nacional de Segurança da Informação deveria ser uma estratégia que englobasse pelo menos esses cinco módulos, mas não separadamente. No entanto, ela o faz.

No entanto, a e-Ciber cumpre a tradição doutrinária e a cultura estratégica brasileira de misturar segurança e defesa, e a dificuldade técnica de separar esses temas no ciberespaço. Quanto à primeira, afirma a intenção de reduzir a vulnerabilidade de 'organizações governamentais' (apenas) "contra qualquer tipo de ameaça cibernética" e ataques "realizados por países, grupos ou indivíduos". Assim, *defesa externa e interna*. Sobre este último, a e-Ciber cita o Exercício Guardião Cibernético, exercício interagências promovido pelos militares com a participação do GSI e representantes de ICs e outros órgãos, para exercitar o processo decisório, responsabilidades e fluxo de comunicação em face de diferentes tipos e níveis de ameaças cibernéticas, reforçando assim a necessidade de esforços conjuntos de segurança e defesa no âmbito cibernético.

Tudo indica que a real motivação para essa separação *sui generis* não é, então, uma imposição legal, como faz parecer o texto da e-Ciber. Uma hipótese

plausível é a de que o módulo de ciberdefesa ainda não estivesse pronto e não pudesse ser integrado ao documento. Outra possibilidade é a de maior importância atribuída à segurança em oposição à defesa. Essa hipótese seria justificada por: (1) uma percepção pública da necessidade de cibersegurança, devido ao grande volume de crimes cibernéticos e sua repercussão na mídia; (2) críticas públicas aos investimentos brasileiros em ciberdefesa, embora eles já sejam comparativamente bastante reduzidos; (3) a ausência de visibilidade clara (e o desejo de não nomear quaisquer "inimigos externos" para ciberdefesa; (4) a falta de cultura sobre a importância do SIGINT e o medo de seu uso em abusos contra os direitos civis. De fato, a e-Ciber afirma, em sua seção 1.1, que a cibersegurança é considerada a "área mais crítica e atual [da ENSI] a ser abordada". De qualquer forma, sinalizou internacionalmente que a ciberdefesa permanece secundária para o Brasil.

Uma terceira hipótese estaria ligada à publicação do Cybersecurity Capacity Review of Brazil [46]. O estudo, iniciado cerca de dois anos antes, foi publicado alguns meses após a e-Ciber, tendo sido conduzido pela Organização dos Estados Americanos (OEA), pelo Centro de Capacidade Global de Cibersegurança da Universidade de Oxford e pelo GSI. Concluiu-se que o Brasil se enquadrava no nível Formativo (o básico) em 17 áreas-chave, no Estabelecido (o segundo nível) em sete delas, e nenhuma área-chave nos níveis Estratégico e Dinâmico, os dois mais avançados. E dentre as sete áreas-chaves que estão no segundo estágio, uma delas é justamente a existência de uma Estratégia Nacional de Cibersegurança. Assim, a e-Ciber poderia ter sido publicada "às pressas"

[46] Oxford GCSCC, "Cybersecurity Capacity Review of Brazil."

para permitir uma melhor avaliação das capacidades brasileiras.

3.4.2 Quanto à Objetividade, Tempos Verbais e Linguagem

Na comunicação estratégica, todo tema deve ser relevante para a missão da entidade. As informações devem ser restritas ao mínimo necessário e suficiente. Este argumento para a simplicidade é consistente com o princípio lógico conhecido como Navalha de Occam: se em todo o resto as várias explicações de um fenômeno são idênticas, a mais simples é a melhor. Além disso, o ditado "escrever é a arte de cortar palavras" deve sempre ser lembrado [47]. Apesar disso, o texto da e-Ciber carece de simplicidade e denota a preocupação de não ser incisivo ou determinista em suas proposições, tornando o texto muito copioso, extenso e repetitivo.

As Estratégias Nacionais de Cibersegurança são frequentemente incisivas e afirmativas. Eles usam principalmente tempos verbais do modo indicativo, particularmente com uso frequente do futuro ou do infinitivo. A e-Ciber, por sua vez, faz uso extensivo de tempos verbais no modo subjuntivo.

Essa opção impacta na credibilidade da estratégia. As formas verbais no modo indicativo referem-se a fatos verossímeis ou considerados como tais: canto, cantei, cantarei; o modo subjuntivo refere-se a eventos incertos: se eu cantasse, quando eu cantar [48]. O modo subjuntivo, então, expressa ações inacabadas, passíveis de execução, incertas, fantasiosas ou imaginativas, geralmente denotando condição, hipótese,

---

[47] Nogueira, "Escrever é a Arte de Cortar Palavras: De Que Mestre Teria Partido Esta Preciosa Lição?"

[48] Bechara, *Moderna Gramática Portuguesa*.

desejo, pedido ou dúvida. O modo subjuntivo está associado ao uso de “se”, “quando” e “que” associado a verbos[49].

Mesmo nas “Ações Estratégicas” propostas pela e-Ciber, essa natureza não determinística está presente. A Ação 2.3.1 declara “Entre as ações **que podem ser adotadas** a esse respeito […]” (grifo nosso). A ação 2.3.6 estabelece que “podem ser tomadas ações como”, enquanto 2.3.7 cita “ações a serem consideradas”. Situações semelhantes existem nas ações 2.3.8, 2.3.9 e 2.3.10.

Por fim, reforçando sua natureza não determinista (muito brasileira, aliás), há pelo menos duas dezenas de recomendações (não determinações), em sua maioria escritas literalmente na forma “a e-Ciber recomenda […]”.

3.4.3 Sobre a Estrutura do Documento

A estrutura da e-Ciber difere até mesmo daquela do PND e END [50]. Isso suscita algumas questões. Por que a e-Ciber é estruturalmente diferente da END? Outros módulos da ENSI seguirão este padrão? Ou a ENSI será um conjunto de módulos de diferentes estruturas?

A e-Ciber também apresenta uma preocupação injustificada em descrever sua metodologia de elaboração, tornando-a mais um documento acadêmico ou um estudo técnico do que uma peça de comunicação estratégica. Nenhuma outra estratégia cibernética no *corpus* deste capítulo descreve o processo utilizado em seu desenvolvimento. A preocupação da e-Ciber parece estar relacionada a críticas sobre a falta de debate público anterior [51].

---

[49] Bechara.

[50] Brasil-MD, “Política Nacional de Defesa e Estratégia Nacional de Defesa.”

[51] Diniz, Muggah, and Glenny, “Deconstructing Cyber Security in Brazil: Threats and Responses.”

Outro aspecto refere-se às extensas referências a dispositivos legais e ações passadas. Nas demais estratégias, raramente são encontradas referências a instrumentos jurídicos específicos. Apenas os franceses as fazem, mas apenas algumas poucas e usando notas de rodapé. A e-Ciber, por sua vez, é prolífica em citações 'no texto' de leis, decretos, instruções normativas e até seus adendos. Isso indica uma preocupação constante em mostrar o cumprimento do marco legal, desconsiderando a premissa de que espera-se que uma estratégia nacional aprovada por um Chefe de Estado e de Governo esteja em conformidade com o marco legal, sendo desnecessária a menção sistemática de cada norma. A preocupação da e-Ciber parece uma defesa prévia contra acusações, típicas daquelas comumente feitas durante o regime militar, mas bastante frequentes ainda hoje no tocante a ações policiais em favelas e comunidades carentes, de agentes do Estado infringindo a lei e os direitos civis.

Além disso, como documento estratégico, a e-Ciber deve apontar e indicar tendências e ações futuras. Como afirma, "constitui uma orientação clara do governo federal para a sociedade brasileira sobre as ações que pretende". Portanto, deve se concentrar no futuro, não no passado. No entanto, em vários pontos, descreve ações passadas, algumas há quase duas décadas, denotando uma preocupação em explicar ou justificar as opções tomadas ou decisões então tomadas, ou mesmo a existência de algumas instituições.

3.4.4 Sobre as "Referências"

Quando os documentos oficiais citam empresas ou indivíduos, eles oferecem uma forma de "endosso" que confere importância e relevância internacional aos nomeados. Este endosso tem valor comercial. Quando os britânicos citam a Cisco e a Symantec em sua Estratégia Nacional de Cibersegurança, afirmam que o governo do Reino Unido confia nessas companhias, permitindo que ambas

desenvolvam campanhas de marketing explorando tal credibilidade. Também abre espaço para questionamentos no sentido dos motivos pelos quais usou dados da Symantec e não de qualquer outro concorrente de renome. Os EUA, que abrigam muitos gigantes de TI, não mencionam uma única empresa, pesquisa ou pesquisador em sua estratégia. Nem a Alemanha, a China ou a Itália. Por outro lado, a e-Ciber nomina diversas empresas e pessoas.

Além disso, muitas citações referem-se a dados sem qualquer relevância estratégica. A ciência da informação consolidou o conceito de hierarquia do conhecimento, ou cadeia DIKW (sigla para dados, informação, conhecimento, sabedoria). Conceitualmente, dados brutos não carregam informações, informações em si não carregam conhecimento e assim por diante. Uma foto, sem qualquer contexto, diz pouco ou quase nada para uma pessoa aleatória. São apenas dados brutos. No entanto, se a pessoa que analisa tal foto tiver algum contexto, como a data em que foi tirada, a localização ou o nome da pessoa fotografada, essa foto se torna uma informação. E assim por diante, nos demais níveis [52].

Posteriormente, o nível "compreensão" foi adicionado à cadeia, tornando-a DIKUW, e uma nova metáfora criada. Os dados são apenas símbolos absolutos; informação são os dados processados, respondendo a perguntas como "quem", "o quê", "quando" e "onde"; conhecimento é a aplicação de dados e informações para responder a perguntas do tipo "como"; compreensão é a apreciação do "porquê"; e a sabedoria é o entendimento calibrado [53].

Assim, os dados descontextualizados não são úteis para a tomada de decisão. No entanto, a e-Ciber traz dezenas de dados descontextualizados ou estatisticamente irrelevantes.

---

[52] Zeleny, "Management Support Systems: Towards Integrated Knowledge Management."

[53] Ackoff, "From Data to Wisdom."

