UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

Pedro Henrique Paulette Favero

O amanhecer do poder cibernético brasileiro? Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020

Florianópolis
2022

Pedro Henrique Paulette Favero

O amanhecer do poder cibernético brasileiro? Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020

Trabalho Conclusão do Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais
Orientador: Prof. Danielle Jacon Ayres Pinto, Dra.

Florianópolis
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Favero, Pedro Henrique Paulette
O amanhecer do poder cibernético brasileiro? : Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020 / Pedro Henrique Paulette Favero ; orientadora, Danielle Jacon Ayres Pinto, 2022.
92 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2022.

Inclui referências.

1. Relações Internacionais. 2. Poder Cibernético. 3. Estratégia Cibernética. 4. Defesa Cibernética. 5. Segurança Cibernética. I. Ayres Pinto, Danielle Jacon. II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Pedro Henrique Paulette Favero

O amanhecer do poder cibernético brasileiro? Uma análise documental sobre defesa e segurança cibernética no Brasil de 2018 a 2020

Florianópolis, 21 de julho de 2022

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

Profa. Danielle Jacon Ayres Pinto, Dra.

Universidade Federal de Santa Catarina (UFSC)

Prof. Graciela de Conti Pagliari, Dra.

Universidade Federal de Santa Catarina (UFSC)

Jéssica Maria Grassi, Ma.

Universidade Federal do Rio Grande (FURG)

Certifico que esta é a **versão original e final** do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.

Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 25/07/2022 20:53:49-0300
CPF: 291.367.488-70
Verifique as assinaturas em https://v.ufsc.br

Profa. Danielle Jacon Ayres Pinto, Dra.

Orientadora

Florianópolis, 2022

AGRADECIMENTOS

Em primeiro lugar agradeço aos meus pais, Laís e Emerson pela pelo suporte e amor que deram a mim e aos meus irmãos. Agradeço também aos meus avós, Sueli, Walter e Myrthes por terem participado ativamente de minha vida. Me lembro também dos meus irmãos João Felipe e Eduardo Augusto, meus grandes companheiros desde a infância. Agradeço por fim a Eneida, Guilherme e Eric por me receberem tão bem em Florianópolis. Todas estas pessoas deixaram a difícil tarefa de morar longe de casa mais leve.

Não tenho dúvida que graças as professoras Graciela Pagliari e Danielle Ayres Pinto, minha formação em Relações Internacionais foi completa. Ter sido agraciado com as bolsas de iniciação científicas de vocês mudou para sempre minha experiência na graduação. Hoje percebo a importância e responsabilidade de participar de projetos como estes ainda na graduação.

Estudar na UFSC foi uma experiencia única. Sou grato por ter tido acesso a uma universidade pública e de qualidade. Nesta caminhada, agradeço os bons momentos que vivi com minha companheira Giovanna e com tantos amigos: Diego, Matheus B, Matheus N, Charles, Luis, Fernando e Bruno B. Obrigado!

RESUMO

Após a década de 1990, a sociedade viveu uma revolução tecnológica inédita, com o advento da internet e do espaço cibernético. Logo foi percebido que a internet seria um meio muito eficiente na troca informal, reduzindo drasticamente o tempo necessário para se trocar informações. Porém, com o passar do tempo, percebeu-se que o espaço cibernético não traria apenas benefícios para a sociedade, mas também desafios, como: crimes cibernéticos e ameaças à defesa nacional. Observando que o tal espaço poderia ser uma nova dimensão de defesa nacional, os Estados começaram a utilizá-lo como um possível lócus de poder, se valendo do poder cibernético. Com este contexto e a partir da análise de documentos brasileiros sobre o tema da cibernética, percebeu-se um aumento na sua produção entre 2018 e 2020. Tal trabalho busca entender se este aumento seria uma maneira do Brasil aumentar sua capacidade de influência global. A capacidade de influência ocorreria através da utilização do poder cibernético, calcado em capacidades cibernéticas. A partir do método hipotético-dedutivo, os documentos foram analisados qualitativamente, entendendo que poderiam ser a fonte de uma estratégia de inserção no espaço cibernético. Além disso, foi feita uma revisão bibliográfica sobre as capacidades cibernéticas do país atualmente e os principais conceitos da área. A investigação documental demonstrou que o país não tem uma estratégia cibernética bem definida. A análise das fontes secundárias revelou que o investimento na área; geração de pesquisa e desenvolvimento; recursos humanos e sistemas de defesas também são inadequados. Tudo isso leva a crer que o país não tem boa capacidade cibernética e nem uma estratégia clara. Portanto, não tem condições de exercer capacidade de influência global através do poder cibernético.

Palavras-chave: Poder cibernético. Estratégia cibernética. Defesa Cibernética. Segurança Cibernética. Capacidade Cibernética. Brasil.

ABSTRACT

After the 1990s, society experienced an unprecedented technological revolution: the advent of the internet and cyberspace. It was soon realized that the internet would be a very efficient instrument of informational exchange, drastically reducing the time needed to exchange information. However, over time, it was observed that cyberspace would not only bring benefits to society, but also challenges, such as: cybercrimes and threats to national defense. Noting that this space could be a new dimension of national defense, states began to use it as a possible locus of power, using cyber power. Considering this context and analyzing Brazilian documents about cybernetics, it was realized that there was an increase in its production between 2018 and 2020. This monograph seeks to understand whether this increase would be a way for Brazil to increase its global influence capacity. The influence ability would occur through use of cyber power and cyber capabilities. Based on the hypothetical-deductive method, Brazilian's documents were analyzed qualitatively, considering that they could be a strategic source of insertion in cyberspace. In addition, a literature review was written about Brazilian's cyber capabilities nowadays, and about main concepts of the area. Documentary research has shown that the country does not have a well-defined cyber strategy. The analysis of secondary sources revealed that investment in area; generation of research and development; human resources and defense systems are also inadequate. Then we can believe that Brazil does not have good cyber capability or a clear strategy. Therefore, it is unable to exert global influence through cyber power.

Keywords: Cyber Power. Cyber Strategy. Cyber Defense. Cybersecurity. Cyber Capability. Brazil

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANATEL Agência Nacional de Telecomunicações
ARPANET Advanced Research Projects Agency Net
CDCiber Centro de Defesa Cibernética
ComDCiber Comando de Defesa Cibernética
E-Ciber Estratégia Nacional de segurança cibernética
E-Digital Estratégia Brasileira para a Transformação Digital
ENadCiber escola de defesa cibernética
END Estratégia Nacional de Defesa
ENSI Estratégia Nacional de Segurança da Informação
ENSIC Estratégia Nacional de Segurança de Infraestruturas Críticas
EPEX Escritório de Projetos do Exército
ESG Estratégia Setorial de Defesa
EUA Estados Unidos Da América
EUROPOL European Police Office
GSI Gabinete de Segurança Institucional da Presidência da República
IBGE Instituto Brasileiro de Geografia e Estatística
ICANN Internet Corporation for Assigned Names and Numbers
IMD International Institute for Management Development
IPEA Instituto de Pesquisa Econômica Aplicada
ITU International Telecommunication Union
LGDP Lei Geral de Proteção de Dados
LNCC Laboratório Nacional de Computação Científica
MD Ministério da Defesa
MCTIC Ministério da Ciência, Tecnologia, Inovações e Comunicações
NBSI Norma Brasileira de Gestão de Segurança da Informação
OCDE Organização para Cooperação e Desenvolvimento Econômico
OEA Organização dos Estados Americanos
P&D Pesquisa e desenvolvimento
PCD Política Cibernética de Defesa
PEE Def CIBER Projeto Estratégico do Exército de Defesa Cibernética
PND Política Nacional de Defesa

PNI Política Nacional de Inteligência

PNSI Política Nacional de Segurança da Informação

PNSIC Política Nacional de Segurança de Infraestruturas Críticas

Prg EE Def Ciber Programa Estratégico do Exército Defesa Cibernética

RFID Sistemas de Identificação por Rádio Frequência

SCADA Supervisory Control And Data Acquisition

SGDC Satélite Geoestacionário de Defesa e Comunicações Estratégicas

SIMOC Simulador de Operações de Guerra Cibernética

SISFRON Sistema Integrado de Monitoramento de Fronteira

SMDC Sistema Militar de Defesa Cibernética

TCU Tribunal de Contas da União

TELEBRÁS Telecomunicações Brasileiras S. A.

TIC Tecnologias da Informação e Comunicação

WWW World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A partir de meados da década de 1990, o mundo viveu uma revolução informacional nunca antes vista: o aparecimento da internet. Com ela, as trocas informacionais ficaram muito mais rápidas e eficientes, favorecendo tanto indivíduos quanto Estados Nacionais. Porém, com o passar dos anos, percebeu-se que essa revolução traria não apenas vantagens, mas também desvantagens, como espionagem e sabotagens cibernéticas (RID, 2013). A partir de então, podemos afirmar que se abriu um novo front de defesa nacional, aquele relacionado com o espaço cibernético (AGOSTINI, 2014), que se transformaria no "quinto domínio da guerra".

Sabendo disso, a comunidade científica se preocupou em analisar e investigar as possíveis relações dessas novas tecnologias com a Política Internacional. Com isso, percebe-se que este novo conceito: "o espaço cibernético" é primordial para entender as relações entre os diversos Estados Nacionais. Desta maneira, Gonzales e Portela (2018) concluem que: "o espaço cibernético se apresenta como mais um lócus onde as relações de poder (política) ocorrem" (p.4). Os Estados se valem cada vez mais desse espaço para aumentar seu poder, monitorando e controlando seus pontos de interesse (FERREIRA NETO, 2012).

O conceito de poder cibernético trabalhado será o de Nye Jr (2010), entendendo sua relevância em um Sistema Internacional cada vez mais influenciado pela internet e pelo espaço cibernético. O autor também entende que o poder cibernético, ao contrário de uma vertente realista, não seria apenas ligado à coerção. Seria possível que o poder fosse cooptativo (soft power), utilizando-se de atração e persuasão, por exemplo (NYE JR, 2010). A revolução trazida pela internet gerou também uma transição e difusão de poder (NYE JR, 2010). Como as barreiras para usufruir dessas novas tecnologias são consideravelmente menores que as anteriores, há um incentivo para que novos atores as utilizem, como indivíduos e organizações internacionais (NYE JR, 2010).

Nesta conjuntura do espaço cibernético como novo espaço das Relações Internacionais percebeu-se a seguinte dinâmica: o número de documentos brasileiros publicados sobre cibernética acelerou a partir de 2018. Prontamente, fez-se o seguinte questionamento: o aumento da produção oficial sobre cibernética por parte do governo brasileiro a partir de 2018 gera maior capacidade de influência global em termos de capacidade cibernética? O termo "capacidade de influência global" é necessariamente entendido como resultado do poder cibernético de uma nação (NYE JR, 2010). Ou seja, através de seu poder cibernético os Estados

podem “conseguir resultados preferíveis" (NYE JR, 2010, p.4, *tradução nossa*)[1] de seus contrapartes no Sistema Internacional, influenciado outros estados (NYE JR, 2010). O próprio poder cibernético emanaria de capacidades cibernéticas, seja através de instrumentos físicos quando informacionais (NYE JR, 2010)

Uma provável hipótese que responderia à pergunta supracitada seria que o aumento da produção oficial não seria suficiente para aumentar a capacidade de influência global do Brasil ou suas capacidades cibernéticas. Afinal, não é suficiente apenas criar arcabouço documental sobre o tema. Seria necessário garantir a geração de capacidades cibernéticas necessárias ao poder cibernético. Neste trabalho, entende-se que são os recursos necessários para a formação do poder cibernético e das capacidades cibernéticas: o capital investido, P&D (Pesquisa e Desenvolvimento), recursos humanos e recursos de defesa. Portanto, seria essencial transformar as estratégias documentais em capacidades cibernéticas reais, sendo que tais recursos seriam primordialmente os vetores de influência globais.

Portanto, as variáveis independentes seriam o aumento da produção oficial em matéria de cibernética no país; o capital investido no tema da cibernética; pesquisa e desenvolvimento na área; recursos humanos disponíveis e os sistemas de defesa cibernética. As variáveis dependentes seriam o aumento da capacidade de influência global do Brasil em forma de poder cibernético e a capacidade cibernética brasileira.

Temos como objetivo geral entender se o aumento da produção documental oficial gera maior influência global (em termos de poder cibernético) ao Brasil. Consequentemente, seria possível entender se (ou como) o país trabalha a questão da cibernética como fonte de poder. Os objetivos específicos seriam: (I) esclarecer os principais conceitos da área cibernética; (II) elencar as características do poder cibernético; (III) definir o caráter dos documentos brasileiros; (IV) analisar qualitativamente o conteúdo dos documentos e as capacidades cibernéticas brasileiras já instaladas.

O primeiro capítulo desta monografia tratará sobre a revolução tecnológica criada pela internet e esclarecerá os principais conceitos da área da cibernética. A criação da internet será contada de maneira breve. Em seguida, se fará um esforço para definir os seguintes conceitos: internet; espaço cibernético; defesa e segurança cibernética; infraestruturas críticas; conflitos cibernéticos e poder cibernético.

[1] No original: “to obtain preferred outcomes”.

Com os conceitos introjetados, se passará para a análise documental. Serão apresentados os documentos sobre cibernética criados no Brasil entre 2008 e 2020. Dado que o foco temporal da pesquisa é de 2018 e 2020, todos os documentos deste período serão classificados[2] quanto sua viabilidade para responder à pergunta de pesquisa. Haverá também uma comparação dos conceitos que aparecem nos documentos, na tentativa de notar se há diferenças entre as definições.

Já o capítulo quatro versa sobre as capacidades cibernéticas atuais do Estado Brasileiro. Ou seja, será feita uma análise qualitativa sobre as seguintes variáveis: investimento no setor, P&D, recursos humanos e sistemas de defesa cibernética. Esta análise procura entender se o país detém uma capacidade cibernética satisfatória.