Como é o caso de uma pesquisa realizada com 200 grandes e médias empresas brasileiras. Este é um número relevante? Desses, 34% (68 empresas) enfrentaram algum tipo de incidente cibernético. Destes, 29% (portanto 20) tiveram impacto operacional. Isso é muito? Além disso, entre esses 68, 4% (portanto, 2,7) tiveram um impacto reputacional nos clientes. Quais são os números internacionais? É uma base sólida para a tomada de decisões estratégicas? Mais um exemplo diz respeito ao uso de certificados digitais, onde o texto indica que os certificados emitidos 'apenas 8,4%' são para uso pessoal dos cidadãos, enquanto 45,9% eram para empresas, silenciando sobre os restantes 45,7%. Esses números são relevantes para fazer ou comunicar a estratégia?

Por fim, há uma lista desnecessária, detalhada, copiosa e extensa de CSIRTs brasileiros e outra de fóruns internacionais exemplificativos em que esses CSIRTs poderiam participar para melhorar sua rede.

3.5 Conclusão

Este capítulo buscou demonstrar que a e-Ciber, ao invés de refletir qualquer tentativa de securitização dos formuladores de políticas brasileiras, reflete fortemente a tradição e a cultura estratégica nacionais ao recusar o desenvolvimento de *hard power* e de estadismo. Como demonstrado, o desenvolvimento das capacidades de segurança e defesa em qualquer sociedade depende dos fatores culturais que determinam sua postura estratégica: suas percepções, tradições, reputação (*face*) e instituições. Além disso, que a estratégia cibernética brasileira reflete muito do 'jeitinho brasileiro': evita incisividade, confronto ou mesmo alocação de recursos ou responsabilidades. Também, como institucionalizado em mais de dois séculos de história do país, particularmente nos últimos 40 anos, uma resistência a qualquer indício de empoderamento estatal.

Além de bastante atrasada, a e-Ciber ‘fica aquém’, falhando em todos os quatro pilares que constroem uma boa estratégia nacional de defesa e segurança. Em primeiro lugar, não comunica o que é essencial para o exercício da influência estatal e a consecução dos fins pretendidos. É, de fato, ‘tímida’ em suas intenções, com muitos ‘faria’ e poucos ‘fará’. Em segundo lugar, não mantém a coesão linguística para criar significado e unidade. Terceiro, não considera que as ações propostas sejam de longo prazo e que sua correção ou adequação em caso de erro seja um processo demorado e desafiador. Quarto, embora indique os objetivos pretendidos, não especifica responsabilidades e recursos para que as ações pretendidas atinjam (e mantenham) seus objetivos. A e-Ciber parece, na prática, uma carta de (boas) intenções, não uma estratégia nacional. A *jabuticaba* de dividir as estratégias de cibersegurança e ciberdefesa corre o risco de fazer com que duas se tornem nenhuma: nem segurança nem defesa.

Tem algum mérito, no entanto. Principalmente o de ser implementada de forma colaborativa e participativa, desde a fase de diagnóstico até a prescrição de ações, e aberta à consulta pública. Esta consulta permitiu a correção de muitos pontos, sendo o resultado final muito melhor que o original.

De maneira bem brasileira, ainda, deve-se dizer que, embora os erros estratégicos sejam difíceis (e demorem) de corrigir, o tempo resolve tudo. Assim, no longo prazo, o resultado final pode ser significativo, até satisfatório, pois pelo menos a e-Ciber aponta em alguma direção, abrindo espaço para uma discussão mais aprofundada sobre a adequação da cultura estratégica brasileira às necessidades de cibersegurança e ciberdefesa.

3.6 Referências

Ackoff, Russell. “From Data to Wisdom.” *Journal of Applied Systems Analysis* 16, no. 1 (1989). https://doi.org/citeulike-article-id:6930744.

Bechara, Evanildo. *Moderna Gramática Portuguesa*. 37th ed. Rio de Janeiro: Editora Nova Fronteira Participações S.A., 2009.

Beer, William. "Cyber Security in Brazil: Can a Grassroots Campaign Help Protect a Country." *Georgetown Journal of International Affairs* 16 (2015): 178–85.

Bigo, Didier. "When Two Become One: Internal and External Securitisations in Europe." In *International Relations Theory and the Politics of European Integration: Power, Security and Community*, edited by Morten Kelstrup and Michael Williams, 171–204. Routledge, 2000. https://doi.org/10.4324/9780203187807-8.

Brasil-CN. Constituição Federal de 1988 (1988).

———. Lei Complementar 97 (1999).

———. "Relatório Da CPI Da Espionagem Eletrônica Do Senado Federal." Brasília, 2014.

Brasil-GSI. Política Nacional de Segurança da Informação (2018).

Brasil-MD-EPEX. "Integrando Capacidades Na Vigilância e Na Atuação Em Nossas Fronteiras." EPEX - Escritório de Projetos do Exército Brasileiro, n.d. http://www.epex.eb.mil.br/index.php/sisfron.

———. "Programa Da Defesa Cibernética Na Defesa Nacional." EPEX - Escritório de Projetos do Exército Brasileiro, n.d. http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica-na-defesa-nacional.

Brasil-MD. "Escola Nacional de Defesa Cibernética é Inaugurada Em Brasília." Ministério da Defesa, 2019. https://www.defesa.gov.br/noticias/52690-escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia.

———. "Exército Brasileiro - Organograma." Exército Brasileiro - Organograma, 2020. http://www.eb.mil.br/organograma.

———. *Manual Básico Vol. 1*. Rio de Janeiro: ESG, 2014.

———. "Missões de Paz." MD Website, n.d. https://www.defesa.gov.br/relacoes-internacionais/missoes-de-paz.

———. "Política Nacional de Defesa e Estratégia Nacional de Defesa." Brasília, 2016.

Buzan, Barry, and Lene Hansen. *The Evolution of International Security Studies*. Cambridge University Press, 2009.

Buzan, Barry, and Ole Wæver. “Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory.” *Review of International Studies* 35, no. 2 (2009): 253–76. https://doi.org/10.1017/S0260210509008511.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 1998.

Caiafa, Roberto. “10 Perguntas Para o General Okamura, Comandante Da Defesa Cibernética Do Exército Brasileiro.” *Tecnologia e Defesa*, 2018. https://tecnodefesa.com.br/10-perguntas-para-o-general-okamura-comandante-da-defesa-cibernetica-do-exercito-brasileiro/.

Clarke, Richard A, and Robert K Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers, 2010.

D’Alama, Luna. “Tragédia Em Alcântara Faz Dez Anos e Brasil Ainda Sonha Em Lançar Foguete.” *G1*, 2013. http://g1.globo.com/ciencia-e-saude/noticia/2013/08/tragedia-em-alcantara-faz-dez-anos-e-brasil-ainda-sonha-em-lancar-foguete.html.

Degaut, Marcos. “Brazil’s Military Modernization: Is a New Strategic Culture Emerging?” *Rising Powers Quarterly* 2, no. 1 (2017): 271–97.

Diniz, Gustavo, Robert Muggah, and Misha Glenny. “Deconstructing Cyber Security in Brazil: Threats and Responses.” *Strategic Paper*. Rio de Janeiro, 2014. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf.

Fagen, Richard. “The United States and Chile: Roots and Branches.” *Foreign Affairs* 53, no. 2 (1975): 297–313.

Franchi, Tássio, Eduardo Xavier Ferreira Glaser Migon, and Roberto Xavier Jiménez Villarreal. “Taxonomy of Interstate Conflicts: Is South America a Peaceful Region?” *Brazilian Political Science Review* 11, no. 2 (2017): 1–23. https://doi.org/10.1590/1981-3821201700020008.

GlobalFirepower.com. “2021 Military Strength Ranking.” Global Firepower Index, 2021. https://www.globalfirepower.com/countries-listing.php.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Penguin Books, 2014.

Herz, Monica. “Concepts of Security in South America.” *International Peacekeeping* 17, no. 5 (2010): 598–612. https://doi.org/10.1080/13533312.2010.516938.

Hurel, Louise Marie, and Luisa Cruz Lobato. “Uma Estratégia Para a Governança Da Segurança Cibernética No Brasil,” 2018.

IMF. “World Economic Outlook Database.” World Economic Outlook Database, 2019. https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/weorept.aspx?pr.x=57&pr.y=17&sy=2019&ey=2019&scsm=1&ssd=1&sort=country&ds=.&br=1&c=512%2C668%2C914%2C672%2C612%2C946%2C614%2C137%2C311%2C546%2C213%2C674%2C911%2C676%2C314%2C548%2C193%2C556%2C122%2C6.

Lewys, Anthony. “The Kissinger Doctrine.” *The New York Times*, 1975.

Lobato, Luísa, and Kai Kenkel. “Discourses of Cyberspace Securitization in Brazil and in the United States.” *Revista Brasileira de Política Internacional* 58, no. 2 (2015): 23–43. https://doi.org/10.1590/0034-7329201500202.

Malagutti, Marcelo. “Estruturas de Ciberdefesa Em Diferentes Países.” In *XVII Ciclo de Estudos Estratégicos*. Rio de Janeiro: ECEME, 2017.

———. “O Necessário Upgrade Na Ciberdefesa Brasileira.” *Revista Política Hoje* 29, no. 2 (2020): 30–53.

Maltchiik, Roberto. “Brasil Deve Lançar Foguete No Espaço Em 2019.” *O Globo*, 2017.

Mandarino, Raphael, and Claudia Canongia, eds. *Livro Verde Segurança Cibernética No Brasil*, 2010.

Muggah, Robert, and Nathan Thompson. “Brazil Must Rebalance Its Approach to Cybersecurity.” CFR Net Politics, 2016. https://www.cfr.org/blog/brazil-must-rebalance-its-approach-cybersecurity.

Nogueira, Armando. “Escrever é a Arte de Cortar Palavras: De Que Mestre Teria Partido Esta Preciosa Lição?” Portal da Imprensa, 2010. http://portalimprensa.com.br/noticias/ultimas_noticias/32240/imprensa+republica+artigo+de+armando+nogueira+sobre+o+desafio+da+edicao+de+texto.

Notícias, Brasil-Senado. “Aprovadas Em Plenário Novas Política e Estratégia Nacional de Defesa.” *Senado Notícias*. 2018.

Okamura, Ângelo. “Abertura Do V Seminário Internacional de Defesa Cibernética.” Brasília, 2017. https://cryptoid.com.br/eventos/v-seminario-internacional-de-defesa-cibernetica/.

Oxford GCSCC. “Cybersecurity Capacity Review of Brazil,” 2020.

Saint-Pierre, Héctor. “‘Defesa’ Ou ‘Segurança’?: Reflexões Em Torno de Conceitos e Ideologias.” *Contexto Internacional* 33, no. 2 (2011): 407–33. https://doi.org/10.1590/s0102-85292011000200006.

Union, European. “What Is the LGPD? Brazil’s Version of the GDPR.” GDPR.EU, n.d. https://gdpr.eu/gdpr-vs-lgpd/.

US-Navy. “Marinha Vai Substituir Fragatas Por Corvetas, Revela Alm. Ivan Taveira.” *Poder Naval*, 2017.

Vales, Tiago. “Is There a Way to Desecuritise Cyberspace? How Brazil’s Legal Framework for the Internet Could Have Done That.” *Encuentro Latinoamericano* 4, no. 2 (2017).

Zeleny, Milan. “Management Support Systems: Towards Integrated Knowledge Management.” *Human Systems Management*, 1987. https://doi.org/10.3233/HSM-1987-7108.

4 A Oportunidade Estratégica

Este capítulo analisa as oportunidades que uma estratégia coordenada de Ciberdissuasão pela Negação apresenta para países com uma cultura estratégica não-agressiva como o Brasil. Analisando dados econômicos relacionados ao mercado de Tecnologia da Informação, mostra que tal estratégia pode oferecer um bom retorno do investimento e impulsionar a economia nacional.

4.1 Introdução – "É a Economia, Estúpido!" ("*It's the Economy, Stupid!*")[1]

A economia é a base do bem-estar de um estado e a razão mais frequente para a busca de poder (e muitas vezes sua fonte primária também). Adicionalmente, é intimamente ligada a todas as outras expressões do poder nacional. É também um elemento essencial da Teoria da Dissuasão. No entanto, os conceitos de custo e valor, expressos em termos econômicos, podem, e freqüentemente relacionam-se a aspectos morais, éticos ou culturais. Além disso, o argumento em favor da Dissuasão pela Punição e contra a Dissuasão pela Negação é, geralmente, baseado no custo da negação ser muito mais elevado.

Mas e quanto ao retorno econômico da ciberdissuasão? Como ciência, a economia mostra que existem duas maneiras fundamentais de se melhorar os resultados econômicos: (i) cortar custos; (ii) aumentar a receita.

4.1.1 Corte de Custos

Fortes ciberdefesas limitarão as perdas financeiras diretas com propriedade intelectual roubada. O governo dos

---

[1] Mantra cunhado pelo estrategista James Carville para a campanha do presidente Clinton em 1992, que enfoca a economia como o elemento político mais importante.

EUA costuma reclamar do roubo de propriedade intelectual de empresas americanas por países estrangeiros por meios informatizados. Em 2018, esse governo chegou a emitir um documento público oficial intitulado Foreign Economic Espionage in Cyberspace, onde afirmava:

> A espionagem econômica e industrial estrangeira contra os Estados Unidos continua a representar uma ameaça significativa à prosperidade, segurança e vantagem competitiva da América. O ciberespaço continua sendo um domínio operacional preferencial para uma ampla gama de atores de ameaças de espionagem industrial, desde estados-nação adversários a empresas comerciais que operam sob a influência do Estado e atividades patrocinadas conduzidas por grupos de hackers proxy.[2]

Apesar de nomear China, Rússia e Irã como atores particularmente agressivos interessados na ciberespionagem econômica, o relatório também aponta que outros atores incorrem nesta prática.

> Países com laços mais estreitos com os Estados Unidos realizaram espionagem cibernética e outras formas de coleta de inteligência para obter tecnologia, propriedade intelectual, segredos comerciais e informações proprietárias dos EUA. Aliados ou parceiros dos EUA muitas vezes aproveitam o acesso de que desfrutam para coletar tecnologias militares e civis sensíveis e para adquirir know-how em setores prioritários.[3]

Não há razão para supor que este seja um problema exclusivamente dos EUA, e não de potências menores. O valor comercial das tecnologias de "exploração de petróleo em águas ultraprofundas" desenvolvidas pela empresa petrolífera brasileira Petrobras é enorme. Como também de tecnologias desenvolvidas pela fabricante brasileira de aeronaves Embraer.

---

[2] United States, "Foreign Economic Espionage in Cyberspace."

[3] United States.

Boas ciberdefesas também limitarão as perdas dos países por serem flanqueados em negociações internacionais como a da Quinta Cúpula das Américas, ou a da aquisição bilionária do SIVAM brasileiro (vigilância por radar da Amazônia) onde a francesa Thomson-CSF foi vencida pela Raytheon americana, com o apoio da NSA, a agência norte-americana de inteligência de sinais (que inclui a ciberinteligência)[4].

Boas ciberdefesas também podem reduzir o dano econômico causado por malware patrocinado por Estados, como WannaCry e NotPetya, que causaram impacto econômico significativo em todo o mundo. Embora a dissuasão, neste trabalho, esteja focada em ciberofensas patrocinadas por Estados, elevar o nível das defesas também pode reduzir o impacto do cibercrime. Assim, esse resultado deve ser contabilizado em qualquer análise da razão de custos e ganhos.

Em 2015, o CEO do grupo de seguros britânico Lloyds estimou os prejuízos causados pelo cibercrime a empresas privadas em todo o mundo em algo entre 400 e 500 bilhões de dólares anuais[5]. O CSIS, um *think tank* americano, estima que enquanto o cibercrime representou 0,62% do PIB global em 2014, em 2016 ele cresceu para 0,8%, atingindo a cifra de USD 600 bilhões[6]. Em 2017, o Brasil foi considerado a segunda maior vítima de crimes cibernéticos no mundo, com perdas de USD 22,5 bilhões[7].

---

[4] Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*; Campbell, *Development of Surveillance Technology and Risk of Abuse of Economic Information Part 2/5*.

[5] Gandel, "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year | Fortune."

[6] Lewis, "Economic Impact of Cybercrime — No Slowing Down."

[7] Brasil-GSI, "Estratégia Nacional de Segurança Cibernética (e-Ciber)."

4.1.2 Aumento de Receita

O mercado global de Software e Serviços tem crescido continuamente nas últimas décadas. Como um produto da "era pós-industrial", dependente de engenhosidade e criatividade mais do que de capacidades industriais elevadas ou habilidades de engenharia complexas, oferece a possibilidade de se pular etapas para o crescimento econômico de nações.

Para uma melhor compreensão dessa alternativa, é necessário compreender a relevância desse mercado, em termos socioeconômicos. Este é o assunto das próximas seções.

4.2 O Mercado Global de Software

Esta seção apresenta e compara dados relativos aos mercados americano, europeu e brasileiro de software e serviços. Os dados coletados mostram que esse setor é relevante em termos de geração de emprego e renda.

4.2.1 Os EUA

A Tabela 4-1 apresenta dados sobre a importância da indústria de software na economia dos EUA em 2014, 2016 e 2018, permitindo a análise de seu crescimento e importância relativa. O produto bruto direto da indústria de software aumentou 77,8% entre 2014 e 2018, enquanto o número de empregos diretos aumentou 24% e os salários cresceram 4,8%. Além disso, enquanto em 2014 havia 3,92 empregos totais na cadeia de valor para cada emprego direto, esse número subiu para 4,64 em 2018.

Adicionalmente, a participação do setor em Pesquisa e Desenvolvimento (P&D) cresceu 59% no período, mais que o dobro da taxa nacional de crescimento de P&D (28,5%). Por fim, o salário médio de TI mantém uma proporção de alguma forma regular de 2,2:1 em comparação com o salário médio nos EUA.

Tabela 4-1 – Evolução do Mercado de Software dos EUA 2014/2018

Item	2014	2016	Dif. 16/14	2018	Dif. 18/14
PIB direto (bilhões de USD)	475,3	564,4	18,7%	845,0	77,8%
PIB Total (bilhões de USD)	1.070,0	1.140,0	6,5%	1.600,0	49,5%
Empregos Diretos (milhões)	2,5	2,9	16,0%	3,1	24,0%
Empregos Totais (milhões)	9,8	10,5	7,1%	14,4	46,9%
Salários TI (USD a.a.)	108.760	104.360	-4,0%	114.000	4,8%
Salários Médios (USD a.a.)	48.320	49.630	2,7%	51.960	7,5%
P&D (bilhões de USD)	52,0	63,1	21,3%	82,7	59,0%
Taxa de P&D (%)	17,2	19,6	14,0%	22,1	28,5%

Fonte: Compilada pelo autor com dados da BSA Foundation[8].

4.2.2 Europa

A Tabela 4-2 apresenta dados relativos ao mercado europeu (União Europeia – UE) de software entre 2014 e 2016, permitindo uma comparação direta com o mercado dos EUA no mesmo período.

Enquanto o PIB direto dos EUA do setor cresceu 18,7% na época, o mercado da UE cresceu 22,1%. O crescimento da participação dos EUA no PIB total foi de 6,5%, enquanto o europeu foi de 9,9%. Em 2016, a relação entre empregos totais e empregos diretos na Europa era de 3,53:1, muito semelhante aos 3,62:1 dos EUA.

Não obstante, duas diferenças principais entre os setores de software da Europa e dos Estados Unidos podem ser observadas. Em primeiro lugar, na relação salário de TI / salário gerais, de apenas 1,34:1 na Europa, contra 2,25:1 nos EUA em 2014 (os dados disponíveis indicaram uma taxa

[8] BSA Foundation, "The $1 Trillion Economic Impact of Software"; BSA Foundation, "The Growing €1 Trillion Economic Impact of Software"; BSA Foundation, "Software: Growing US Jobs and the GDP."

semelhante não confirmada em 2016). Essa diferença provavelmente está relacionada à história das políticas de bem-estar social na Europa desde a segunda guerra mundial, que reduziram as desigualdades sociais na Europa, políticas não observáveis nos EUA. Segundo, na participação (taxa) do setor em P&D. A taxa do setor de software nos EUA foi de 17,2%, contra 7,3% na Europa em 2014.

Tabela 4-2 – Evolução do Mercado de Software da Europa 2014/2016

Item	2014	2016	Diff. 16/14
PIB direto (bilhões de EUR)	249,0	304,0	22,1%
PIB Total (blihões de EUR)	910,0	1.000,0	9,9%
Empregos Diretos (milhões)	3,1	3,6	16,1%
Empregos Totais (milhões)	11,6	12,7	9,5%
Salários TI (EUR a.a.)	45.333	45.307	-0,1%
Salários Médios (EUR a.a.)	33.790	N/A	N/A
P&D (bilhões de EUR)	12,7	N/A	N/A
Taxa de P&D (%)	7,3	N/A	N/A

Fonte: Compilada pelo autor com dados da BSA Foundation [9].