Partindo de uma abordagem hipotético-dedutiva, o trabalho contou tanto com fontes primárias quanto secundárias. As fontes primárias foram os documentos oficiais brasileiros sobre cibernética. As fontes secundárias fazem referência ao trabalho de diversos autores que versam tanto sobre conceitos da área quanto analisam a capacidade cibernética do país. Consequentemente, além de uma pesquisa exploratória (quanto a busca das fontes primárias) este trabalho também desenvolveu uma revisão bibliográfica sobre os conceitos da área cibernética e sobre as capacidades cibernéticas brasileiras, produzindo, de outra parte, também análises qualitativas sobre o tema em tela.

[2] A única exceção é o documento da ANATEL (ANATEL, 2020).

2 A CIBERNÉTICA: SURGIMENTO E CONCEITOS

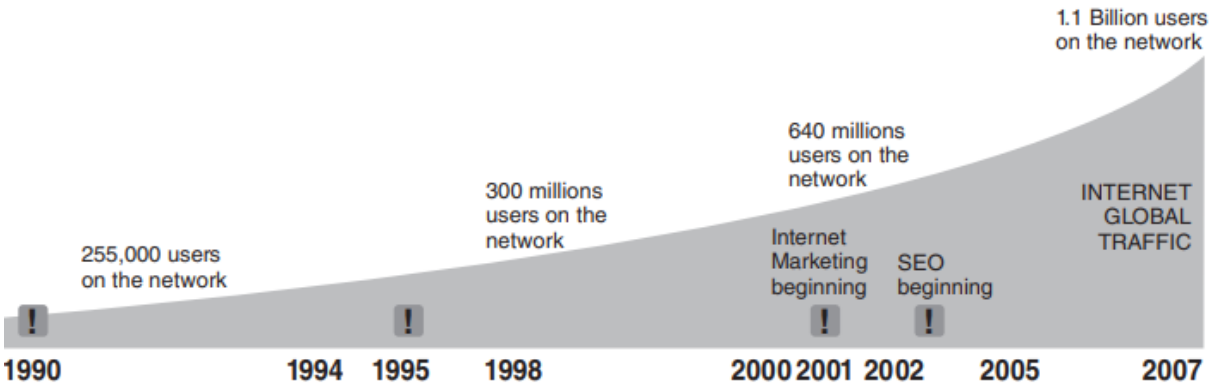
Antes de analisarmos os documentos brasileiros sobre cibernética e as capacidades do país, é necessário contar brevemente sobre o surgimento da internet e explicitar os conceitos específicos da área da cibernética. Só assim será possível se apropriar da discussão específica e tão atual trazida pela cibernética.

2.1 A REVOLUÇÃO TECNOLÓGICA E O SURGIMENTO DA INTERNET

Atualmente, é impossível imaginar a vida no século XXI sem a cibernética e a internet. Embora as revoluções comunicacionais como o telégrafo e o telefone datem ainda do século XIX, a internet revolucionou o mundo com sua instantaneidade. Apenas três mudanças mudaram a vida humana de forma tão intensa quanto a internet: quando os seres humanos deixaram seu nomadismo para serem sedentários e a revolução industrial (TOFFLER 1980 apud MANDARINO JR., 2010). Provavelmente a maior revolução trazida pela internet é sua enorme eficácia e rapidez na troca informacional (SINGER; FRIEDMAN 2014).

O surgimento da internet data da década de 70, com a ARPANET (Advanced Research Projects Agency Net). A ideia era criar uma rede que pudesse interligar os diversos computadores “isolados” nos Estados Unidos, conectando assim diversos pesquisadores em diferentes universidades. A ideia logo acabou sendo do interesse militar do Pentágono (SINGER; FRIEDMAN 2014), que ajudou a desenvolvê-la. A luta pela privatização da internet (SINGER; FRIEDMAN 2014) impulsionou sua utilização por civis ainda na década de 1990, marcada pela ascensão da World Wide Web (“WWW”) e ferramentas como o E-mail. Em pouco tempo, o número de usuários da internet cresceu rapidamente:

Figura 1 - Evolução do número de usuários da internet de 1990 a 2007

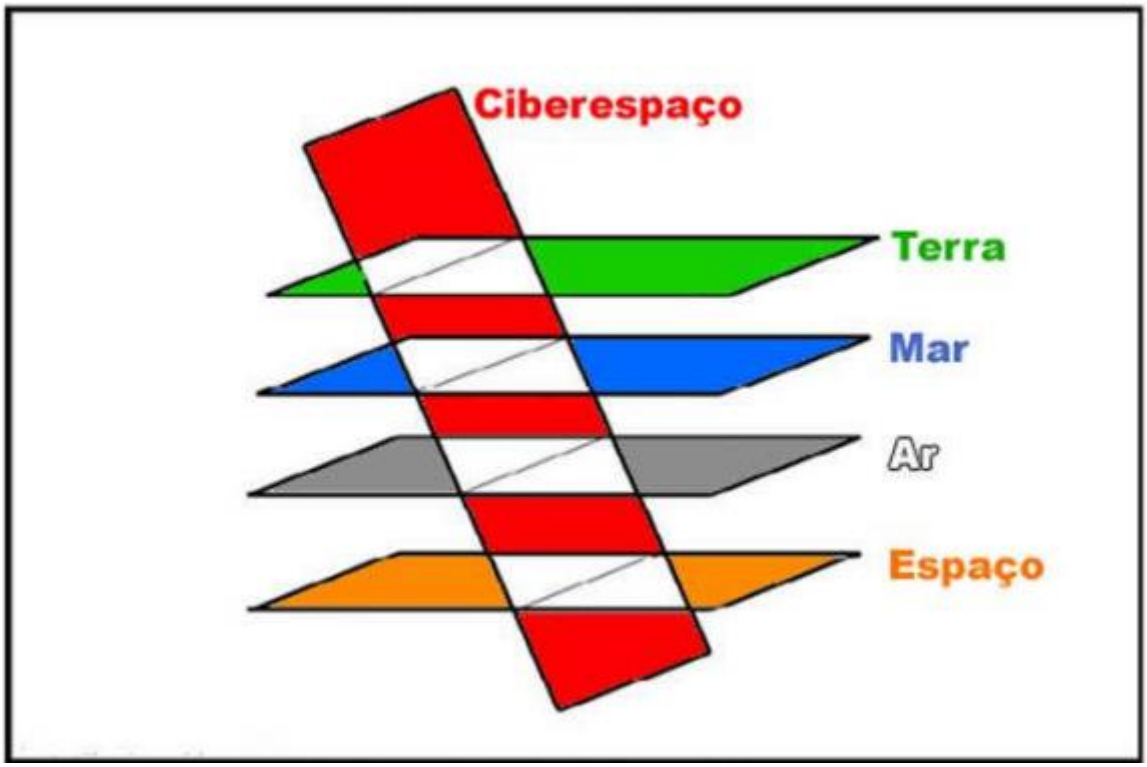


Fonte: adaptado de CHOUCRI, 2012

Mas é claro que não foram apenas os indivíduos que se aproveitaram dessa revolução informacional. Os Estados nacionais logo perceberam as vantagens de utilizarem a internet como meio de alcançarem seus objetivos. Com o passar dos anos, um grande número de Estados buscou modernizar sua estrutura administrativa e burocrática, com processos e armazenamentos digitais.

Ao mesmo tempo, se percebeu que a internet não traria apenas vantagens e benefícios, mas também desafios, como: sabotagem, espionagem e ataques cibernéticos (RID, 2013). Dessa maneira, começou-se a pensar que a internet poderia ser um novo fronte de defesa nacional: o "quinto domínio da defesa" (AGOSTINI, 2014). O domínio cibernético seria transversal aos outros quatro domínios tradicionais (terrestre, naval, aéreo e aeroespacial) (AGOSTINI, 2014). Logo, seria possível utilizá-lo em conjunto com algum outro domínio. Um exemplo seria a conexão de satélites à rede de internet, por exemplo.

Figura 2 - Transversalidade do domínio cibernético



Fonte: AGOSTINI, 2014

2.2 CONCEITOS DA ÁREA CIBERNÉTICA

Sabendo do surgimento da internet e sua possível utilização por Estados, é importante esclarecer conceitos da área cibernética. Em primeiro lugar, devemos esclarecer que, a maioria dos conceitos da área da cibernética padecem de consenso. Dessa forma, é muito comum que os conceitos mudem ligeiramente quando se comparam definições de diferentes atores. Em segundo lugar, a rapidez com que se transforma o espaço cibernético faz com que algumas estruturas e dinâmicas se tornem rapidamente obsoletas (OLIVEIRA; PORTELA, 2017). Além disso, a intangibilidade intrínseca da área cibernética e a abstração necessária para se compreendê-la impossibilita uma análise simplista.

2.2.1 Cibernética e internet

A primeira e mais frequente dúvida seria sobre a diferença entre cibernética e a internet. Ao contrário do que se possa imaginar, os dois conceitos não são sinônimos. A cibernética antecede a internet, e também não há um consenso sobre sua definição. O termo cibernética aparece pela primeira vez em 1961, em um livro de Wiener (1961). Na época, a computação dava ainda seus primeiros passos, e Wiener chamava a atenção para a automação trazida por computadores. De qualquer forma, a definição de cibernética aparece no título do livro: "Controle e Comunicação em humanos e máquinas" (WIENER, 1961, pI, *tradução nossa*)[3]. O termo também aparece na doutrina militar de defesa cibernética do Brasil: "comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação" (BRASIL, 2014a, p. 18).

Já a definição de internet seria: "rede global composta pela interligação de inúmeras redes" (BRASIL, 2019a, não paginado). O próprio nome internet deriva desta análise: "inter" em inglês significa: "entre"; enquanto "net", rede. Choucri (2012), também a define nesse sentido: "Como uma amálgama de redes interoperacionais, sendo que a internet tornou-se parte crítica da infraestrutura global de comunicação" (p.8, *tradução nossa*)[4]. Consequentemente, podemos entender que cibernética e internet não são sinônimos.

2.2.2 Espaço cibernético/ciberespaço

A definição de espaço cibernético também não é consensual entre os autores (OLIVEIRA; PORTELA, 2017). O termo espaço cibernético apareceu pela primeira vez no livro Neuromancer de Gibson (2016) (MANDARINO JR, 2010). Uma definição possível para o termo seria ligada a suas camadas, que converge com a ideias de de Clark (2010) e Nye Jr (2010):

> Nós vemos o espaço cibernético como sistema contingente hierárquico composto de (1) bases físicas e infraestruturas que permitem o campo de atuação cibernético, (2) os blocos de construção lógicos que suportam a plataforma física e permitem serviços, (3) informações armazenadas, transmitidas ou transformadas e (4) os atores, entidades

[3] No original: "the control and communication in the animal and the machine".
[4] No original: "As an amalgam of interoperable networks, the Internet has become a critical part of the emerging global communication infrastructure".

> e usuários com diversos interesses que participam desta arena com vários papéis (CHOUCRI, 2012, p.8, tradução nossa)[5].

Essa ideia de camadas converge com as definições de software, hardware e peopleware (LIBICKI, 2009; VENTRE, 2012). O hardware faria menção a parte física dos sistemas como: computadores, cabos submarinos de internet e celulares. O software está ligado ao sistema (não físico) como códigos fontes e algoritmos. Já a peopleware seria a camada humana do sistema: os atores que o utilizam (MANDARINO JR, 2010; OLIVEIRA; PORTELA, 2017; VENTRE, 2012). De qualquer forma, chama-se atenção que os usuários desse espaço (nós, os internautas) somos parte fundamental do sistema.

Enquanto isso, a doutrina militar de defesa cibernética (2014) define espaço cibernético como: "o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas" (BRASIL, 2014a, p. 18). Nota-se a passagem de Guedes e Portela (2017), que comentam a ideia de Clarke Knake (2012):

> Para esses autores, a internet está dentro do espaço cibernético, mas esse não pode ser resumido somente a ela. O espaço cibernético é mais abrangente, pois também se refere às estruturas que não estão conectadas à internet e todos os aparelhos submetidos a ela (OLIVEIRA; PORTELA, 2017, p. 80).

Logo percebe-se que a internet é uma seção do espaço cibernético. Mesmo assim, podemos dizer que a internet é a seção mais relevante do espaço cibernético (informação verbal)[6], e não seu sinônimo perfeito (CLARKE; KNAKE, 2012; OLIVEIRA; PORTELA, 2017). Ventre (2012) dá um exemplo do espaço cibernético sem a internet: "Mas o espaço cibernético é muito maior: os satélites, os drones, os sistemas de identificação por rádio frequência, os computadores (conectados ou não), e os sistemas industriais informatizados, todos são componentes do ciberespaço" (p. 34)[7].

---

[5] No original: "we view cyberspace as a hierarchical contingent system composed of (1) the physical foundations and infrastructures that enable the cyber playing field, (2) the logical building blocks that support the physical platform and enable services, (3) the information content stored, transmitted, or transformed, and (4) the actors, entities and users with various interest who participate in this arena in various roles".

[6] Falas da profª Danielle Jacon Ayres Pinto no webinário: "Encontro Preparatórios ABRI: Perigos e desafios do mundo cibernético Frente à COVID-19", da Associação Brasileira De Relações Internacionais em 20 de junho de 2020 por meios virtuais: https://www.youtube.com/watch?v=j3sz9eC3_hw&ab_channel=ABRIOficial e na mesa redonda 6: "Novas tecnologias e vulnerabilidades: pensando segurança e defesa no século XXI", do XI Encontro Nacional da Associação Brasileira de Estudos de Defesa no dia 7 de novembro de 2021, em meios virtuais: https://www.youtube.com/watch?v=fJ8SsJV95Zk&ab_channel=ABEDAssocia%C3%A7%C3%A3oBrasileiradeEstudosdeDefesa

[7] No original: "Pero el ciberespacio es mucho más: los satélites, los drones, el RFID, los ordenadores conectados o no, los sistemas industriales informatizados, todos son componentes del ciberespacio".