4.2.3 Brasil

A Business Software Alliance (BSA) não produziu relatórios sobre o mercado brasileiro semelhantes aos dos EUA ou UE até o momento. No entanto, a Associação Brasileira das Empresas de Software (ABES) produz relatórios anuais que permitem alguns insights.

A Figura 4-1 mostra a distribuição do mercado mundial de TI em relação aos mercados de Software, Serviços e

[9] BSA Foundation, "Software: A € 910 Billion Catalyst for the EU Economy"; BSA Foundation, "The Growing €1 Trillion Economic Impact of Software."

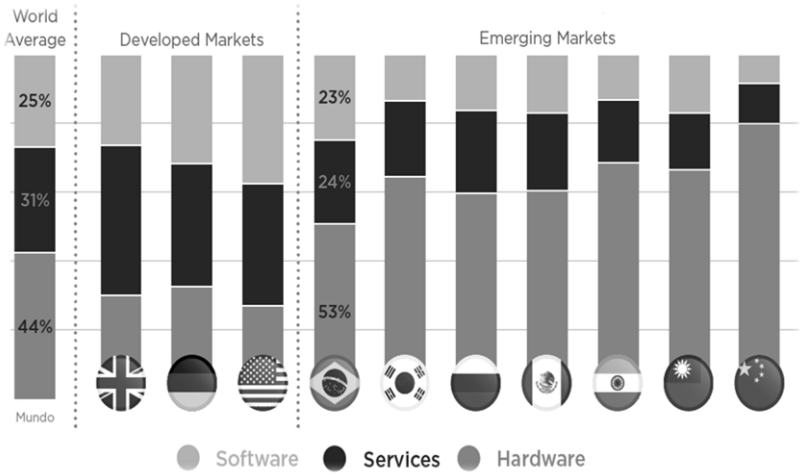
Hardware. Está dividido em três grupos: Média Global, Mercados Desenvolvidos e Mercados Emergentes.

Em relação aos Mercados Desenvolvidos, pode-se observar que a Alemanha possui distribuições semelhantes entre os três setores de seu mercado, com cerca de um terço de participação para cada um. O mercado dos EUA é um pouco mais concentrado em Software do que em Hardware. O mercado do Reino Unido está mais concentrado em Serviços do que em Software e Hardware. Em qualquer caso, o Hardware, como produto da "era industrial", responde por menos que o Software ou os Serviços, produtos da "era pós-industrial".

Por outro lado, no âmbito dos Mercados Emergentes, o Hardware tem maior participação do que Software e Serviços juntos em todos os países analisados. A situação é consistente com o fato de que China, Taiwan, Coréia do Sul e Índia (bem como Cingapura e Malásia) concentram a maior parte das fábricas de componentes eletrônicos no mundo. A famosa frase "Projetado pela Apple na Califórnia - Montado na China", presente em iPhones e iPads, sintetiza a ideia. O México, por sua vez, concentra um grande número de maquiladoras, empresas que importam componentes com isenção de impostos, os montam e exportam o produto acabado para os EUA e Canadá. Resultado do Acordo de Livre Comércio da América do Norte (NAFTA), de 1994, e seu substituto, o Acordo EUA-México-Canadá (USMCA), assinado em 2018 e aprovado pelo Congresso dos Estados Unidos em 2020.

O único país da amostra que se aproxima da Média Mundial, indo na direção dos Mercados Desenvolvidos, é o Brasil, denotando um mercado de TI que está se tornando maduro, embora ainda um pouco mais concentrado em Hardware do que em Software e Serviços.

Figura 4-1 – Distribuição do Mercado Mundial de TI



Fonte: ABES[10].

A Tabela 4-3 apresenta a evolução do mercado brasileiro de software e serviços entre 2015 e 2019. É observável que até 2018 esse mercado ainda não havia se recuperado da crise brasileira de 2015, e então em 2019 caiu novamente.

A ABES [11] mostra que apenas 19,4% do mercado brasileiro de software foram preenchidos com Software nacional, enquanto 78,5% vieram do exterior. Além disso, em 2019, havia 21.020 empresas de software em operação: 26,3% em desenvolvimento de software; 32% em serviços; e 41,7% na distribuição e comercialização. Adicionalmente, as Pequenas e Médias Empresas (PME) constituem 95,3% delas.

[10] ABES, “Mercado Brasileiro de Software 2020.”

[11] ABES.

Tabela 4-3 – Evolução do Mercado Brasileiro de Software 2015/2019

Area	Item	2015 (milhões USD)	2016 (milhões USD)	2017 (milhões USD)	2018 (milhões USD)	2019 (milhões USD)
Software	Desenvolvimento Nacional	2.736	1.947	1.961	2.256	1.995
	Desenvolvimento no Exterior	9.601	6.528	6.220	8.223	8.061
	Mercado de Exportação	245	177	174	200	213
Serviços	Desenvolvimento Nacional	12.799	9.167	9.360	10.985	9.411
	Software sob Encomenda	1.404	989	996	1.198	1.003
	Desenvolvimento no Exterior	97	70	69	79	68
	Mercado de Exportação	680	499	495	566	608
Total		*27.562*	*19.377*	*19.275*	*23.507*	*21.359*

Fonte: Compilada pelo autor com dados da ABES[12].

Os dados mostram que os setores Finanças (26,4%) e Telecom (23,2%) constituem cerca de metade do mercado local, seguidos por Indústria (20%), Comércio (10,8%) e Governo (6,3%) como os principais consumidores de Software.

A Tabela 4-4 apresenta os principais *players* do mercado global de Software e serviços em 2018. Pode-se observar que o Brasil está atrás da Austrália no ranking mundial, embora a economia brasileira seja cerca de 30% maior que a australiana. Além disso, o Reino Unido e a França

[12] ABES, "Mercado Brasileiro de Software," 2016; ABES, "Mercado Brasileiro de Software," 2017; ABES, "Mercado Brasileiro de Software," 2018; ABES, "Mercado Brasileiro de Software 2019"; ABES, "Mercado Brasileiro de Software 2020."

têm mercados muito maiores do que o Brasil, embora com economias de tamanhos semelhantes. Disso, depreende-se que há espaço para crescimento da indústria brasileira de software.

Tabela 4-4 – Mercado Global de Software e Serviços em 2018

País	Posição	Software & Serviços 2018 (bilhões de USD)	Participação Global 2018
EUA	1	563	46,1%
Japão	2	79	6,5%
Reino Unido	3	75	6,2%
Alemanha	4	65	5,4%
França	5	47	3,9%
China	6	41	3,4%
Canadá	7	31	2,5%
Austrália	8	24	2,0%
Brasil	9	23	1,9%
Países Baixos	10	21	1,7%
Itália	11	20	1,6%
Espanha	12	17	1,4%
Índia	13	16	1,3%
Suíça	14	16	1,2%
Suécia	15	13	1,1%
Coreia do Sul	16	12	1,0%
Dinamarca	17	9	0,7%
Outros	---	148	12,1%
Total	---	1.220	100,0%

Fonte: Compilada pelo autor com dados da ABES[13].

[13] ABES, “Mercado Brasileiro de Software 2019.”

A situação brasileira fica ainda pior em 2019, conforme mostra a Tabela 4-5. Os símbolos à direita de cada coluna indicam o status relativo em comparação com 2018.

Tabela 4-5 – Mercado Global de Software e Serviços em 2019

País	Posição		Software & Serviços 2019 (USD Billions)		Participação 2019	
EUA	1	●	615,4	▲	46,2%	▲
Japão	2	●	83,1	▲	6,2%	▼
Reino Unido	3	●	81,9	▲	6,2%	▼
Alemanha	4	●	72,9	▲	5,5%	▲
França	5	●	52,8	▲	4,0%	▲
China	6	●	49,1	▲	3,7%	▲
Canada	7	●	32,8	▲	2,5%	▼
Austrália	8	●	26,0	▲	2,0%	▼
Países Baixos	9	▲	23,1	▲	1,7%	▲
Itália	10	▲	22,1	▲	1,7%	▲
Brasil	11	▼	20,5	▼	1,5%	▼
Espanha	12	●	18,6	▲	1,4%	▼
Índia	13	●	17,3	▲	1,3%	▼
Suíça	14	●	17,1	▲	1,3%	▲
Suécia	15	●	14,1	▲	1,1%	▼
Coreia do Sul	16	●	13,0	▲	1,0%	▼
Dinamarca	17	●	10,3	▲	0,8%	▲
Outros	---	●	160,9	▲	12,1%	▼
Total	---	●	1,331,0	▲	100,0%	●

Fonte: Compilada pelo autor com dados da ABES[14].

[14] ABES, “Mercado Brasileiro de Software 2020.”

O Brasil caiu duas posições globalmente e agora está atrás da Holanda e da Itália também. Além disso, foi o único país a apresentar um mercado retraído, em um cenário de crescimento global. Isso se explica, em parte, pelo fato de a indústria local de software e serviços ser concentrada e altamente dependente do mercado nacional, sendo apenas 2,3% de sua receita proveniente do mercado externo. Portanto, quando a economia local não tem um bom desempenho, não há outro mercado para apoiar esse setor. Ademais, em 2019, o Brasil ainda reduziu sua já pequena participação anterior de mercado.

Japão, Reino Unido, Canadá, Austrália, Espanha, Índia, Suécia e Coréia do Sul, ao mesmo tempo em que aumentaram suas indústrias, também perderam participação no mercado global em comparação com o ano anterior. Por outro lado, os EUA, Alemanha, França, China, Holanda, Itália, Suíça e Dinamarca aumentaram sua participação global.

4.3 O Mercado de Ciberdefesa e Cibersegurança

Somente em 2015, os EUA investiram USD 75 bilhões em segurança cibernética, e os gastos globais são estimados em USD 1 trilhão entre 2017 e 2021[15]. Esse gasto trilionário é uma tentativa de "parar o sangramento" não só de crimes, mas também de espionagem e coerção, praticada com o uso de cibermeios e patrocinada por indivíduos, quadrilhas ou Estados. Um pensamento comum é que nações como o Brasil, com a escassez de recursos característica de países em desenvolvimento ou emergentes, não serão capazes de investir o suficiente para ter a capacidade de proteção adequada e necessária, e que assim ficarão, por muito tempo ainda, à mercê de "cibersuperpotências" como EUA, China, Rússia, Reino Unido ou mesmo França.

---

[15] Morgan, "Cyber Security Industry Outlook : 2017 to 2021."

O mercado brasileiro de cibersegurança, em 2018, era estimado em cerca de USD 2 bilhões[16]. Este valor é muito menor que o dos EUA; na verdade, é desproporcionalmente menor, considerando os tamanhos relativos das duas economias e as perdas geradas por violações de cibersegurança. Portanto, o mercado brasileiro está muito provavelmente subestimado até agora, possivelmente devido à falta de consciência situacional adequada sobre o tema. Isso pode ter começado a mudar com uma recente onda de ciberataques de ponta, como o que paralisou o Superior Tribunal de Justiça, fechando o tribunal por mais de uma semana[17]. Com efeito, um atentado que ofendeu a soberania brasileira, ao afetar a possibilidade de exercer uma reconhecida "função elementar de Estado", e envolveu o Comando Cibernético Brasileiro (ComDCiber) e a Polícia Federal nas investigações[18].

Israel, Irã e Coreia do Norte, no entanto, demonstram que é possível para nações em estágios inferiores de desenvolvimento "abreviarem" este novo domínio da geopolítica e, assim, se tornarem atores relevantes no ciberespaço. No entanto, os embargos internacionais ao Irã e à Coréia do Norte limitam seu alcance no mercado global. Israel, por outro lado, concentrou enormes investimentos realizados em *startups* focadas em cibersegurança, tendo se tornado o segundo destino desse tipo de investimento no mundo[19]. Somente em 2015, 300 empresas de cibersegurança ativas

---

[16] Brigatto, "Tempest, Empresa de Segurança Digital, Compra Integradora EZ-Security."

[17] Lima, "Ataque Hacker No STJ: O Que Se Sabe Sobre o Maior Ataque Da História"; Paganini, "Brazil's Court System Shut down after a Massive Ransomware AttackSecurity Affairs."

[18] Lima, "Ataque Hacker No STJ: O Que Se Sabe Sobre o Maior Ataque Da História."

[19] Solomon, "Israel Wins Second-Largest Number of Cybersecurity Deals Globally."

exportaram USD 3,5 bilhões em software, 5% do mercado cibernético mundial[20]. Mas o mercado israelense é limitado por sua proximidade política com os EUA e seu confronto histórico com países de maioria religiosa muçulmana.

De olho neste mercado mundial em crescimento, o governo do Reino Unido publicou sua Estratégia de Exportação de Cibersegurança 2018. Possivelmente, o aspecto mais relevante disso foi o reconhecimento oficial da cibersegurança como um mercado crescente que merece atenção oficial e esforços diplomáticos.

> O ritmo acelerado da mudança digital traz uma grande oportunidade de promover a experiência em cibersegurança do Reino Unido para os mercados internacionais. Regimes de controle de exportação robustos garantirão que os direitos humanos sejam uma parte essencial do processo.[21]

Embora indique restrições às suas ações para mercados específicos: "Em mercados prioritários, o DIT [Departamento de Comércio Internacional] atuará como um consultor de confiança para apoiar as empresas britânicas em licitações de grandes oportunidades, principalmente vendendo para governos estrangeiros e provedores de Infraestruturas Nacionais Críticas (CNI)"[22].

Tendo uma indústria de software consolidada, o Brasil também poderia explorar o crescente mercado internacional de cibersegurança e ciberdefesa, tendo alguma vantagem estratégica em relação aos britânicos, americanos e israelenses.

4.4 Oportunidade Estratégica

O mercado de produtos de defesa é muito representativo na economia mundial. No entanto, como a

---

[20] Azulai, "Israel Seeks Larger Slice of Security Market."

[21] UK-Department for International Trade, "Cyber Security Export Strategy."

[22] UK-Department for International Trade.

maioria dos produtos militares pode ser usada tanto para o ataque quanto para a defesa, os exportadores desses produtos devem ser seletivos com quem os compra; caso contrário, eles podem vender um produto que poderá vir a ser usado contra eles mesmos.

Cibervulnerabilidades também são responsáveis por restrições à aquisição e venda de produtos. Já em 2001, funcionários da inteligência americana acreditavam "que certos equipamentos e softwares importados da Rússia, China, Israel, Índia e França" estavam infectados com "dispositivos" capazes de "ler dados e destruir sistemas", embora essa suspeita fosse difícil de provar[23]. Mais recentemente, hardware falsificado foi identificado em sistemas adquiridos pelo DoD[24]. Um relatório da Comissão Permanente de Inteligência da Câmara dos Estados Unidos em 2012 restringiu a compra de equipamentos das empresas chinesas Huawei e ZTE[25].

Em 2015, Israel invadiu computadores russos e identificou informações confidenciais dos EUA em bancos de dados russos. Quando os israelenses informaram aos americanos, as investigações culminaram na proibição de aquisição de software da empresa russa de cibersegurança Kaspersky[26].

Nem mesmo equipamentos fornecidos por empresas de países tradicionalmente neutros podem ser considerados insuspeitos e inalcançáveis pelos tentáculos de países agressores. A empresa suíça Crypto AG, fabricante de

---

[23] Adams, "Virtual Defense."

[24] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy."

[25] Banach, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE."

[26] Nakashima, "Israel Hacked Kaspersky, Then Tipped the NSA That Its Tools Had Been Breached"; Whittaker, "What Is Kaspersky ' s Role in NSA Data Theft ? Here Are Three Likely Outcomes A Bombshell News Report on Kaspersky ' s Alleged Involvement in the Theft of."

criptógrafos usados em mais de 120 países, pertenceu, entre 1970 e 2018, a uma parceria altamente secreta entre a CIA e o serviço de inteligência alemão BND, quando os equipamentos vendidos pela empresa eram sabotados para que aquelas agências tivessem acesso às informações criptografadas por eles[27]. Russos e chineses, desconfiados da neutralidade da empresa, nunca usaram seus dispositivos. É relevante notar que os alemães saíram da parceria na década de 1990, temerosos das consequências de possíveis revelações públicas, com os americanos permanecendo sozinhos na operação ainda por cerca de duas décadas mais.

Agora, o governo dos EUA acusa a Huawei, líder mundial em telefonia 5G, de ter conexões obscuras com a inteligência chinesa. Os EUA argumentam que preferem o uso de equipamentos da sueca Ericsson e da finlandesa Nokia, mesmo que mais caros, e personalidades do governo norte-americano até sugeriram a aquisição do controle acionário dessas empresas[28].

Os Estados Unidos também estão pressionando seus aliados a vetar o uso da tecnologia 5G chinesa. Em 2019, o governo do Reino Unido anunciou que usaria a tecnologia 5G da Huawei, embora limitando seu uso a áreas não sensíveis. Sob forte pressão do governo dos EUA, em maio de 2020, o Reino Unido anunciou a proibição total da empresa em redes 5G e 4G. A alemã Deutsche Telekom (32% estatal), respondeu que excluir a Huawei de suas redes 5G seria o 'Armagedom' e, embora não restringindo sua participação, anunciou recentemente que a Ericsson foi escolhida como sua fornecedora de tecnologia 5G[29]. Sob enorme pressão dos EUA

---

[27] Miller, "How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades - Washington Post."

[28] Kharpal, "US Should Take Stake in Nokia, Ericsson to Counter Huawei in 5G: Barr."

[29] Petzinger, "Deutsche Telekom Describes Potential Huawei Ban as 'Armageddon' Scenario"; Alleven, "Deutsche Telekom Selects Ericsson

em relação à participação da Huawei nas redes brasileiras, com o embaixador dos EUA ameaçando "consequências", os militares brasileiros teriam dito ao seu governo que "a mesma eventual exposição que o Brasil pode sofrer com a tecnologia chinesa com a Huawei também ocorrerá com qualquer outra empresa"[30]. Na verdade, uma posição muito pragmática, considerando-se os casos Crypto AG, Cisco e Juniper.

Conforme detalhado em outro trabalho, armas cinéticas geralmente podem ser usadas tanto defensivamente quanto ofensivamente. Mas não as ciberarmas[31]. Assim, um software defensivo jamais se tornaria um problema para os exportadores, a menos que eles tivessem a intenção de atacar seus clientes algum dia. E não é provável que seja o caso de países historicamente não-agressivos. Por outro lado, seus clientes tenderiam a evitar produtos defensivos produzidos por países considerados agressivos (ou por países com laços estreitos com esses), por temerem que pudessem deixar espaço para permitir vulnerabilidades intencionais (*backdoors*) no futuro. Novamente, esse não parece ser o caso de nações não-agressivas.

Assim, o mercado internacional para esses produtos torna-se virtualmente ilimitado para estados não-agressivos. E é mais provável que se beneficiem da confiança que conquistaram nas últimas décadas. Ou pelo menos podem capitalizar a desconfiança acumulada por nações consideradas ciberagressivas como EUA, China, Rússia, ou mesmo Israel

---

for 5G RAN in Germany"; Ericsson, "Deutsche Telekom and Ericsson Strengthen Partnership with 5G Deal - Ericsson."

[30] Amado, Barreto, and Matsui, "O Recado Das Forças Armadas Ao Ministério Da Defesa Sobre o 5G - Época"; Rosa and Antunes, "Embaixador Dos EUA Alerta Que Se Brasil Permitir Chinesa Huawei No 5G Enfrentará 'consequências' - Jornal O Globo."

[31] Malagutti, *Software Power: Um Olhar Brasileiro*.

ou Reino Unido (e os demais Five Eyes), devido ao seu comportamento agressivo e sua proximidade com os EUA.

4.5 Conclusão

O mercado de internacional de produtos e serviços de cibersegurança e ciberdefesa oferece uma excelente oportunidade a ser explorada por nações não-agressivas, que poderia permitir o desenvolvimento de software, hardware e serviços. Isso poderia mais do que justificar investimentos estatais orientados por boas políticas públicas. Na economia globalizada de hoje, toda nação terá interesses que conflitem com pelo menos um dos citados países com cultura agressiva. Portanto, sentem a necessidade de proteger tais interesses de acordo.