Outra consideração importante sobre o espaço cibernético é feita por Ferreira Neto (2014). Para o autor, o espaço cibernético é um lócus onde há disputa de poder:

> As possibilidades advindas do uso do recurso cibernético transformam-no em uma fonte de poder, ligado ao controle e ao armazenamento da informação. No nível político e no estratégico, a capacidade cibernética permite ao Estado, por exemplo, o monitoramento e o controle de seu território e de "pontos" de seu interesse. (p. 158-9)

Mesmo que o espaço cibernético não seja físico, mas artificial, pode-se entender que os estados o territorializam:

> No ambiente cibernético do globo, os Estados delimitam seus territórios "nitidamente", isto é, apropriam-se de espaço por meio do poder. Como exemplos imediatos, mas não únicos, basta-nos ver os domínios dos sítios ".br; .us; .uk; .it; (FERREIRA NETO, 2014, P. 157).

Portanto, embora uma discussão de fronteira geográfica tradicional, como nos moldes de Ratzel (1987) não se encaixe, afirma Ferreira Neto (2014):

> A fronteira cibernética, por conseguinte, obedece à forma de "pontos" ("nós") ou "pacotes" de informações eleitos pelos Estados devido ao seu grau de interesse – sistemas de Defesa, infraestruturas críticas/estruturas estratégicas são exemplos. Com isso, defendemos que a fronteira nesse ambiente apresenta-se na forma de "fronteira-ponto (p. 158)

Outra característica do espaço cibernético é a questão do anonimato, tão cara nos dias atuais. Rid (2013) o denomina-o de "problema da atribuição". O autor chama a atenção para a enorme dificuldade de descobrir os autores dos ataques. Isso se dá principalmente por três camadas de dificuldade: a técnica, a social e a política (RID, 2013). Sobre a camada técnica, elenca-se a dificuldade de se rastrear a máquina utilizada para perpetrar o ataque. A camada social diz respeito a saber quem de fato usou tal máquina para fazer o ataque. Caso essas duas camadas sejam superadas, há ainda a camada política: necessidade de que os países nos quais foram praticados os delitos possam cooperar na investigação (RID, 2013).

Mas é claro que essas três camadas não necessariamente inviabilizam a possibilidade de se descobrir o autor dos delitos ou ataques cibernéticos. Existem também facilitadores, como: erros cometidos, motivações particulares suspeitas, evidências testemunhais e a gravidade do ataque (RID, 2013).

2.2.3 Defesa cibernética e segurança cibernética

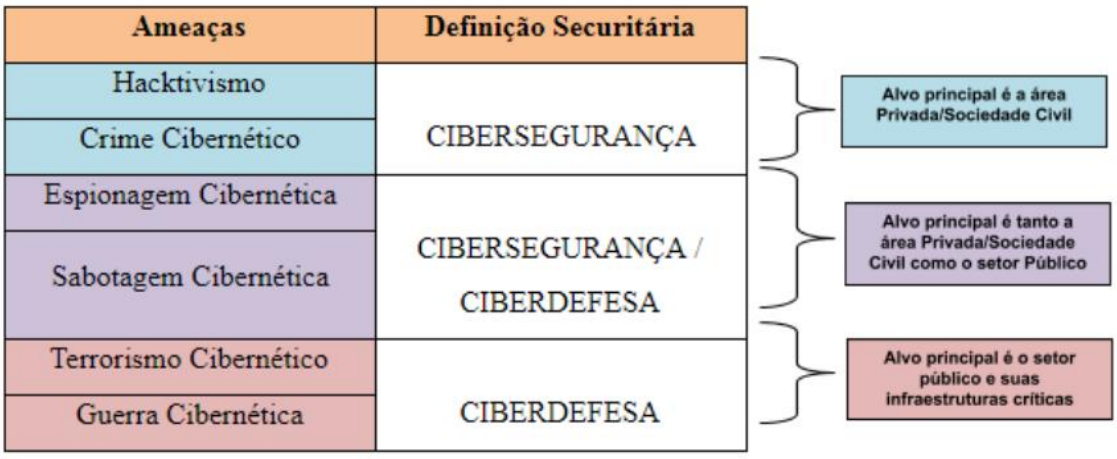
Os próximos dois conceitos a serem tratados são a segurança cibernética e a defesa cibernética. Quanto a eles, não há também consenso, e não são necessariamente sinônimos

(PAGLIARI; AYRES PINTO; VIGGIANO, 2020). A diferenciação entre segurança e defesa começou a se esboçar de maneira mais clara no *Human Development Report* (UNITED NATIONS, 1994). A partir de então, uma visão de segurança internacional meramente ligada aos estados começou a ser questionada (DE RÊ, 2021).

Com o passar dos anos, a ideia de segurança cibernética passou a se relacionar com a sociedade civil, setor privado, segurança pública e ilícitos (MEDEIROS FILHO, 2014; NAIM, 2006). Enquanto isso, a defesa cibernética estaria vinculada a defesa do estado nação, na tentativa e proteger seus interesses e soberania (PAGLIARI; AYRES PINTO; VIGGIANO, 2020), Autores como Naim (2006) e Medeiros Filho (2014) acreditam a defesa cibernética estaria também relacionada a guerra.

Muitas vezes, porém, essa diferenciação se torna mais complexa. A sabotagem e a espionagem cibernéticas, por exemplo, podem afetar tanto o domínio privado quanto o público (PAGLIARI; AYRES PINTO; VIGGIANO, 2020; RID, 2013). Essa dificuldade está bem expressa na seguinte imagem:

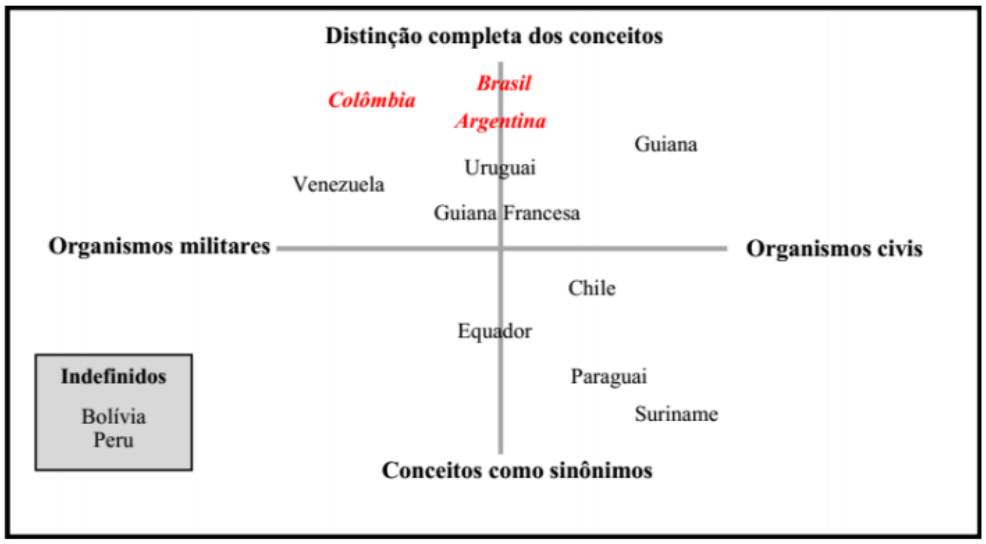
Figura 3 - Classificação de ameaças cibernéticas



Fonte: PAGLIARI; AYRES PINTO; VIGGIANO, 2020

Além disso, vale destacar que a diferenciação dos conceitos de segurança e defesa cibernética não são utilizados uniformemente em todos os países (GONZALES; PORTELA, 2018). Uma análise da utilização de tais conceitos indica que alguns países sul-americanos os tratam como sinônimos, enquanto outros não:

Figura 4 - Distinção de segurança e defesa cibernética nos países da América do Sul



Fonte: GONZALES; PORTELA, 2018

2.2.4 Infraestruturas críticas e conflitos cibernéticos

Outro conceito muito discutido nos dias atuais faz menção às infraestruturas críticas:

> As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente. (BRASIL, 2020a, não paginado)

Possíveis exemplos destas infraestruturas seriam sistemas de distribuição de água e energia elétrica, sistemas de telecomunicações e de internet. Sem tais sistemas, o funcionamento de serviços essenciais para a sociedade estaria ameaçada (BRASIL, 2020a).

Há também a discussão de que a democracia pode ser entendida como infraestrutura crítica. Ou seja, o sistema democrático seria basilar para uma sociedade mais justa (AYRES PINTO, 2021). Na virada do século, acreditava-se que: “o surgimento das redes sociais no início dos anos 2000 era de que essa nova forma de comunicação aumentaria a participação popular e daria voz aos oprimidos” (AYRES PINTO; MORAES, 2020, p 72-3).

Porém, ao longo do tempo percebeu-se que a internet poderia ser fonte de populismo, dada a comunicação não mediada entre eleitores e políticos (BIMBER, 1998). Principalmente a partir de 2016, o fenômeno das fake news na internet começou a ganhar força (AYRES

PINTO; MORAES, 2020). As fakes news atacam um pilar fundamental da democracia descrito por Dahl (1989): “fontes alternativas de informação que sejam protegidas por lei” (p. 120). O uso mal intencionado de algoritmos pode suprimir fontes alternativas de informação e estimular uma visão parcial dos eleitores.

Junto com a discussão sobre as infraestruturas críticas, devemos passar também pelos conceitos de conflitos cibernéticos. Os conflitos cibernéticos mais notórios são: hacktivismo, crime cibernético, sabotagem cibernética, espionagem cibernética, terror cibernético e guerra cibernética (CAVELTY, 2012). Uma síntese de tais conceitos podem ser vista abaixo:

Quadro 1 - Tipos de conflitos cibernéticos segundo Cavelty (2012)

Tipos de conflitos cibernéticos	**Descrição**
Hacktivismo	“A combinação de hacking e ativismo, incluindo operações que usam técnicas de hacking contra um site de internet, que é alvo, com a intenção de interromper operações normais.” (p. 116)
Crime cibernético	“Uma atividade criminal realizada com a utilização de computadores e da internet.” (p. 116)
Espionagem cibernética	“A sondagem não autorizada para testar uma configuração de um computador de destino ou avaliar seus sistemas de defesa, ou a visualização e cópia não autorizadas de arquivos de dados.” (p. 116)
Sabotagem cibernética	“A perturbação deliberada de um processo econômico ou militar para alcançar um objetivo específico (geralmente político) com meios cibernéticos.” (p. 116)
Terror cibernético	“Ataques ilegais contra computadores, redes, e as informações nele armazenados, para intimidar ou coagir um governo ou seu povo em prol de objetivos políticos ou sociais. Este tipo de ataque deve resultar em violência contra pessoas ou propriedade, ou, pelo menos, causar danos suficientes para gerar o nível de medo necessário para ser considerado "ciberterrorismo". O termo também é usado livremente para caracterizar incidentes cibernéticos de natureza política.” (p. 116)
Guerra cibernética	“O uso de computadores para interromper as atividades de um país inimigo, especialmente ataques deliberados aos sistemas de comunicação. O termo também é usado livremente para caracterizar incidentes cibernéticos de natureza política.” (p. 116)

Fonte: CASTRO, 2020

Dentre os conflitos cibernéticos, Rid (2013) chama a atenção para a sabotagem e a espionagem. É comum, segundo o autor, que a sabotagem cibernética tenha como alvo infraestruturas críticas A sabotagem tem natureza técnica, e tem como alvo maquinário (RID, 2013). Nem sempre a sabotagem consegue a completa destruição dos sistemas atacados, podendo incapacitá-los parcialmente (RID, 2013). Um exemplo seria o caso Shamoon, caso de sabotagem contra a empresa petrolífera Saudi Aramco (RID, 2013). O caso em questão afetou somente o software da empresa, o que permitiu que fosse possível a continuidade dos trabalhos logísticos (RID, 2013).

A espionagem cibernética, por sua vez, não seria ato de guerra ou ataque cibernético, e nem diretamente instrumental. Ou seja, a espionagem é um instrumento para se conseguir algum objetivo intermediário, como documentos sigilosos (RID, 2013). Para além disso, grifa-se a importância da inteligência humana na espionagem cibernética, que serve para complementar a qualidade da espionagem (RID, 2013). Afinal, embora a quantidade de dados que podem ser roubados seja maior com a espionagem cibernética, é cada vez mais difícil organizá-los de forma favorável (RID, 2013). Podemos elencar também algumas dificuldades da área de espionagem como: dificuldade de encontrar dados relevantes, necessário fazer uma boa análise de dados e dificuldade de descobrir se a ameaça é doméstica ou internacional (RID, 2013).

2.2.5 O poder cibernético

Muito provavelmente, o conceito mais relevante a ser analisado neste estudo seja o poder cibernético. Antes de analisá-lo propriamente, é interessante discorrer sobre um fenômeno central nas Relações Internacionais do século XXI - a difusão de poder.

A difusão de poder começou ainda na década de 70 (NYE JR, 1990), e vem se intensificando ao longo do tempo. São os fatores primordiais para a difusão de poder: interdependência econômica, nacionalismo em estados fracos, atores transnacionais (como empresas e organizações não-governamentais) e o avanço tecnológico (NYE JR, 1990).

Além disso, pode-se afirmar que uma sociedade internacional cada vez mais interdependente e balizada pelos direitos humanos resulte no alto custo do poder militar (NYE JR, 1990). Assim, aspectos econômicos como o comércio bilateral e interdependência econômica têm importância real para impedirem os conflitos (RUSSETT, 2021).

Essa visão que compartilhamos com Nye Jr (1990) de alguma maneira foge dos cânones realistas das Relações Internacionais. Isso porque acreditamos que uma sociedade mais complexa e interdependente, diminui a fungibilidade do poder. Ou seja, é cada vez mais difícil fazer com o poder seja em transferível para outras esferas (NYE JR, 1990). Um exemplo seria a transformação do poder econômico em militar:

> Hoje, porém, o uso direto da força para gerar ganhos econômicos é geralmente muito custoso e perigoso para as grandes potências modernas. Até mesmo em pequenas agressões, a transposição de poderio econômico em militar pode ser muito alta. (NYE JR, 1990, p. 159, *tradução nossa*)[8]

Dada a menor fungibilidade do poder atualmente, é necessário que uma visão menos estatocêntrica das Relações Internacionais seja levada em conta. Isso não quer dizer que os Estados Nacionais deixem de ser os atores por excelência das Relações Internacionais. Porém, é necessário assumir que outros atores têm relevância na esfera internacional.

Outra consequência ligada a difusão de poder e alto custo do poder militar é a generalização do uso do poder cooptativo, ou soft power (NYE JR, 1990). O soft power ("poder macio") seria justamente uma forma cooptativa e não coercitiva de poder (NYE JR, 1990). Assim, o soft power ocorreria quando um Estado A faz com que o Estado B queira o mesmo que ele (NYE JR, 1990). Outra definição possível seria: "o poder cooptativo é habilidade de um país de estruturar uma situação para que outros países desenvolvam preferências ou definam interesses de maneira consistentes com o seu próprio" (NYE JR, 2010, p. 168, *tradução nossa*)[9]. Logo, o soft power estaria relacionado com a persuasão.

Tal processo difere do chamado "hard power". O "poder duro" seria aquele coercitivo, ligado à ideia de que um Estado A force um Estado B a fazer algo que normalmente ele não faria (NYE JR, 2010). Enquanto esse poder estaria relacionado a recursos tradicionais (força militar, território, capacidade de produção) o soft power está ligado a recursos não tradicionais, como por exemplo: ideologias, valores e políticas públicas internacionais (NYE, 1990).

Nye Jr (1990) também pontua que tanto o hard como o soft power são igualmente importantes, não havendo qualquer hierarquia de importância dentre eles. Eles seriam duas facetas do termo "poder". Os Estados Unidos, por exemplo, além de terem grande poderio bélico são também muito eficientes em soft power. A cultura americana, e o modo de viver

[8] No original: "Today, however, the direct use of force for economic gain is generally too costly and dangerous for modern great powers. Even short of aggression, the translation of economic into military power resources may be very costly".

[9] No original: "Co-optive power is the ability of a country to structure a situation so that other countries develop preferences or define their interests in ways consistent with its own".

americano (“american way of life”) são tidos como ideais em boa parte do mundo ocidental. Além disso, muitas regras básicas de instituições internacionais (como livre comércio e democracia) são valores notadamente da sociedade estadunidense (NYE JR, 1990).

Falando propriamente sobre o poder cibernético, poderíamos defini-lo como “a habilidade de conseguir resultados preferíveis pelo uso de recursos de informação através do domínio cibernético” (NYE JR, 2010, p. 3-4, *tradução nossa*)[10]. Exemplos destes recursos de informação seriam: capital investido, P&D, recursos humanos e sistemas de defesa, que serão analisados no capítulo quatro. Uma definição mais abrangente seria: “a habilidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder” (NYE JR, 2010, p. 4, *tradução nossa*)[11]. Ou seja, o espaço cibernético seria um espaço onde o poder cibernético é exercido por excelência (FERREIRA NETO, 2014) e: “a cibernética é tratada como um meio, que inclusive auxilia no exercício de poder” (FERREIRA NETO, 2014, p.170).

Um fator de grande importância do poder cibernético é que ele pode gerar consequências dentro e fora do espaço cibernético (NYE JR, 2010). Além da variável interna ou externa ao espaço cibernético, devemos considerar a possibilidade do poder cibernético ser utilizado na forma hard ou soft, através de instrumento da informação ou físicos (NYE JR, 2010). Os quadros 1 e 2 ilustram bem essas características:

Quadro 2 - Implicações do poder cibernético (na forma Hard Power) dentro e fora do ciberespaço

	Dentro do Espaço Cibernético	**Para além do espaço cibernético**
Instrumentos de informação	Ataques de negação de serviço (a)	Ataques de sistema SCADA (b)
Instrumentos Físicos	Controle governamental sobre empresas (c)	Ataques a infraestruturas físicas (ex: corte de cabos submarinos) (d)

Fonte: adaptado de NYE JR, 2010

[10] No original: “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain”.

[11] No original: “is “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.”

Quadro 3 - Implicações do poder cibernético (na forma Soft Power) dentro e fora do ciberespaço

	Dentro do Espaço Cibernético	**Para além do espaço cibernético**
Instrumentos de informação	Estabelecimento de normas e padrões (e)	Campanhas de diplomacia pública para influenciar opiniões (f)
Instrumentos Físicos	Infraestruturas para ativistas de direitos humanos (g)	Protestos para identificar e difamar provedores cibernéticos (h)

Fonte: adaptado de NYE JR, 2010

As colunas dos quadros acima indicam se o poder cibernético gera consequência dentro ou fora do espaço cibernético. Já as linhas dizem respeito ao tipo de instrumento utilizado: informacional ou físico. O quadro 1 faz jus as consequências do poder cibernético em sua forma “Hard”, enquanto o segundo na sua forma “Soft”.

Cruzando-se a coluna “dentro do espaço cibernético” com a linha “instrumento informacional” na forma “hard” do poder cibernético, temos como resultado os ataques de negação de serviço (a). Estes seriam ataques que que coordenam o acesso simultâneo de milhares (ou milhões) de computadores em um mesmo site, o que congestiona o servidor e o tira do ar (NYE JR, 2010). O próximo resultado obtido seria o ataque a sistemas SCADA (Supervisory Control And Data Acquisition) (b). Sistemas SCADA são sistemas que coordenam processos industriais ou de distribuição de serviços como água e eletricidade (NYE JR, 2010) que podem ser alvos de sabotagem (RID, 2013).

Já o controle governamental sobre empresas (c) diz respeito a coerção que governos podem perpetrar contra empresas. Um exemplo seria quando o governo alemão processou o Google para que fossem tirados discursos de ódio do resultado de pesquisa da empresa (NYE JR, 2010). Por fim, o ataque a infraestruturas físicas (d) está relacionado com os danos físicos causados a infraestruturas determinantes para a existência do espaço cibernético, como cabos submarinos ou servidores.

Analisando o quadro 2, referente às implicações do poder cibernético na forma "soft", temos como primeiro resultado o estabelecimento de normas e padrões (e). Nye JR utiliza o exemplo de que é possível “atrair [...] programadores de software a aderir a um novo padrão”

determinado (NYE JR, 2010, p 5, *tradução nossa*) [12]. O resultado (f) diz respeito às campanhas de diplomacia pública na internet para influenciar cidadãos em outros países (NYE JR, 2010).

Outro resultado possível é a infraestrutura para ativistas dos direitos humanos (g): "governos podem configurar servidores especiais e softwares que ajudem ativistas de direitos humanos a propagarem suas mensagens" (NYE JR, 2010 p.6, *tradução nossa*) [13]. Por fim, temos o processo de identificação e difamação de certos provedores cibernéticos (h). Assim, atores não estatais poderiam desincentivar atores que abusam da internet (NYE JR, 2010).

Logo em seguida, Nye JR (2010) traz outro quadro, que relaciona as três faces do poder no domínio cibernético com as formas "soft" e "hard" do poder cibernético. Nye Jr (2010) também mostra a definição de três aspectos do poder, visíveis no quadro 3. A primeira está relacionada com a visão de Dahl (1961), que se daria quando um ator obriga o outro a fazer o que ele normalmente não faria. O segundo aspecto de poder está ligado a definição de agenda: "enquadrar questões de tal forma que a questão da coerção nunca apareça" (NYE JR, 2010, p2, *tradução nossa*) [14]. Por fim, o terceiro e último aspecto estaria relacionado às ideias: "ideias e crenças também ajudam a moldar preferências alheias, e é possível exercer poder determinando os desejos dos outros." (NYE JR, 2010, p.2, *tradução nossa*) [15].

[12] No original: "attracting [...] software community of programmers to adhere to a new standard".
[13] No original: "governments can set up special servers and software designed to help human rights activists propagate their messages".
[14] No original: "framing issues in such a way that the issue of coercion never arose".
[15] No original: "pointed out that ideas and beliefs also help shape others' preferences, and one can also exercise power by determining others' wants.

Quadro 4 - As três faces do poder no domínio cibernético

	Face 1	**Face 2**	**Face 3**
	A induz B a fazer algo que B normalmente não faria	A impede escolhas de B excluindo estratégias de B	A molda preferências de B fazendo com que algumas estratégias nem sejam consideradas
Hard Power (coerção)	Ataques de negação de serviço, ataques SCADA, prisão de "bloggers" (i)	Firewalls, filtros de conteúdo (k)	Ameaças de punição de "bloggers" que espalham material censurado (m)
Soft Power (cooptação)	Campanha de informação para mudar preferências iniciais de hackers, recrutamento de organizações terroristas (j)	Provedores de serviço de internet, normas da ICANN de domínios (l)	Informações para criar preferências (estímulo de nacionalismo, hackers patrióticos) (n)

Fonte: adaptado de NYE JR, 2010

Cruzando-se a coluna da face um do poder com a linha de hard power, obtemos prisão de “bloggers", ataques de negação de serviço ou ataques SCADA (i), já explicitados no quadro um. O resultado (j) seria quando existe uma campanha de desinformação (NYE JR, 2010), como por exemplo os vídeos da organização terrorista Al-Qaeda, disseminados para recrutar novos integrantes (NYE JR, 2010).

A próxima coluna, referente a segunda face do poder, gera os resultados (k) com hard power e (l) com soft power. O primeiro resultado (k) é amplamente utilizado em países que buscam censurar conteúdos, como por exemplo a China, que se vale de firewalls na tentativa de bloquear acessos a determinados sites (NYE JR, 2010). O resultado (l) faz referência às normas de domínios da ICANN (Internet Corporation for Assigned Names and Numbers). Essa instituição dá a palavra final na atribuição de domínios. Assim, uma estratégia de um ator pode acabar sendo excluída pelos padrões mais rígidos da ICANN.

A última face do poder gera os resultados (m) e (n), seguindo a ideia que o ator A quer que B deixe de considerar suas próprias estratégias. O primeiro (m) faz referência a ameaças de punição de “bloggers” que espalhem material censurado, ou campanhas governamentais de deslegitimação de pautas específicas, consideradas nocivas (NYE JR, 2010).

Já o resultado ligado ao soft power, (n), ocorre quando há divulgação de informações para criar preferências como: fortalecer o nacionalismo ou estimular o aparecimento de hackers patrióticos. Hackers patrióticos seriam indivíduos que, em nome do nacionalismo, visam atacar outros países, em nome do interesse nacional. Esse tipo de conduta é comum na Rússia, o que permite que o governo russo seja possa se eximir da acusação de ataques cibernéticos (SOLDATOV; BOROGAN, 2018).

Logo em seguida, Nye Jr (2010) traz um último quadro. Tal quadro traz uma análise dos recursos relativos de poder de três classes de atores: (I) governos, (II) organizações e redes bem estruturados e (III) indivíduos e redes pouco estruturadas. Cada classe é analisada individualmente e são citadas suas vantagens e vulnerabilidades no espaço cibernético:

Quadro 5 - Recursos relativos de poder de diferentes atores no domínio cibernético

	Governos	**Organizações e redes bem estruturadas**	**Indivíduos e redes pouco estruturadas**
Vantagens	1- Desenvolvimento e suporte de infraestrutura, educação e propriedade intelectual 2- Coerção Legal e física de indivíduos dentro das fronteiras 3- Tamanho do mercado e controle de acesso (ex. China, Estados Unidos) 4- Recursos de ataques e defesas cibernéticos 5- Geração de bens públicos 6- Reputação e legitimidade, competências que produz soft power	1- Grandes orçamentos e recursos humanos, economias de escala 2- Flexibilidade transnacional 3- Controle de código e desenvolvimento de produtos 4- Marcas e reputação	1- Baixo custo de entrada 2- Anonimato virtual e facilidade de saída 3- Menos vulnerabilidades se comparado com governos e grandes organizações
Vulnerabilidades	1- Grande dependência de sistemas complexos facilmente disruptivos 2- Estabilidade política 3- Perda de reputação	1- Roubo de propriedade intelectual 2- Disrupção de sistemas 3- Perda de reputação	1- Coerção legal e ilegal de governos e organizações

Fonte: adaptado de NYE JR, 2010

Em primeiro lugar, os governos (Estados), atores por excelência das Relações Internacionais, têm papel fundamental nesta análise. A infraestrutura e orçamento disponíveis pelos Estado são uma vantagem se comparado às outras duas classes de atores. Capacidade de investimento é fundamental para que se possa resultar em poder cibernético (FARIAS; FERRAZ, 2018). Essa capacidade gera também a possibilidade de atacar outros atores ou defender seu próprio espaço cibernético.

Os governos também detêm o monopólio legal do uso da força dentro de suas fronteiras, o que permite liberdade de ação para punir transgressores e criar mecanismos legais de punição. É interessante destacar que Nye Jr (2010) afirma também que Estados com grande tamanho podem ter alguma influência "extraterritorial". Isso é visto quando as normas adotadas pela União Europeia acabam servindo de modelo para outros países (NYE JR 2010).

Os Estados Nacionais também são geradores de bens públicos, o que pode gerar regulamentações necessárias, como por exemplo a do comércio (NYE JR, 2010). Essas regulamentações poderiam trazer vantagens, uma vez que poderiam determinar as regras e normas de processos. Por fim, governos têm a possibilidade de usar sua reputação positiva para gerar soft power e gerar persuasão (NYE JR, 2010).

Porém, como qualquer ator, os governos têm também vulnerabilidades. Um exemplo seria a sua dependência de sistemas informacionais. Nye Jr (2010) afirma que tais sistemas podem ser facilmente suspensos. Um exemplo seria o ataque a sistemas SCADA, já citados anteriormente. A estabilidade política também seria um problema, já que a alternância política pode gerar constantes mudanças em estratégias, comprometendo a geração de uma estratégia sólida no longo prazo (NYE JR, 2010).