As políticas públicas que visam incrementar as capacidades de cibersegurança e ciberdefesa nacionais podem aumentar a resiliência e reduzir as perdas, compensando parcialmente (se não totalmente) os custos dessas capacidades. E se essas políticas forem elaboradas de uma forma que também fomente uma indústria de software vibrante e capaz, podem consolidar um mercado de software e serviços de cibersegurança e ciberdefesa que gera empregos e receitas muito superiores aos dos setores da indústria de transformação e do agronegócio. Com apoio diplomático adequado para explorar iniciativas comerciais internacionais, novos mercados podem ser abertos e explorados por nações não-agressivas enquanto desenvolvem suas próprias capacidades.

4.6 Referências

ABES. “Mercado Brasileiro de Software,” 2016.

———. “Mercado Brasileiro de Software,” 2017.

———. “Mercado Brasileiro de Software,” 2018.

———. “Mercado Brasileiro de Software 2019,” 2019.

———. “Mercado Brasileiro de Software 2020,” 2020.

Adams, James. “Virtual Defense.” *Foreign Affairs* 80, no. 3 (2001): 98. https://doi.org/10.2307/20050154.

Alleven, Monica. “Deutsche Telekom Selects Ericsson for 5G RAN in Germany.” *FierceWireless*, 2020. https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany.

Amado, Guilherme, Eduardo Barreto, and Naomi Matsui. “O Recado Das Forças Armadas Ao Ministério Da Defesa Sobre o 5G - Época.” *Época*, 2020. https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588.

Azulai, Yuval. “Israel Seeks Larger Slice of Security Market.” *Globes*, 2016.

Banach, William. “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,” 2012. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE Investigative Report (FINAL).pdf.

Brasil-GSI. “Estratégia Nacional de Segurança Cibernética (e-Ciber).” *Participa.Br*. Brasília, 2020. http://www.participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber.

Brigatto, Gustavo. “Tempest, Empresa de Segurança Digital, Compra Integradora EZ-Security.” *Valor Econômico*. 2018.

BSA Foundation. “Software: A € 910 Billion Catalyst for the EU Economy,” 2016.

———. “Software: Growing US Jobs and the GDP,” 2019.

———. “The $1 Trillion Economic Impact of Software,” 2016.

———. “The Growing €1 Trillion Economic Impact of Software,” 2017.

Campbell, Duncan. *Development of Surveillance Technology and Risk of Abuse of Economic Information Part 2/5*, 1999. http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf.

Ericsson. “Deutsche Telekom and Ericsson Strengthen Partnership with 5G Deal - Ericsson.” Ericsson.com - Press Releases, 2020. https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal.

Gandel, Stephen. “Lloyd’s CEO: Cyber Attacks Cost Companies $400 Billion Every Year | Fortune.” *Fortune*, 2015. https://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Penguin Books, 2014.

Kharpal, Arjun. “US Should Take Stake in Nokia, Ericsson to Counter Huawei in 5G: Barr.” *CNBC*, 2020.

Lewis, James. “Economic Impact of Cybercrime — No Slowing Down,” 2018.

Lima, Wilson. “Ataque Hacker No STJ: O Que Se Sabe Sobre o Maior Ataque Da História.” *Gazeta Do Povo*. 2020. https://www.gazetadopovo.com.br/republica/hacker-stj-tribunal-ataque-pf-investiga/.

Lynn, William. “Defending a New Domain: The Pentagon’s Cyberstrategy.” *Foreign Affairs* 89, no. 5 (2010).

Malagutti, Marcelo. *Software Power: Um Olhar Brasileiro*. Brasília: Instituto Vegetius, 2022.

Miller, Greg. “How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades - Washington Post.” *The Washington Post*, 2020.

Morgan, Steve. “Cyber Security Industry Outlook : 2017 to 2021.” *CSO*, 2016.

Nakashima, Ellen. “Israel Hacked Kaspersky, Then Tipped the NSA That Its Tools Had Been Breached.” *The Washington Post*, 2017.

Paganini, Pierluigi. “Brazil’s Court System Shut down after a Massive Ransomware AttackSecurity Affairs.” *Security Affairs*, 2020.

Petzinger, Jill. “Deutsche Telekom Describes Potential Huawei Ban as ‘Armageddon’ Scenario.” *MSN*, 2020. https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM.

Rosa, Bruno, and Cláudia Antunes. “Embaixador Dos EUA Alerta Que Se Brasil Permitir Chinesa Huawei No 5G Enfrentará ‘consequências’ - Jornal O Globo.” *O Globo*, 2020.

Solomon, Shoshanna. “Israel Wins Second-Largest Number of Cybersecurity Deals Globally.” *The Times of Israel*, 2018.

UK-Department for International Trade. “Cyber Security Export Strategy,” 2018.

United States. “Foreign Economic Espionage in Cyberspace,” 2018.

Whittaker, Zack. “What Is Kaspersky ’ s Role in NSA Data Theft ? Here Are Three Likely Outcomes A Bombshell News Report on Kaspersky ’ s Alleged Involvement in the Theft of.” *ZDNet*, 2017.

Página intencionalmente deixada em branco.

5 Elevando o Software Power Brasileiro

5.1 Introdução

Ofensas cibernéticas, patrocinadas ou não por estados, tornar-se-iam práticas corriqueiras. Qualquer nação que pretenda evitar a coação ou ser prejudicada em negociações na arena internacional, que pretenda melhorar sua capacidade de ciberdissuasão e de ciberresiliência, ou que queira disputar o gigantesco mercado de produtos e serviços de cibersegurança e ciberdefesa deve enfrentar os desafios de como obter os melhores resultados possíveis com políticas públicas adequadas.

E isso nos remete de volta aos fundamentos da Teoria da Dissuasão: racionalidade no tocante a custo e valor.

5.2 O Caso em Favor da Ciberdissuasão por Negação

Ciberdissuasão por Medo apresenta muitas dificuldades inerentes. Todavia, a mais complexa talvez seja a necessidade de capacidades ofensivas capazes de instilar medo e infligir dor. Pode ser economicamente mais barata que a Dissuasão por Negação, mas dada a natureza efêmera das ciberarmas ofensivas e a dúbia efetividade das mesmas contra defesas capazes seu resultado é incerto.

> Uma criteriosa análise conceitual e um detalhado exame dos dados empíricos corrobora nossa hipótese: o desenvolvimento e implantação de ciberarmas potencialmente destrutivas contra alvos protegidos requererá recursos significativos, dados de inteligência bastante específicos e difíceis de obter, e tempo para preparar, lançar e executar um ataque. (RID e MCBURNEY, 2012)

Adicionalmente, o risco de descoberta (dos implantes previamente instalados) que venha a gerar ataques

preemptivos ou retaliatórios, não necessariamente de mesma natureza, pode elevar seu custo final a níveis inaceitáveis.

Possivelmente, no entanto, o maior custo relativo à Ciberdissuasão por Medo seja aquele relacionado aos valores morais: ciberarmas ofensivas vão contra a cultura (estratégica e institucional) de Estados não-agressivos. Estes provavelmente não terão a intenção, nem o arcabouço legal, para suportar o desenvolvimento, aquisição ou desenvolvimento dessas ciberarmas ofensivas.

A Ciberdissuasão por Futilidade, por sua vez, somente será atingida se os oponentes perceberem que os custos das ferramentas de ataque contra o dissuasor não serão justificados. Assim, para impor a lógica da futilidade, é necessário "elevar a barra" dos custos dos oponentes, tornando-os inaceitáveis ou inviáveis, ou ao menos não provendo suficiente retorno do investimento para justificá-los.

A Ciberdissuasão por Entranhamento (ou Embricamento), por sua parte, depende da criação de uma interdependência do ciberespaço do dissuasor e do dissuadido de tal monta que somente pode ser criada a longo prazo, e que ainda assim somente será aplicável a uns poucos Estados-alvos,

Por fim, a Ciberdissuasão por Individualização demanda capacidades forenses e de inteligência muito significativas, bem como a capacidade de impor sanções no contexto internacional, fora das fronteiras do dissuasor,

A única opção lógica restante, então, é a Ciberdissuasão por Negação, seja ela por meio da negação de quaisquer benefícios ao oponente ou pela imposição de elevados custos por meio de fortes defesas.

O desafio é criar ciberdefesas que incrementem a negação de área e a resiliência, e que sejam suficientemente efetivas para negar ao adversário o benefício de um ataque a

despeito da força de suas cibercapacidades ofensivas[1]. Não é o caso de se pretender manter o inimigo fora das redes defendidas, mas de tornar difícil (custoso) que ele atinja os objetivos visados[2].

Detectar e derrotar preparações para o ataque tornam o mesmo sem efeito. Mais ainda, defesas fortalecidas servem para dissuadir, seja por serem percebidas pelo atacante como muito efetivas ou por reduzirem a efetividade do assalto ao ponto deste ser considerado uma forma ineficiente de uso de recursos [3].

5.3 Como Implementar Ciberdissuasão por Negação?

Esta seção, na forma de "propostas de políticas" (*policy briefing*), contém recomendações para a aplicação de elementos de todas as expressões do poder nacional para atingir o objetivo político de desenvolver um *Software Power* nacional capaz de evitar a coação por uma nação estrangeira. Em resumo, propostas para comporem uma macro-estratégia (*grand strategy*) nacional.

As políticas propostas são um tanto independentes, e cada uma pode ser implementada em diferentes níveis de profundidade, considerando seus custos e o valor dos ativos defendidos. Somadas elas podem prover um elevado grau de Negação para o ciberespaço de qualquer nação.

Embora os contextos nacionais possam ser bastante diferentes, recomendações genéricas são factíveis, aqui agrupadas por área.

---

[1] Lynn, “Defending a New Domain: The Pentagon’s Cyberstrategy.”

[2] Carr, “Cyber Attacks: Why Retaliating against China Is the Wrong Reaction.”

[3] Lukasik, “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains.”

5.3.1 Avaliação Situacional

Em termos práticos, a dissuasão cibernética é um sistema bastante dinâmico. Como tal, uma avaliação situacional abrangendo o uso de indicadores para a compreensão das capacidades e ameaças reais deve constituir-se na etapa inicial de qualquer política[4].

Entendido o contexto específico, a implementação das cibercapacidades dissuasórias poderá ser estruturada em políticas específicas, estratégias, livros verdes e brancos, normas, manuais, guias e, ao final, diretivas e atividades.