Devemos então partir para a análise de redes estruturadas. Um exemplo destas redes seriam grandes organizações internacionais ou grandes empresas. Suas principais vantagens são seus grandes orçamentos e disponibilidade de pessoal. Nye Jr (2010) ressalta que existem empresas que têm orçamentos maiores que de Estados pequenos, por exemplo. Outra vantagem seria seu desenvolvimento de produtos e tecnologias. O autor utiliza o exemplo de empresas de tecnologia como Amazon e Google, que desenvolveram suas próprias tecnologias de computação em nuvem (NYE JR, 2010).

A possibilidade de serem transnacionais também é vantajosa. Neste caso, tais organizações (ao contrário de governos) não estariam presos a jurisdições específicas. Mas isso não quer dizer as organizações desprezem as leis locais: "ao mesmo tempo, para preservar seu status legal e sua marca, corporações transnacionais têm fortes incentivos para se manter em conformidade com estruturas legais locais (NYE JR, 2010, p. 12, *tradução nossa*)"[16].

Redes estruturadas também têm vulnerabilidades como: roubo de propriedade intelectual, disrupção de sistemas e perda de reputação. Uma das questões centrais é justamente o roubo de propriedade intelectual, tão comuns em casos de espionagem cibernética. Estas

[16] No original: "At the same time, to preserve their legal status as well as their brand equity, transnational corporations have strong incentives to stay compliant with local legal structures".

redes, assim como os governos, dependem de sistemas informacionais que podem ser atacados. Além disso, a perda de reputação pode ser considerada uma vulnerabilidade. A partir do momento que uma organização ou empresa se envolve em algum caso polêmico, sua reputação pode ser questionada, o que pode ser difícil de reverter no curto prazo.

Por fim, temos a análise de redes pouco estruturadas e individuais. Suas maiores vantagens são justamente o baixo custo de entrada e a possibilidade de anonimato (NYE JR, 2010). Nos domínios tradicionais de defesa como o terrestre e o naval, o custo de entrada é alto. É possível perceber este custo com a necessidade de grandes gastos de capital por Estados para a compra ou modernização de armamentos e treinamento de tropas. Nesse sentido, o Estado Nação centraliza a tomada de decisão e costuma despender quantias consideráveis. Já no domínio cibernético, é possível que cidadãos, se valendo do anonimato e explorando vulnerabilidades, possam cometer ataques ou crimes cibernéticos, sem ter que necessariamente investir qualquer orçamento. Outra vantagem está relacionada a:

> atores individuais no domínio cibernético se beneficiam de vulnerabilidades assimétricas se comparada com governos e grandes organizações. Eles necessitam de investimentos muito baixo e tem muito pouco (ou nada) a perder com sua saída ou reentrada. (NYE JR, 2010, p.13, *tradução nossa*)[17]

Embora o espaço cibernético permita que atores menos capacitados inflijam danos a atores maiores, não se deve pensar que os atores fracos não têm vulnerabilidades. A grande desvantagem desses autores é a coerção que podem sofrem de governos. Essa coerção pode ser tanto legal quanto ilegal, considerando casos de governos autoritários, por exemplo.

Como conclusão, podemos entender que embora atores menores sejam favorecidos pela difusão de poder e pelo advento do espaço cibernético, os atores estatais ainda são os atores mais relevantes: “Governos ainda são os atores dominantes da internet, mas os atores menores ainda podem fazer estragos” (NYE JR, 2010, p.13, *tradução nossa*)[18].

[17] No original: “individual actors in the cyber domain benefit from asymmetrical vulnerability compared to governments and large organizations. They have very low investment and little to lose from exit and re-entry”.
[18] No original: “Governments are top dogs on the internet, but smaller dogs still bite, and dealing with those bites can lead to a complex politics”.

3 OS DOCUMENTOS BRASILEIROS

Neste capítulo, buscaremos analisar os documentos brasileiros oficiais sobre cibernética. A produção documental seria a primeira variável relevante para mensurar o poder cibernético do país. Seriam tais documentos que guiaram o país, através de estratégias claras e pragmáticas, a se colocar como player global em termos de poder cibernético. Os documentos não apenas devem citar as estratégias de forma clara, mas também mapear vulnerabilidades e explorar de maneira precisa como superá-las.

Em um primeiro momento, os documentos serão apresentados. Logo em seguida os documentos serão analisados e então separados em dois grupos, seguindo sua utilidade explicativa para comprovar se são úteis como instrumento de poder cibernético do país.

3.1 MAPEAMENTO DOS DOCUMENTOS

Com os principais conceitos da área cibernética mapeados, podemos passar para a análise documental. A procura de documentos oficiais brasileiros sobre cibernética se baseou no site do instituto Igarapé (2022). Grifa-se a importância do Instituto Igarapé (2022) como fonte de pesquisa, uma vez que organiza de maneira sistemática e em formato de linha do tempo os diversos documentos brasileiros sobre cibernética.

O quadro abaixo compila todos os documentos encontrados. Os documentos foram categorizados pelo seu ano de expedição, autor/órgão responsável, caráter do órgão responsável–l e se são legislativos ou estratégicos.

Quadro 6 - Documentos Brasileiros Sobre cibernética 2008 – 2020

Título	Ano	Autor/Órgão responsável	Caráter do órgão responsável	Legislativo ou estratégico?
Estratégia Nacional de Defesa (END)	2008	MD	Público	Político Estratégico
Livro Verde de segurança cibernética	2010	GSI	Público	Político Estratégico
Política Cibernética de Defesa (PCD)	2012	MD	Público	Político Estratégico
Livro Branco	2012	MD	Público	Político Estratégico
Estratégia Nacional de Defesa e Política Nacional de Defesa	2012	MD	Público	Político Estratégico
Lei nº 12.317	2012	Lei	Público	Legislativo
Doutrina militar de defesa cibernética	2014	MD	Público	Estratégico
Marco civil da internet	2014	Legislativo	Público	Legislativo
Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal	2015	GSI	Público	Político Estratégico
Guia Básico de orientações ao gestor em segurança da informação e comunicações	2015	Comitê Gestor da Segurança da Informação	Público	Político Estratégico
Glossário das forças armadas	2015	MD	Público	Estratégico
Estratégia Setorial de Defesa (ESD) 2015	2015	MD	Público	Estratégico
Política Nacional de Inteligência (PNI)	2016	GSI	Público	Político Estratégico
Diretriz para a implantação do comando de defesa cibernética	2016	MD	Público	Estratégico
Política Nacional de Defesa & Estratégia Nacional de Defesa	2016	MD	Público	Político Estratégico

Estratégia Nacional de Inteligência	2017	GSI	Público	Político Estratégico
Norma Brasileira de Gestão de Segurança da Informação (NBSI)	2017	Associação Brasileira de profissionais e empresas da segurança da informação e defesa cibernética	Privado	-
E-Digital - Estratégia Brasileira para a Transformação Digital	2018	Presidência da República	Público	Político Estratégico
Política Nacional de Segurança da Informação	2018	GSI	Público	Político Estratégico
Estratégia Nacional de Ciência Tecnologia e Inovação (2016-2022)	2018	Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC)	Público	Político Estratégico
Política Nacional de Segurança de Infraestruturas Críticas	2018	GSI	Público	Político Estratégico
Planejamento estratégico setorial - 2020-2031	2019	MD	Público	Político Estratégico
Transformação do Projeto Estratégico do Exército de Defesa Cibernética (PEE Def CIBER) em Programa Estratégico do Exército Defesa Cibernética	2019	MD	Público	Político Estratégico
Glossário de Segurança da Informação	2019	GSI	Público	Estratégico
Lei geral de proteção de dados (LGPD)	2020	Presidência da República	Público	Legislativo
Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica	2020	MD	Público	Estratégico
Livro Branco	2020	MD	Público	Político Estratégico

Estratégia Nacional de segurança cibernética (E-ciber)	2020	Gabinete institucional da Presidência (GSI)	Público	Político Estratégico
Revisão da capacidade de cibersegurança do brasil	2020	OEA (Organização dos Estados Americanos)	OI	-
Estratégia Nacional de Segurança de Infraestruturas Críticas	2020	GSI	Público	Político Estratégico
Política Nacional de Defesa & Estratégia Nacional de Defesa	2020	MD	Público	Político Estratégico
Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações	2020	ANATEL (Agência Nacional de Telecomunicações)	Público	-
Sistema Militar de Defesa Cibernética	2020	MD	Público	Estratégico

Fonte: Adaptado de Favero, 2021

Antes de mais nada, é necessário destacar que a produção oficial pode ser tanto estratégica quanto legislativa. A primeira não tem força normativa e costuma ser atualizada com o passar dos anos (como os Livros Brancos). Já a segunda, por serem leis e terem força normativa, não mudam com tanta frequência.

De qualquer forma, a divisão entre documentos legislativos e estratégicos pode ser sutil. Alguns documentos estratégicos podem aparecer em forma de lei, por exemplo. Portanto, o que faz de um documento ser legislativo não é sua forma (divisão por incisos, formatação ou assinatura de autoridades). O que separa os documentos legislativos dos estratégicos é o seu alvo. Enquanto os documentos legislativos tem como função criar normas jurídicas para determinados assuntos, os estratégicos buscam criar um arcabouço estratégico sobre determinado tema. Isso é visível quando distinguimos o marco civil da internet (BRASIL, 2014b) com a política nacional de segurança da informação (BRASIL, 2018b). Enquanto o primeiro cria normas jurídicas, o segundo tenta traçar as bases e objetivos de uma estratégia.

Outra distinção diz respeito à diferença entre documentos políticos estratégicos e documentos apenas estratégicos. Os documentos políticos estratégicos têm maior preocupação de informar a sociedade civil. Os documentos estratégicos minimizam essa necessidade e geralmente são documentos específicos das forças armadas.

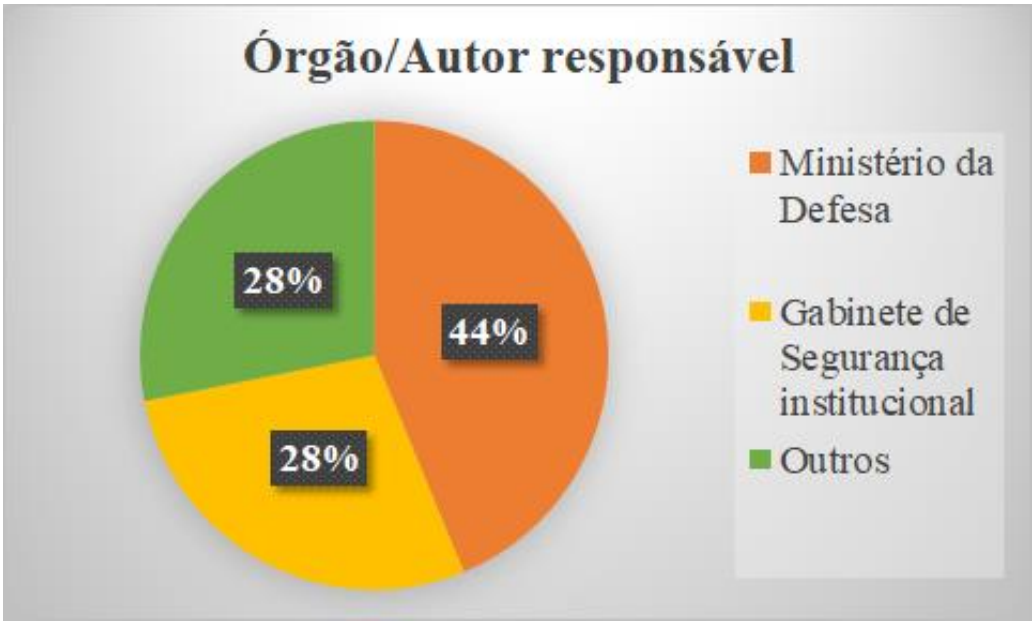
Por fim, existem documentos que não se encaixam em nenhuma destas classes. São os casos de documentos elaborados pela esfera privada, ou por organizações internacionais. O documento feito pela ANATEL (2020) também não entra nessa conceituação, já que seu alvo é a regulamentação interna do setor de telecomunicações.

O mapeamento dos 32 documentos indica forte prevalência de documentos públicos frente aos privados, como visto no gráfico 1 (FAVERO, 2021). O gráfico 2 demonstra que os principais órgãos/autores dos documentos são o Ministério da Defesa (MD) e o Gabinete de Segurança Institucional da Presidência da República (GSI) (FAVERO, 2021).

Figura 5 - Caráter do órgão responsável

Fonte: FAVERO, 2021

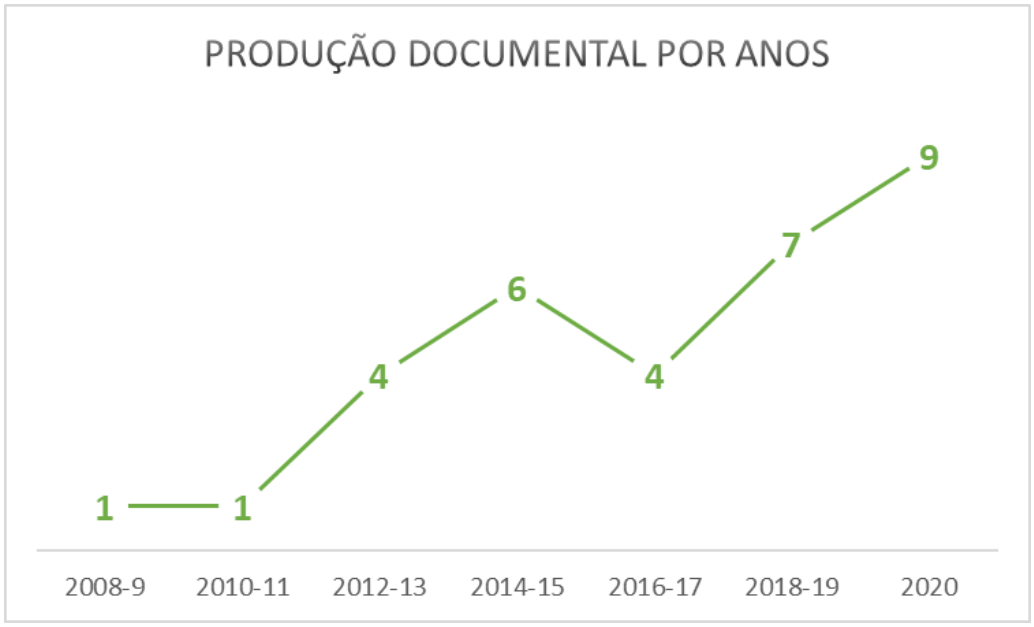
Figura 6 - Órgão/Autor responsável



Fonte: FAVERO, 2021

Uma análise atenta do quadro 5, também revela a tendência de aumento da produção de documentos após 2017. O último biênio e o ano de 2020 tiveram um aumento considerável na produção destes documentos.

Figura 7 - Número de documentos oficiais por ano



Fonte: Elaboração própria

A partir daí, (re)aparece como problema central: o aumento da produção oficial sobre cibernética por parte do governo brasileiro a partir de 2018 gera maior capacidade de influência global? Ou seja, dado o aumento da importância do espaço cibernético nos últimos anos, o governo brasileiro teria a partir de 2018 formulado estratégias documentadas para aumentar seu poder cibernético em termos de capacidade cibernética? Para responder a tal pergunta é necessário se debruçar sobre o conteúdo dos 32 documentos citados.

3.2 SUPERFICIALIDADE E IMPRECISÃO DA MAIORIA DOS DOCUMENTOS

Nesta seção, buscaremos analisar parte dos documentos lançados entre 2018 e 2020, demonstrando que a superficialidade e falta de estratégia clara é uma tônica da maioria dos documentos do período.

3.2.1 Livro Branco de 2020

É provável que o Livro Branco (BRASIL, 2020b) seja um dos documentos mais conhecidos da área de segurança nacional. Em primeiro lugar, deve-se notar que o Livro Branco de 2020 (BRASIL, 2020b) ainda não foi aprovado pelo congresso nacional[19]. Portanto, é o Livro Branco de 2012 (BRASIL, 2012a) que tem validade legal no país. Além disso, a lei complementar 136, de 25 de agosto de 2010 diz que:

> O Poder Executivo encaminhará à apreciação do Congresso Nacional, na primeira metade da sessão legislativa ordinária, de 4 (quatro) em 4 (quatro) anos, a partir do ano de 2012, com as devidas atualizações: I - a Política de Defesa Nacional; II - a Estratégia Nacional de Defesa; III - o Livro Branco de Defesa Nacional (BRASIL, 2010a, não paginado).

Desta maneira, logo percebe-se que além da não aprovação do congresso do livro branco de 2020 (BRASIL, 2020b), não foi respeitada a temporalidade necessária para a produção do Livro Branco. Caso contrário, o Livro Branco de 2016 estaria disponível publicamente. Muito provavelmente, caso a discussão em defesa nacional fosse prioridade no debate político do país, a lei complementar (BRASIL, 2010a) teria sido honrada e o livro de 2020 (BRASIL, 2020b) já aprovado pelo congresso nacional.

[19] A notícia mais atual que dispomos sobre a aprovação da PND e END (BRASIL, 2020c) e do Livro Branco (BRASIL, 2020b) é de junho de 2022, quando o senado as aprovou. O texto agora seguirá para a câmara dos deputados (AGÊNCIA SENADO, 2022).

Convém também explicitar as funções do livro branco. O Livro branco tem como principais funções: dizer abertamente à sociedade quais são as estratégias de defesa do país em questão e anunciá-las aos vizinhos (PLUM, 2020). Assim, busca-se inserir a defesa nacional no debate político e democrático, além de deixar claro aos países limítrofes quais são as intenções e finalidades do poder militar brasileiro. Por consequência, pode-se dizer que o Livro Branco seria também uma espécie de Diplomacia de Defesa (PLUM, 2020).

Entendendo a centralidade da produção dos Livros Brancos para a defesa nacional, esperaria-se que o documento traçasse estratégias fundamentais para o Brasil no espaço cibernético. Embora os Livros Brancos de 2020 e 2012 (BRASIL, 2012a; BRASIL, 2020b) afirmem que o setor cibernético, nuclear e o aeroespacial sejam estratégicos para a defesa nacional, os documentos são excessivamente genéricos e não tratam a cibernética com o aprofundamento necessário.

Além da definição de que o setor cibernético ficaria a cargo do exército, o documento elenca que significativos avanços vêm sendo feitos (BRASIL, 2020b), mas apenas discorre sobre o Comando de Defesa Cibernética (ComDCiber):

> O Setor Cibernético acolhe as áreas operacional e de ciência e tecnologia. Sob a coordenação do Exército, **significativos avanços** têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. A proteção do espaço cibernético abrange um grande número de áreas, como capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede. O Comando de Defesa Cibernética (ComDCiber), organização militar conjunta, na estrutura organizacional do Comando do Exército, ativada em 2016, vem somar esforços com outras organizações governamentais e tem como principais atribuições: planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinária, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa. (BRASIL, 2020b, p. 46-7, grifo do autor)

O documento reconhece também a importância da interação entre instituições de pesquisa, mas de forma alguma diz como ela poderia ser fortalecida: “A interação entre instituições de pesquisa civis e militares, universidades e empresas é fundamental para integrar os esforços na criação de polos de alta tecnologia em variadas áreas”. (BRASIL, 2020b, p. 135).

As duas últimas citações são praticamente as únicas partes do extenso documento que discutem com maior profundidade as necessidades do setor cibernético. Mesmo assim, pode-se entender que tais citações são muito mais “resumos informativos” sobre o tema que propriamente estratégias. O documento padece claramente de uma discussão qualificada sobre

as estratégias pragmáticas pelas quais o país poderia se projetar como *player* internacional no espaço cibernético.

3.2.2 PND e END de 2020

A necessidade de atualização periódica discutida acima vale também para a PND e a END (Estratégia Nacional de Defesa. A END foi lançada em 2008 (BRASIL, 2008), 2012 (BRASIL, 2012b), 2016 (BRASIL, 2016) e em 2020 (BRASIL, 2020c). Já a PND foi elaborada em 2012 (BRASIL, 2012b), 2016 (BRASIL, 2016) e em 2020 (BRASIL, 2020c). Em maio de 2022, a última END e PND aprovadas pelo congresso eram as de 2016 (BRASIL, 2018g)[20]. Assim como o livro branco (BRASIL, 2020c), os documentos supracitados não são documentos específicos sobre cibernética. Diante disso, a discussão sobre cibernética aparece em tópicos específicos e não é profunda.

A importância da PND (BRASIL, 2020c) é clara:

> A PND é o documento condicionante de mais alto nível para o planejamento de ações destinadas à defesa do País. Voltada prioritariamente para ameaças externas, estabelece objetivos para o preparo e o emprego **de todas as expressões do Poder Nacional**, em prol da Defesa Nacional (BRASIL, 2020c, p.7, grifo do autor)

Grifa-se a importância do termo: "todas as expressões do poder nacional" (BRASIL, 2020b, p.7), que poderia facilmente enquadrar o poder cibernético. Além disso, o termo poder aparece novamente em: "Coordenada pelo Ministério da Defesa, a PND articula-se com as demais políticas nacionais, com o propósito de integrar os esforços do Estado brasileiro para consolidar o seu Poder Nacional" (BRASIL, 2020c, p.11).

O documento também reconhece as "eventuais insuficiências e obsolescências de equipamentos das Forças Armadas e a falta de regularidade nas aquisições" (BRASIL, 2020c, p.13), que também é reconhecida por Oliveira e Portela (2017). Uma maneira de reduzir as insuficiências das forças armadas e diminuir a dependência da importação de tecnologia importada faz referências ao IV objetivo nacional de defesa: "promover a autonomia produtiva e tecnológica na área de defesa" (BRASIL, 2020c). Essa necessidade de criação nacional de tecnologias será melhor explorada no próximo capítulo. O documento também faz referência ao espaço cibernético:

> Adicionalmente, requerem especial atenção a segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de

[20] Tal decreto diz que foram aprovadas a END e a PND de 2016 (BRASIL, 2016) e também o Livro Branco de 2016. Mas Após as pesquisas, o Livro Branco de 2016 não foi encontrado.

> informações, de gerenciamento e de comunicações de interesse nacional (BRASIL, 2020c, p.14).

A END e a PND, na versão de 2020 (BRASIL, 2020c), foram lançadas na forma de um mesmo livro. Podemos afirmar que a END (BRASIL, 2020c) seria uma continuação natural da PND (BRASIL, 2020c). Ou seja, a END (BRASIL, 2020c) trataria de pôr em prática de forma estratégica as questões levantadas pela PND (BRASIL, 2020c). Visto por este ângulo, esperaria-se que a END (BRASIL, 2020c) tratasse de objetivos mais pragmáticos em matéria de cibernética. A questão do poder nacional também aparece na END, mas não relacionado ao poder cibernético:

> O Poder Nacional apresenta-se como a conjugação interdependente de vontades e meios, voltada para o alcance de determinada finalidade. De vontades, por ser este um elemento imprescindível à sua manifestação, tornando-o um fenômeno essencialmente humano, individual ou coletivo; de meios, por refletir as possibilidades e limitações das pessoas que o constituem e dos recursos de que dispõe. (BRASIL, 2020c, p. 35)

O documento levanta igualmente a importância do processo de dissuasão (BRASIL, 2020c). Tal processo seria eficaz para desestimular ataques ao Brasil (BRASIL, 2020c). Entre os possíveis elementos materiais da dissuasão, estariam o Sistema Integrado de Fronteira (SISFRON) e o sistema de defesa cibernética (BRASIL, 2020c), ambos tratados no próximo capítulo. Há também uma preocupação da atuação entre a academia, setores públicos e base industrial de defesa, para que possam juntos fortalecer as capacidades de defesa (BRASIL, 2020c). Porém, mais uma vez, a discussão sobre o tema é apenas mencionada, sem que saídas objetivas sejam mapeadas.

Embora a END (BRASIL, 2020c) seja essa espécie de continuação natural da PND (BRASIL, 2020c), ela não aprofunda de maneira razoável as estratégias a serem seguidas no espaço cibernético. Há semelhança no tom da END e PND (BRASIL, 2020c) com o do livro branco (BRASIL, 2020b): estratégias cibernéticas mencionadas de forma genérica mas não especificadas.

3.2.3 Planejamento estratégico setorial (2020-2031) e SMDC

Seguindo a imprecisão dos documentos já citados, temos o Planejamento estratégico setorial - 2020-2031 (BRASIL, 2019b). O documento menciona o fator recurso humano e da

infraestrutura seguindo a forma já vista anteriormente, e cita de forma genérica o ponto 7.2 e suas subdivisões:

> ESD 7.2 - Atuar no espaço cibernético de forma efetiva e negar o seu uso contra os interesses da defesa nacional. 7.2.1 - **Implantar o Sistema Militar de Defesa Cibernética** (SMDC). ASD 7.2.2 - Promover a interoperabilidade do setor cibernético na defesa nacional. ASD 7.2.3 - **Implantar a infraestrutura necessária ao desenvolvimento do setor cibernético**. ASD 7.2.4 - Implantar o Sistema de Homologação e Certificação de Produtos de Defesa Cibernética. ASD 7.2.5 - **Capacitar recursos humanos para atuar no setor cibernético**. ASD 7.2.6 - Implantar o Sistema de Informações Seguras no setor de defesa. ASD 7.2.7 - **Fomentar a pesquisa e o desenvolvimento de produtos de defesa cibernética**. ASD 7.2.8 - Contribuir para a construção da capacidade nacional de defesa de gestão da informação e a capacidade militar de defesa de superioridade de informações (BRASIL, 2019b, p.25, grifo do autor).

Algo muito parecido ocorre com o documento "Sistema militar de defesa cibernética" (BRASIL, 2020d). O documento em questão tem o mesmo nome do órgão objeto do documento (Sistema Militar de Defesa Cibernética - SMDC):

> O SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses (BRASIL, 2020d, não paginado).

Como principal setor do SMDC, temos o já citado Comando de Defesa Cibernético (COMDCiber) (BRASIL, 2020d). São também do SMDC (Sistema Militar de Defesa Cibernética) as estruturas de defesa cibernética das forças singulares (marinha e aeronáutica) e estruturas de guerra cibernética dos comandos operacionais ativados (BRASIL, 2020d). Podemos depreender que o SMDC seria uma espécie de estrutura guarda-chuva, que englobaria setores e outros órgãos centrais para a defesa cibernética brasileira.

O documento não vai muito além da setorização do próprio SMDC e das interações desse órgão com o ministério da defesa e de setores não relacionados diretamente com a defesa (como o GSI). Também seria atribuição do SMDC: "fomentar a pesquisa, o desenvolvimento e a inovação das capacidades cibernéticas de interesse da Defesa" (BRASIL, 2020d, não paginado), mas não se desenvolve como isso seria colocado na prática.

3.2.4 Transformação do PEE Def CIBER em Prg EE Def Ciber e Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica

Ao contrário dos documentos anteriores, o documento "Transformação do Projeto Estratégico do Exército de Defesa Cibernética em Programa Estratégico do Exército Defesa

Cibernética" (BRASIL, 2018a) traz algum nível de especificidade de estratégias, mesmo que insuficientes. O documento secciona o programa estratégico de defesa cibernética do exército:

Figura 8 - Programa estratégico de defesa cibernética e seus desdobramentos I

Fonte: BRASIL, 2018a

Figura 9 - Programa estratégico de defesa cibernética e seus desdobramentos II

Fonte: BRASIL, 2018a

A título de exemplo, segue a definição completa de do subprojeto gestão de talentos:

> Estruturar e consolidar a gestão de recursos humanos de modo a suprir as necessidades da Força Terrestre, organizar a procura e a admissão, gerir a capacitação e a administração do pessoal, bem como sua permanência nas atividades do setor cibernético (BRASIL, 2018a, p.86).