5.3.2 Arcabouço Legal

A busca por um arcabouço legal internacional é essencial. Ela é, por óbvio, muito difícil, ainda que necessária. O sucesso obtido por Brasil e Alemanha na ONU a respeito da privacidade no contexto imediato pós-Snowden é um sonoro exemplo de como um momento político particular pode ajudar. Acordos podem ser implementados em foros mais limitados, como nos casos da Convenção de Budapeste e do acordo Sino-Russo, e então servirem de base para a posterior adesão de outros países[5]. Embora de cumprimento difícil de verificar, eles podem ao menos prover suporte para ações diplomáticas no caso de alguma das partes descumpri-los.

Em paralelo, é necessário trabalhar na infraestrutura (arcabouço) legal nacional. Equalizar o cibercrime ao crime comum (tipificar os crimes) é um bom começo. Isso evita a não punição de ciberofensas devido a lacunas na legislação. Mas, em seguida, é necessária a implementação de legislação específica para o cibercrime. Adicionalmente, é necessário adaptar a legislação nacional para permitir a coleta de inteligência e evidências, bem como seu uso para suportar

---

[4] Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems."

[5] Korzak, "The Next Level For Russia- China Cyberspace Cooperation ?"

punições de perpetradores de crimes realizados no (ou com o suporte do) ciberespaço. Embora dificilmente possam atingir efeitos punitivos práticos, os indiciamentos de oficiais chineses e iranianos pelo FBI proveem suporte político para o governo americano, tanto internamente como na arena internacional.

Adicionalmente, a legislação relativa às concessões públicas (geralmente eletricidade, gás, água, telecomunicações, transporte público e emissoras de rádio e TV) deve ser alterada para requerer que as empresas privadas que as gerenciam implementem determinados níveis de cibersegurança em suas redes.

5.3.3 Uma Agência Nacional de Cibersegurança

É necessária a criação de uma Agência ou Autoridade Nacional de Cibersegurança que seja o ponto focal da nação para o tema e concentre as orientações e ações nacionais no tocante à cibersegurança nos mais variados aspectos aqui propostos.

Exemplos desse tipo de Agência podem ser a ACN (Agenzia Cybersicurezza Nazionale) Italiana, a ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) francesa, ou o NCSC (National Cyber Security Centre) britânico. Em todos os casos, tais agências são de natureza civil, mas trabalham em coordenação com seus pares militares. Outrossim, a Agência brasileira deve atuar em coordenação com o ComDCiber, responsável pela ciberdefesa nacional.

Dentre outras tarefas, essa agência deveria gerir um *Cyber Security Incident Response Team* (CSIRT), possivelmente o CTIR.Gov, hoje integrante do GSI, com funções um pouco ampliadas.

A Agência também deve ser a responsável pela definição dos níveis e prazos de implementação das regras estabelecidas tanto para o setor público quanto para o setor privado. Essas implementações deveriam ser regularmente

avaliadas, acreditadas e certificadas por essa agência (ou por uma certificadora credenciada por ela). Como contrapartida pelos custos adicionais envolvidos, as companhias compradoras de bens e serviços de cibersegurança com implementações acreditadas poderiam ser compensadas com diferentes níveis de isenções tributárias, para evitar que aumentem seus preços para os usuários. Já as empresas fornecedoras de bens e serviços de cibersegurança acreditados poderiam gozar de pequenas margens de preferência nas compras públicas desses itens.

A Agência também deve atuar na proposição de currículos escolares e acadêmicos, no financiamento de pesquisas aplicadas, e na promoção de exercícios e competições nacionais, bem como apoiar a participação de equipes nacionais em eventos similares internacionais.

Outras funções dessa Agência devem ser as de suas congêneres já citadas.

5.3.4 Educação e Treinamento

Muitas ciberofensas tiram proveito de práticas pobres de segurança pelos usuários. Educar os usuários nas melhores práticas em segurança cibernética elevaria os custos de muitas das ofensas. Os empregados das empresas (e do governo) deveriam ser retreinados em intervalos regulares, reforçando suas habilidades e sua motivação.

O treinamento de investigadores especializados em forense digital não vai, inicialmente, evitar ciberofensas, mas tornará mais fácil identificar seus perpetradores. Treinar desenvolvedores de software na implementação de arquiteturas de segurança de sistemas também é essencial, como o é treinar analistas de segurança e a criação de CSIRTs.

Também é necessário treinar hackers "chapéus brancos" para aplicarem as técnicas dos adversários contra as redes defendidas, para testar suas vulnerabilidades antes que as mesmas sejam exploradas pelo inimigo, atuando como os

"times vermelhos" que simulam o inimigo em exercícios militares, como os EUA e outros países já fazem [6].

Também essencial é trabalhar nos currículos de cursos de mestrado em universidades, similarmente ao que já fazem a NSA americana e o GCHQ britânico, e enviar estudantes para centros de pesquisa e universidades internacionais avançadas, formando pesquisadores capazes de desenvolverem ferramentas e técnicas de defesa cibernética. Competições anuais de segurança cibernética, tanto em tecnologia quanto em políticas, revelariam novos talentos, elevando também o interesse pelo assunto e reforçando sua importância para o público.

5.3.5 Implementação de uma Arquitetura de Segurança

O conceito de arquitetura de segurança aqui apresentado engloba tanto as fronteiras quanto o interior das redes.

Ferramentas de defesa automatizadas, preferencialmente inteligentes e capazes de aprender, necessitam ser adquiridas ou desenvolvidas. Essas ferramentas constituiriam aquilo que se denomina defesas ativas, sendo "parte sensores, parte sentinelas, parte atiradores" [7]. Elas devem englobar o escopo completo do modelo da cadeia destrutiva cibernética. E assim não apenas trabalhar como uma Linha Maginot nas fronteiras externas (interfaces) das redes defendidas.

A elaboração de diretivas para sistemas de segurança padronizados, incluindo padrões para a configuração das ferramentas, podem ser um ativo de grande valor em termos de tempo e efetividade, com rápida replicação de boas práticas. Alvos de grande valor devem ser protegidos por ferramentas e protocolos desenvolvidos para sua encriptação e para

---

[6] Lynn, “Defending a New Domain: The Pentagon’s Cyberstrategy.”

[7] Lynn.

assegurar que eles não permaneçam por muito tempo no mesmo local, tornando-se alvos fáceis, e os sistemas críticos devem ser apartados sempre que possível.

O uso de "times vermelhos" para aferir a segurança dos sistemas traria um duplo benefício, assegurando tanto a resiliência e confiabilidade dos sistemas quanto à prontidão dos próprios "times vermelhos".

Redes de computadores são essencialmente sistemas descentralizados, onde a confiança é essencial [8]. Protocolos para gerenciamento de identidades integrados ao controle de acesso, incluindo a autenticação, autorização, contabilização e responsabilização devem ser implementados. Autenticação identifica o usuário, e deve ser reforçada pelo uso de um componente lógico, como uma senha ou um dado pessoal, e por um componente físico (token, cartão de acesso, *smartphone*) ou biométrico (impressão digital, *palm vein*, imagem de íris ou retina, ou reconhecimento facial). Depois de autenticado, o usuário precisa obter autorização para acessar os ativos e serviços ou executar ações na rede. A contabilização é obtida pelo registro dos recursos consumidos e dos serviços utilizados, enquanto a responsabilização é feita com base nas ações tomadas e nos ativos acessados na rede.

5.3.6 Preparação para Resposta e Resiliência

Dado que alguns ataques certamente serão bem-sucedidos, os defensores devem ter as habilidades e as ferramentas para reconstituírem o que for destruído ou danificado, e para executarem análises para o entendimento do *modus operandi* das ferramentas de ataque, bem como dos sinais de advertência que devem ter sido desconsiderados [9]. Os defensores então deverão "ensinar" suas ferramentas

---

[8] Grimaila, Mills, and Beeker, “Applying Deterrence in Cyberspace.”

[9] Lukasik, “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains.”

defensivas, ou desenvolver (ou adquirir) novas, para reduzirem a probabilidade ou efetividade de ataques similares futuros.

A resiliência pode ser obtida de muitas formas: backups “quentes” (ou dinâmicos), que permitem a criação de pontos de recuperação sem a interferência na operação normal do sistema; "clusters passivos", onde o sistema (ou sítio) backup permanece em espera até ser ativado; "clusters ativos", onde as múltiplas instâncias do sistema processam simultaneamente, possivelmente em diferentes sítios, e que permitem "distribuição de carga" para compensar a falha de uma das instâncias pelas demais; e "virtualização", criação de máquinas virtuais, por meio de software, que agem como computadores reais com um sistema operacional sobre o qual são instalados os sistemas aplicativos, e que podem ser dinamicamente movidas de um equipamento físico para outro.

Utilizando-se instalações distribuídas aumenta-se o número de alvos, ao tempo em que a criação de instalações “ilusórias” (ou falsas), atrás das quais podem ser ocultadas aquelas verdadeiras, pode enganar o oponente e prover contrainteligência (por meio de "potes de mel”, ou *honeypots*).

Também útil é a habilidade de se desconectar do atacante durante os estágios iniciais de um ataque [10].

5.3.7 Adoção de Boas Práticas Internacionais

O próprio ciberespaço provê muitas fontes de informação sobre boas práticas que podem e devem ser usadas.

Governos publicam políticas, estratégias, diretivas, guias e relatórios em seus sítios oficiais. A Agência Europeia para Segurança de Redes e Informações (ENISA) tem guias e recomendações em diversas línguas. O Centro Cooperativo de Excelência em Defesa Cibernética da OTAN (NATO/CCDCOE) também provê bons textos contendo análises e recomendações práticas.

---

[10] Lukasik.

Em seu "lado escuro" (*dark web*) a Internet também provê muitas informações e ferramentas para infiltração. Algumas delas são gratuitas, mas outras, como vulnerabilidades *zero-day*, podem custar dezenas de milhares de dólares. Esses ativos devem ser monitorados e usados por "chapéus brancos" e "times vermelhos" para testar as defesas implementadas.

5.3.8 Desenvolvimento de Tecnologia Autônoma

Considerando-se que portas dos fundos (*backdoors*) de fato existem, qualquer nação que pretenda estar segura no contexto cibernético não pode confiar apenas em ativos importados, ao menos para seus sistemas críticos, a não ser que seus códigos sejam abertos para inspeção.

Há uma argumentação consistente em favor do desenvolvimento de uma distro Linux nacional, bem como de alguns outros itens de software básico ou middleware para se evitar a presença de backdoors[11]. Não obstante, nem todas as tecnologias podem ser desenvolvidas por todos os países. Muitas ferramentas de software de alta qualidade para diversas áreas são de código aberto (*open source*), significando que seu código pode ser analisado para identificar falhas ou portas dos fundos, e para assegurar que a versão executável em uso corresponda àquele código-fonte.