Sem fazer referência ao capital investido em cada um dos subprojetos[21] e nem do número de pessoas que nele trabalham, é complexo precisar suas reais capacidades, e se são suficientes.

O mesmo ocorre com o documento "Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica" (BRASIL, 2020e). O documento é parcialmente pragmático, já que desenvolve ligeiramente alguns objetivos:

> Estabelecer e aplicar, nos estabelecimentos de ensino (formação, aperfeiçoamento e altos-estudos), um currículo mínimo para a integração dos conhecimentos e difusão das características comuns das atividades de Guerra Eletrônica (BRASIL, 2020e, não paginado).

Mesmo tentando traduzir objetivos mais gerais para mais específicos (sobretudo no tema da guerra eletrônica) o documento novamente não exemplifica qual seria o conteúdo do currículo mínimo e nem como seria aplicado (BRASIL, 2020e). Também não traz o montante disponível para "estimular o financiamento de Pesquisa e Desenvolvimento na área de guerra eletrônica (BRASIL, 2020e, não paginado).

3.2.5 PNSI

A Política Nacional de Segurança da informação (PNSI) (BRASIL, 2018b), tem como objetivo "assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional". (BRASIL, 2018b, não paginado). No documento aparece também a ideia de que o termo segurança da informação engloba tanto defesa quanto segurança cibernética (BRASIL, 2018b).

Um fator interessante sobre este documento é que ele prevê a criação da Estratégia Nacional de Segurança da Informação (ENSI). A ENSI teria participação da sociedade civil na sua elaboração (BRASIL, 2018b). O último documento, que até o momento não foi criado, deveria ser dividido em módulos, dentre os quais: I - segurança cibernética; II - defesa cibernética; III - segurança das infraestruturas críticas (BRASIL, 2018b). O módulo de segurança cibernética já foi elaborado (BRASIL, 2020f), assim como a estratégia nacional de infraestruturas críticas (BRASIL, 2020a) e constam no próximo subcapítulo. O documento referente à defesa cibernética não foi lançado até a escrita desta monografia.

[21] Como será visto no capítulo 4, o documento traz o capital investido no programa estratégico defesa cibernética como um todo, mas não em cada subprojeto.

A PNSI (BRASIL, 2018b) se refere a divisão de funções entre o MD (Ministério da Defesa e o GSI, que será melhor explorada no próximo capítulo (BRASIL, 2018b). Mesmo que os módulos de segurança cibernética (BRASIL, 2020f) e de infraestruturas críticas (BRASIL, 2020a) gerados a partir da PNSI (BRASIL, 2018b) sejam documentos relevantes, o mesmo não ocorre com a própria PNSI (BRASIL, 2018b), que define objetivos muito gerais.

3.2.6 PNSIC

A PNSIC (Política Nacional de Segurança de Infraestruturas Críticas) (BRASIL, 2018c) é um documento que serviu de base para a criação da ENSIC (Estratégia Nacional de Segurança de Infraestruturas Críticas) (BRASIL, 2020a). Uma das suas principais colaborações é a consolidação do termo infraestruturas críticas e seus associados:

> I - infraestruturas críticas - instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade; II - segurança de infraestruturas críticas - conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas; III - interdependência de infraestruturas críticas - relação de dependência ou interferência de uma infraestrutura crítica em outra ou de uma área prioritária de infraestruturas críticas em outra (BRASIL, 2018c, não paginado).

Os princípios gerais que regem a PNSIC (BRASIL, 2018c) são: a prevenção e precaução, integração de esferas do poder público e redução de custos para sociedade através de investimentos e segurança (BRASIL, 2018c). O principal objetivo do documento é evitar a interrupção do funcionamento das infraestruturas críticas e garantir diretrizes e instrumentos para protegê-las (BRASIL, 2018c).

No próprio documento, fala-se da necessidade de que a ENSIC (BRASIL, 2020a) consolide conceitos, defina eixos estruturantes e mapeie desafios sobre o tema das infraestruturas críticas (BRASIL, 2018c). Seguindo a tônica da PNSI (BRASIL, 2018b), a PNSIC (BRASIL, 2018c) gera um documento de relevância a ENSIC (BRASIL,2020f), mas seu conteúdo define objetivos muito pouco específicos. Seu maior feito seria:

> caracterizar a segurança de infraestruturas críticas como uma atividade de Estado, sinalizando à sociedade brasileira a prioridade que o Governo brasileiro atribui ao tema no âmbito da segurança institucional (BRASIL, 2020a, não paginado).

3.2.7 Outros documentos

Falando propriamente de questões de segurança cibernética, há a Lei Geral de Proteção de Dados (BRASIL, 2018d). Com o objetivo de estabelecer normas para a proteção de dados, esta lei não trata sobre defesa nacional. Isso é visível através da sua definição de segurança, focada na questão de dados sensíveis: “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2018d, não paginado).

Por fim, a Estratégia Nacional de Ciência Tecnologia e Inovação 2016-2022 (BRASIL, 2018e), centraliza a questão de defesa nacional na discussão aeroespacial, e trata da muito brevemente (e de forma vaga) sobre defesa e seguranças cibernéticas:

> iii. Fortalecimento da indústria de tecnologia digital e de segurança cibernética crítica para a competitividade produtiva, a valorização da capacidade de expressão e opinião e a segurança nacional”. iv. Fortalecimento do Centro Nacional de Defesa cibernético, com fomento à pesquisa e ao desenvolvimento em defesa cibernética, e da indústria de segurança cibernética para a competitividade produtiva (BRASIL, 2018e, p.19).

3.3 COMPARANDO DEFINIÇÕES

A título de comparação, foram colocados lado a lado cada um dos principais conceitos sobre cibernética e suas definições foram comparadas. As definições foram retiradas de quatro documentos distintos. O resultado se encontra no quadro abaixo:

Quadro 7 - Comparação de conceitos nos diferentes documentos

Conceitos	**Livro Verde de Segurança cibernética**	**Doutrina militar de defesa cibernética**	**Glossário das forças armadas**	**Glossário de segurança de informação**
Segurança Cibernética	"Arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infra-estruturas críticas" (BRASIL, 2009, não paginado).	Mesma do Livro Verde	Mesma do Livro Verde	"Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;" (BRASIL, 2019a, não paginado)
Defesa Cibernética	-	"Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento	Mesma da doutrina militar de defesa cibernética	Muito parecida com a definição da doutrina militar de defesa cibernética (BRASIL, 2019a, não paginado).

		de Inteligência e comprometer os sistemas de informação do oponente". (BRASIL, 2014a, p.18)		
Infraestruturas Críticas	"Instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade" (BRASIL, 2009, não paginado).	Definição muito parecida com a do Livro Verde	Mesma da doutrina militar de defesa cibernética	"instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;" (BRASIL, 2019a, não paginado)
Espaço Cibernético	-	"Espaço virtual, composto por **dispositivos computacionais conectados em redes ou não**, onde as informações digitais transitam, são processadas e/ou armazenadas". (BRASIL, 2014a, p.18, grifo do autor)	Mesma da doutrina militar de defesa cibernética	"Espaço virtual **composto por um conjunto de canais de comunicação da internet e outras redes** de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente" (BRASIL, 2019a, não paginado, grifo do autor).
Guerra Cibernética	"Guerra cibernética: Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para	"Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para	Mesma da doutrina militar de defesa cibernética, acrescida de:	"Atos de guerra utilizando predominantemente elementos de TIC em escala suficiente por um período específico de

	negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil". (BRASIL, 2007, p.123).	negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2" . (BRASIL, 2014a, p.19).	"Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC" (BRASIL, 2015, p.124).	tempo **e em alta velocidade em apoio a operações militares** através de ações tomadas exclusivamente no espaço cibernético de forma a abalar ou incapacitar as atividades de uma nação inimiga, especialmente pelo ataque aos sistemas de comunicação, visando obter vantagem operacional militar significativa. Tais ações são consideradas uma ameaça à Segurança Nacional do Estado (BRASIL, 2019a, não paginado, grifo do autor).
Poder cibernético	-	"Capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder" (BRASIL, 2014a, p.19)	Mesma da doutrina militar de defesa cibernética	-

Fonte: Elaboração Própria

Em primeiro lugar, é necessário dizer que nem todos os documentos mapeados definem conceitos. Aqueles que o fazem são exceções, como os citados acima. Para além disso, a análise do quadro nos traz uma série de conclusões. A mais óbvia é que não há uma padronização de conceitos. Essa falta de padronização apenas demonstra que os documentos não necessariamente conversam entre si. Padronizar conceitos seria um dos primeiros passos para criar uma estratégia sólida de atuação no espaço cibernético, garantindo que todas as partes "falassem a mesma língua". Como visto no capítulo 2, diversos conceitos da área cibernética carecem de definições consensuais, portanto unificar conceitos seria ainda mais urgente. A unificação de conceitos é vista apenas entre a doutrina militar de defesa cibernética (BRASIL, 2014a) e o glossário das forças armadas (BRASIL, 2015). Outra exceção seria a razoável uniformidade vista no conceito de defesa cibernética (BRASIL, 2014a; BRASIL, 2015; BRASIL, 2019a).

Um questionamento possível a esta visão seria de que as diferenças entre as definições são mínimas e, portanto, não fariam diferença na prática. As partes grifadas no quadro tentam desmentir este argumento. Para o glossário da segurança da informação (BRASIL, 2019a), por exemplo, o espaço cibernético é necessariamente ligado a redes. A outra definição contrasta frontalmente com esta ideia, dizendo que o espaço cibernético pode ou não estar ligado a redes (BRASIL,2014a). Embora essa diferença pareça sutil, não é o que se percebe. Como já visto no segundo capítulo, Ventre (2012) acredita que o espaço cibernético não depende da existência de redes. Ou seja, computadores desconectados de redes[22] não fariam parte do ciberespaço para o glossário de segurança da informação (BRASIL, 2019a), mas fariam para a doutrina militar de defesa cibernética (BRASIL, 2014a).

Aliás, a definição de guerra cibernética é mais cirúrgica no glossário da segurança da informação (BRASIL, 2019a). Ao contrário dos outros documentos, o último diz claramente que os atos de guerra cibernética devem ser rápidos e em função das operações militares (BRASIL, 2019a).

A última consideração a ser feita é sobre o poder cibernético. Ele é o único conceito que aparece somente em dois documentos (BRASIL, 2014a; BRASIL, 2015). Isso pode demonstrar a falta de centralidade do termo para os formuladores de estratégia e na pauta de defesa cibernética nacional. O que mais chama a atenção é que o conceito não é encontrado nem mesmo no documento mais atual e que trata especificamente do tema da segurança da

[22] Embora a rede mais conhecida seja a internet, pode-se entender o termo no seu sentido alargado, considerando qualquer rede que exista.

informação (BRASIL, 2019a).

3.4 AS EXCEÇÕES

Neste subcapítulo procuramos analisar os documentos que, ao contrário dos analisados na seção 3.2, tendem a ser menos genéricos e com boa capacidade de diagnosticar debilidades. Serão analisados os seguintes documentos: Estratégia Nacional de segurança cibernética (E-ciber) (BRASIL, 2020f), Estratégia Brasileira para a Transformação Digital (E-digital) (BRASIL, 2018f), Revisão da capacidade de cibersegurança do Brasil (OEA, 2020) e Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) (BRASIL, 2020a).

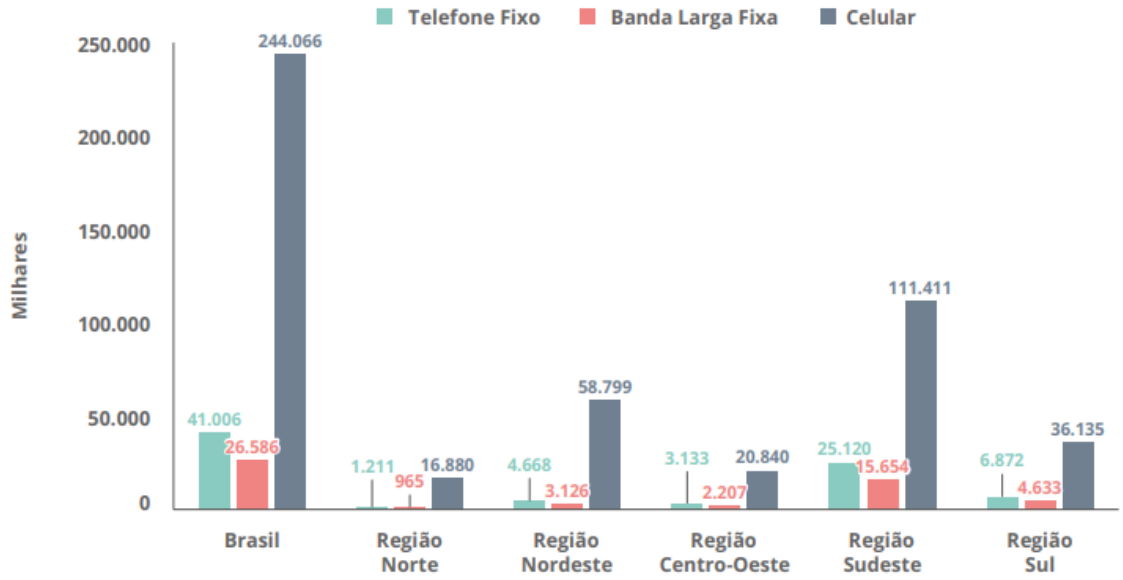
3.4.1 E-digital

A Estratégia Brasileira para a Transformação Digital (E-digital) (BRASIL, 2018f) tem como objetivo traçar uma estratégia de transformação digital no Brasil (BRASIL, 2018f). Sua formulação se deu através da união do Governo Federal; Ministério da Ciência, Tecnologia, Inovações e Comunicações; sociedade e comunidade acadêmica (BRASIL, 2018f). Sob o pano de fundo das rápidas transformações advindas pela internet, a E-digital entende que essa seria uma oportunidade para que o país dê um salto qualitativo nesta esfera (BRASIL, 2018f).