Mas ativos de software comercial, de código não aberto, serão crescentemente necessários. Isso cria a necessidade pelo desenvolvimento de capacidades técnicas e meios para a avaliação e recusa de códigos de software tanto para o setor privado quanto para aquele público. E a aplicação de sanções a companhias de nações estrangeiras envolvidas em atividades maliciosas deveria rapidamente persuadi-las no sentido de que cooperarem com seus governos não é do seu

---

[11] Malagutti and Gama Neto, “Por Que o Brasil Deveria Adotar Uma Distro Linux Própria?”

melhor interesse econômico[12]. De fato, após as revelações de Snowden de que companhias como Google e Facebook, dentre outras, trabalhavam com a NSA em atividades de vigilância, elas recuaram. Oito gigantes tecnológicas americanas, incluindo as acima mencionadas e a Microsoft, criaram um movimento denominado *Reform Government Surveillance* e começaram a pressionar o Senado norte-americano a impor limites nos direitos de vigilância do governo, em benefício de seus clientes (e embora não publicamente comunicado, de seus negócios)[13].

5.3.9 Desenvolvimento de Ferramentas e Técnicas Forenses e de Atribuição

Procedimentos para investigação forense e atribuição devem ser desenvolvidos, melhorados e normatizados, combinando diferentes técnicas dado que nenhuma isoladamente vai funcionar para todos os ataques [14]. Nesta área, tanto a DARPA quanto o DHS americano estão desenvolvendo pesquisas para melhorar a habilidade do governo de atribuir ataques e obstruir capacidades de intrusos[15].

Capacidades de atribuição são mandatórias para retaliação, embora isso esteja mais conectado à ciberdissuasão por medo que àquela por negação. Todavia, não se está falando aqui do uso da atribuição para aplicação de ataques preemptivos ou retaliatórios, mas sim para a aplicação da lei e de sanções comerciais (no caso de empresas) ou diplomáticas

---

[12] Adams, “Virtual Defense.”

[13] Miller and Wyatt, “Tech Giants Issue Call for Limits on Government Surveillance of Users.”

[14] Grimaila, Mills, and Beeker, “Applying Deterrence in Cyberspace.”

[15] US-DHS, “A Roadmap for Cybersecurity Research”; Lynn, “Defending a New Domain: The Pentagon’s Cyberstrategy.”

(no caso de estados). Outrossim, de Ciberdissuasão por Individualização.

5.4 Conclusão

Este capítulo apresentou um pequeno conjunto de propostas de políticas públicas correntemente em uso em diferentes países, e que poderiam ser implementadas no Brasil de forma relativamente simples e rápida, em sua maioria.

Em sua totalidade, ainda que os custos possam inicialmente parecer elevados, eles se tornam irrisórios quando comparados ao custo e às perdas postos pela atual inação frente ao crescente número de ciberofensas perpetradas no (ou contra o) Brasil. Diante de perdas da ordem de USB 22 bilhões anuais para a economia nacional, a mera redução de 5% significaria uma economia de mais de USD 1 bilhão ao ano, o que, por si só, justificaria um enorme investimento no setor de produtos e serviços de cibersegurança e ciberdefesa.

Se considerarmos que a grande maior parte dos ciberincidentes tem origem em ofensas de baixa complexidade tecnológica, que exploram apenas o desconhecimento e despreparo dos usuários, as práticas aqui propostas têm o potencial de atingirem resultados significativos bastante rapidamente.

Se isso já não fosse motivo bastante, há que se recordar que, como visto, há ainda significativos ganhos de emprego e renda associados ao setor, representando ganhos sociais relevantes para qualquer país.

Portanto, há uma situação de crise e uma janela de oportunidade associada. É um bom momento para contradizer a famosa frase de Roberto Campos, “o Brasil não perde uma oportunidade de perder uma oportunidade”, e “fazermos do limão uma caipirinha”!

5.5 Referências

Adams, James. “Virtual Defense.” *Foreign Affairs* 80, no. 3 (2001): 98. https://doi.org/10.2307/20050154.

Carr, Jeffrey. “Cyber Attacks: Why Retaliating against China Is the Wrong Reaction.” *The Diplomat*, August 2015.

Endsley, Mica. “Toward a Theory of Situation Awareness in Dynamic Systems.” *Human Factors* 37, no. 1 (1995): 32–64.

Grimaila, Michael, Robert Mills, and Kevin Beeker. “Applying Deterrence in Cyberspace.” *IO Journal* 1, no. 4 (2010): 21–27.

Korzak, Elaine. “The Next Level For Russia- China Cyberspace Cooperation ?” Council on Foreign Relations Blog, 2015. https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

Lukasik, Stephen J. “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, edited by National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 99–121. National Academies Press, 2010.

Lynn, William. “Defending a New Domain: The Pentagon’s Cyberstrategy.” *Foreign Affairs* 89, no. 5 (2010).

Malagutti, Marcelo, and Ricardo Gama Neto. “Por Que o Brasil Deveria Adotar Uma Distro Linux Própria?” *Revista Brasileira de Estudos de Defesa* 7, no. 2 (2020): 161–83. https://doi.org/10.26792/RBED.v7n2.2020.75248.

Miller, Claire Cain, and Edward Wyatt. “Tech Giants Issue Call for Limits on Government Surveillance of Users.” *The New York Times*, 2013. http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html?pagewanted=all&_r=0.

US-DHS. “A Roadmap for Cybersecurity Research,” 2009. https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf.

Página intencionalmente deixada em branco.

6 Conclusões

Este livro demonstrou que o Brasil, conquanto tenha começado a construir sua estrutura de ciberdefesa e cibersegurança em paralelo com a maioria de seus pares no sistema internacional, investiu significativamente menos que estes, e assim "perdeu o passo", distanciando-se muito e permitindo a criação de um *gap* em relação aos países do "arco do conhecimento" na área.

Para demonstrar isso, primeiro analisou-se a lacuna entre as capacidades e os investimentos brasileiros e os de outros países com PIB comparável, em termos de poder de compra, mostrando que ela é crescente. Observou-se que a própria estrutura organizacional do Comando de Defesa Cibernética, bem como o tamanho de seu efetivo e até mesmo a subordinação dele, diferem em muito do padrão seguido pela maioria dos países, em boa medida refletindo a cultura estratégica brasileira que evita a confrontação e o empoderamento do Estado.

Em seguida, analisou-se a e-Ciber, demonstrando-se que ela também difere muito de suas congêneres, e reflete muito de nossa cultura e nossas tradições, evitando ser assertiva, sem designar tarefas, recursos e prazos, e assim sendo mais uma "carta de intenções" do que um documento de comunicação estratégica voltado a construir capacidades.

Depois, mostrou-se que a crescente demanda mundial por produtos e serviços de ciberdefesa e cibersegurança, aliada a essa mesma cultura estratégica "não-agressiva", pode representar uma enorme oportunidade estratégica para o país.

Para que o Brasil possa explorar essa janela de oportunidade estratégica que se apresenta, são necessárias ações imediatas e políticas públicas consistentes a curto, médio e longo prazos. Várias dessas medidas foram apresentadas aqui, com o objetivo de suscitar uma discussão mais

aprofundada, mas que não pode tardar, sob pena de perda da janela de oportunidades agora existente.

As propostas apresentadas refletem ações em diversas áreas, o que caracteriza a necessidade de formulação de uma verdadeira "política nacional" apoiada em uma genuína "estratégia nacional", que determine objetivos, meios e recursos, de forma a direcionar esforços, dirimir dúvidas e mitigar riscos e conflitos.

Parafraseando Winston Churchill, esse conjunto de propostas "não significa o fim. Nem sequer o começo do fim. Talvez, o fim do começo" de um debate mais embasado e focado no desenvolvimento de cibercapacidades nacionais que, além de nos permitirem nos defendermos melhor, podem nos permitir ocupar um lugar mais relevante no cenário internacional, e elevar o perfil de emprego e renda de nossa população. *Alea jacta est* (a sorte está lançada)!

Marcelo Malagutti é Pesquisador Sênior do Instituto Vegetius. É Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME) com um ano como Doutorando Visitante no King's College London (Reino Unido); Mestre em Estudos de Guerra pelo King's College London; Diplomado no Curso de Altos Estudos em Política e Estratégia pela Escola Superior de Guerra (ESG); MBA em Estratégia Corporativa pela Fundação Getúlio Vargas (FGV); Bacharel em Ciência da Computação pela Universidade de Brasília (UnB); Agraciado com a Medalha do Pacificador e a Medalha Exército Brasileiro; Empresário do Setor de Software; Membro do King's College Cyber Security Research Group; Membro do King's College Wargaming Network.

Qual a situação atual das cibercapacidades brasileiras? Quais as perspectivas de futuro? Estas são questões respondidas neste livro, escrito com um enfoque didático voltado a explicar elementos relevantes da ciberdefesa e cibersegurança nacionais para pessoas que não necessariamente tenham conhecimento de informática, computação nem tecnologia da informação. Ele apresenta o estado atual da ciberdefesa e da cibersegurança nacionais sob uma perspectiva comparada, usando as lentes da cultura estratégica brasileira. Indo além de simplesmente problematizar o tema, aponta a existência de uma grande oportunidade estratégica, e sugere medidas para não somente elevar nossas capacidades, mas também permitir o aproveitamento da oportunidade apresentada e "fazer do limão uma caipirinha"!

O Instituto Vegetius é uma instituição brasileira, de caráter filantrópico, sem finalidades lucrativas e sem qualquer vinculação política ou partidária, que atua na área social mediante a realização de pesquisas, estudos, análises e ações voltados a auxiliar na melhoria de políticas públicas e tomada de decisão e no engajamento da sociedade nos temas de defesa nacional, segurança nacional e internacional, guerra e a paz, relações entre forças armadas e sociedade, ciência e tecnologia no âmbito da defesa e segurança nacionais e internacionais, geopolítica e relações internacionais, planejamento, estratégia, estudos estratégicos e ciências militares em geral.

As publicações do Instituto Vegetius não necessariamente refletem as opiniões de seus clientes e patrocinadores.

www.vegetius.org.br

ISBN: 978-65-997420-2-6

CBL

9 786599 742026