O documento faz considerações importantes sobre o acesso à internet por parte dos brasileiros (BRASIL, 2018f). O enorme território brasileiro traz condições que interferem no acesso dos brasileiros à internet (BRASIL, 2018f). Por um lado, uma vantagem seria a concentração da população brasileira, que concentra 80% da sua população em 0,63% do território (IBGE, 2016). Uma desvantagem seriam os hiatos de acesso (NAVAS-SABATER, 2002). Esses seriam locais afastados que são majoritariamente habitados por populações carentes (NAVAS-SABATER, 2002). Nestes locais o custo da instalação de infraestrutura é alto, e aliado à pequena demanda, impossibilita a criação de infraestrutura de ponta por empresas privadas (BRASIL, 2018f).

Uma forma de superar estes desafios é a utilização de internet por celulares (3G e 4G) (BRASIL, 2018f). Os celulares já são o meio de acesso responsável para 89% das pessoas incluídas digitalmente no Brasil (BRASIL, 2018f). Tal dominância é vista claramente abaixo:

Figura 10 - Quantidade de acessos por serviço no Brasil em 2016



Fonte: (BRASIL, 2018f)

O documento defende claramente que os hiatos de acesso deveriam ser resolvidos por atores privados, atendendo uma demanda reprimida (BRASIL, 2018f). Mas existem também iniciativas públicas, como o Projeto Amazônia Conectada:

> uma rede de cabos subfluviais nos leitos dos rios da bacia amazônica para constituir um backbone de fibra ótica para prover infraestrutura de telecomunicações às regiões mais remotas do norte do País (BRASIL, 2018f, p.19-20).

O documento destaca também a necessidade de uma estratégia de longo prazo para vencer os problemas de infraestrutura e os hiatos de acesso (BRASIL, 2018f).

Logo em seguida, faz-se referência ao marco civil da internet (BRASIL, 2014b). O marco civil garantiu princípios e deveres para a utilização da internet no país (BRASIL, 2018f). De todo modo, a E-digital afirma a: "necessidade de um marco legal específico para tratar do tema preenchendo-se o espaço para regulamentação posterior aberto pelo Marco Civil da Internet" (BRASIL, 2018f, p.38). A E-digital afirma a necessidade de criação de estratégias nacionais para a defesa e segurança cibernética (BRASIL, 2018f). A estratégia referente a segurança cibernética (BRASIL, 2020f) já foi criada e será foco de análise no próximo tópico.

Por fim, o documento faz uma análise sobre a produção de P&D sobre cibernética no país, examina a capacidade brasileira em recursos humanos e faz considerações sobre o estágio de segurança cibernética brasileira (BRASIL, 2018f). Estas variáveis serão analisadas de forma detalhada no próximo capítulo.

3.4.2 E-ciber

A E-ciber (BRASIL, 2020f) é provavelmente o documento mais relevante em matéria de segurança cibernética no Brasil. É um documento que manifesta uma orientação do governo à sociedade brasileira sobre o tema e terá validade entre 2020 e 2023 (BRASIL, 2020f). Foi formulada pelo GSI, mas houve participação da comunidade acadêmica e de instituições privadas em sua formulação (BRASIL, 2020f). Na E-ciber, a questão da defesa cibernética é marginalizada.

É interessante perceber que o próprio documento percebe a lacuna em matéria de estratégia de segurança cibernética no país:

> Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. **Em segundo, nota-se a falta de um alinhamento normativo, estratégico e operacional, o que frequentemente gera retrabalho** ou resulta na constituição de forças-tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações (BRASIL, 2020f, p.2, grifo do autor).

Essa visão corrobora com o subcapítulo anterior, demonstrando que em alguma medida, o próprio governo assume as deficiências brasileiras na construção de uma visão estratégica e operacional sobre o tema. Portanto, o objetivo central do documento é transformar o Brasil em um lócus de excelência em segurança cibernética (BRASIL, 2020f). Como objetivos estratégicos, cita-se a necessidade de:

> 1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020f, p.4-5).

A relação já citada entre as esferas públicas, privadas e acadêmicas deve ser mantida em função do "acompanhamento contínuo e proativo de ameaças e ataques cibernéticos" (BRASIL, 2020f, p.6). Esta reunião desses três setores pode ser chamada de tríplice hélice (PAGLIARI; AYRES PINTO; VIGGIANO, 2020). A tríplice hélice seria uma forma de aumentar as capacidades do país, e consequentemente, gerar mais poder ao Brasil (PAGLIARI; AYRES PINTO; VIGGIANO, 2020). Com a complexidade e rápidas mudanças ocorridas no setor cibernético, nenhum ator poderá sozinho enfrentar todos os desafios impostos por essa revolução informacional (BRASIL, 2020f), sendo primordial a formação da tríplice hélice. O

papel do governo neste contexto seria coordenar o funcionamento deste sistema tripartite (BRASIL, 2020f).

Logo em seguida, a E-ciber faz um diagnóstico dos riscos econômicos de ameaças cibernéticas para o Brasil, que é o segundo país com maiores perdas por ataques cibernéticos (BRASIL, 2020f)[23]. Cita-se também que apenas 11% dos órgãos federais têm nível adequado em governança cibernética (BRASIL, 2020f). Por fim, o documento apresenta o dado de que o Brasil seria o 70º colocado no índice de segurança global da ITU (International Telecommunication Union) (2018) e 66º no ranking das Nações Unidas de tecnologia da informação e comunicação (ITU, 2017).

A falta de legislação também seria um problema que corrobora para os índices acima referidos, e transforma o Brasil no principal alvo dos países da América Latina (EUROPOL, 2018). Mais da metade de todos os ataques cibernéticos registrados no país tem origem doméstica (EUROPOL, 2018).

Portanto, é importante que as instituições mapeiam suas vulnerabilidades e o estágio de desenvolvidos na qual se encontram (BRASIL, 2020f). Esse mapeamento permite que uma estratégia de mudança de processos possa ser iniciada. Vale lembrar que no Brasil, as instituições são livres para adotar suas próprias metodologias de gestão de riscos (BRASIL, 2013). Essa falta de uniformidade se transforma em um problema:

> dificulta a análise do grau de maturidade em segurança cibernética do País de forma geral, uma vez que os critérios e requisitos de cada normativo não são os mesmos, so que torna necessário padronizar as melhores práticas (BRASIL, 2020f, p.14).

Com esta miscelânea de regulamentações individuais, é fundamental a criação de uma lei que centralize, regule e especifique responsabilidades (BRASIL, 2020f). Embora seja citada a importância de marcos regulatórios como o Marco Civil da Internet (BRASIL, 2014b) e a LGPD (BRASIL, 2018d), elas não foram suficientes: "o nível de articulação e de normatização das instituições brasileiras nos temas relacionados à segurança cibernética ainda é tímido, e exigem esforço adicional (BRASIL, 2020f, p.24)".

Finalmente, o documento destaca que a falta de profissionais capacitados em cibernética está aliada a uma "baixa conscientização dos usuários" (BRASIL, 2020f, p. 33). A carência de alfabetização digital no país aumenta a probabilidade de ataques cibernéticos, já que os usuários tendem a não fazer um uso seguro da internet (BRASIL, 2020f).

[23] Embora não haja uma definição dos alvos destes ataques (à sociedade ou ao Estado Nacional), dado que o foco do documento seja segurança cibernética, acredita-se que o termo "ataques" faça referência à sociedade e órgãos do governo não ligados às forças armadas

3.4.3 ENSIC

Como já dito anteriormente, a ENSIC (BRASIL, 2020a) foi precedida pela PNSIC (BRASIL, 2018c) e já citada como importante pela PNSI (BRASIL, 2018b). A ENSIC (BRASIL, 2020a) ressalta a centralidade e importância das infraestruturas críticas, sobretudo numa sociedade cada vez mais conectada e dependente de sistemas. O funcionamento da sociedade moderna sem tais infraestruturas gera caos social (BRASIL, 2020a), como por exemplo, falta de energia elétrica, sistemas governamentais eletrônicos instáveis e etc. O documento também afirma que: "quando não são capazes de suportar os impactos de um choque, as infraestruturas críticas podem atuar como multiplicadores de riscos, aumentando a gravidade da situação" (BRASIL, 2020a, não paginado).

Assim sendo, é necessário que o Brasil mapeie suas próprias infraestruturas críticas e se adiante para quaisquer imprevistos que as envolva (BRASIL, 2020a). É essencial ressaltar que não apenas danos humanos (como sabotagem) podem afetar tais infraestruturas, mas também naturais (BRASIL, 2020a). Furacões, terremotos ou chuvas intensas podem colocar em xeque o funcionamento perfeito de infraestruturas críticas. Outro fator multiplicador de riscos é certamente a extensão das fronteiras e das dimensões do país, justificando uma vigilância ativa das infraestruturas críticas (BRASIL, 2020a).

Com a centralidade supracitada das infraestruturas críticas, o GSI (Gabinete de Segurança Institucional da Presidência da República) criou um grupo de trabalho sobre o tema, composto por representantes de órgãos especialistas no assunto (BRASIL, 2020a). Entre seus objetivos constam a classificação e identificação de infraestruturas críticas e suas respectivas ameaças (BRASIL, 2020a). Partindo desta ideia, poderíamos afirmar que o processo de securitização de tais infraestruturas no país já começou.

Há também o chamado problema das ilhas de informação (BRASIL, 2020a). Ilhas de informação seriam os sistemas comandados por empresas privadas, que são construídos de acordo com as particularidades de cada infraestrutura (BRASIL, 2020a). Com um planejamento específico para cada infraestrutura, é complexo para que o governo administre crises de maneira eficaz a partir de uma visão integrada dos sistemas (BRASIL, 2020a). Portanto, o documento prega algum tipo de "sistema centralizado de gestão da informação" (BRASIL, 2020a, não

paginado). Como já visto na análise da E-ciber (BRASIL, 2020f) não são apenas as empresas privadas que fazem sistemas próprios de segurança, mas também instituições públicas.

Em sua parte final, a ENSIC (BRASIL, 2020a) traz uma tabela. Esta tabela discorre sobre os objetivos mais gerais (eixos estruturantes) para transformá-los em mais específicos. Destacamos o eixo conscientização e capacitação (BRASIL, 2020a). Dada a carência da cultura de proteção das infraestruturas críticas no Brasil, é necessário que o país trace algumas estratégias. Algumas delas seriam a integração da PNSIC com outras políticas de estado e: "Fomentar as ações de capacitação existentes em defesa e segurança de infraestruturas críticas [...] Estimular o interesse no tema de segurança de infraestruturas críticas por meio de reconhecimento de mérito" (BRASIL, 2020a, não paginado). Além disso, é primordial que haja uma prioridade de orçamento para que possa se manter a prevenção de ataques nas infraestruturas críticas (BRASIL, 2020a).

3.4.4 Revisão da capacidade de cibersegurança do Brasil

O último documento "Revisão da Capacidade de Cibersegurança do Brasil" (OEA, 2020) é o único documento elaborado por uma Organização Internacional. O documento analisa cinco esferas sobre o tema no país: a) Política e estratégia de segurança cibernética, b) cultura cibernética e sociedade, c) educação, treinamento e competências em segurança cibernética, d) normas, organizações e tecnologias e e) Estruturas jurídicas e regulamentações (OEA, 2020). De forma geral, os destaques negativos vão para cultura cibernética na sociedade e educação e treinamento em segurança cibernética (OEA, 2020). O item "c" será analisado no próximo capítulo, enquanto os itens "b", "d" e "e" ainda nesta seção.

Sobre a dimensão cultura cibernética e sociedade, o documento afirma que são setores financeiros e de Tecnologia da Informação que estão melhor preparados em segurança cibernética, justamente por serem alvos constantes de ataques (OEA, 2020). A população também padece de uma cultura informacional sólida (OEA, 2020).

A análise sobre as estruturas jurídicas sobre cibernética no Brasil faz alusão à falta de legislação específica sobre o assunto no país, uma análise aproximada com a da E-ciber (BRASIL, 2020f) e da E-digital (BRASIL, 2018f). Por fim, a dimensão de normas, organizações e tecnologias conclui que no país há uso de software seguro na administração

pública federal e que existe ampla gama privada de softwares voltados para a segurança cibernética no país[24] (LINS, 2007; OEA, 2020).

3.5 CONCLUSÕES PARCIAIS

A partir da leitura deste capítulo, é possível tirar algumas conclusões. A primeira é que entre os documentos mapeados nos anos de 2018 a 2020, a maioria deles trata a cibernética de forma genérica. Há aqueles como o Livro Branco (BRASIL, 2020b) PND e END (BRASIL, 2020c) que meramente citam a questão da cibernética. Há também os documentos específicos sobre o tema, mas que também traçam objetivos gerais. Quando não o fazem e têm algum grau de especificidade (BRASIL, 2018a; BRASIL, 2020e) não tratam de dados relevantes, como o orçamento, por exemplo.

A análise de conceitos da área cibernética nos documentos também reforça a falta de estratégia clara do governo brasileiro em cibernética. A falta de padronização de conceitos leva a definições distintas dos mesmos termos, dificultando que todos os atores possam se entender objetivamente. É difícil imaginar que possa haver uma estratégia clara de atuação no espaço cibernético se nem mesmo os termos mais centrais do tema foram debatidos e estabelecidos.

Mesmo assim, existem documentos que fogem desta generalidade vista. Os documentos da seção 3.4 são exemplos. Eles têm principalmente uma preocupação diagnóstica, se apoiando em dados e índices para explorar a situação do país nas diferentes subáreas da cibernética. Muitas vezes, esta análise diagnóstica permite que as vulnerabilidades do país sejam melhor inventariadas, o que poderia servir de base para a sua superação.

Vale ressaltar que embora diagnósticos, os documentos da seção 3.4 tem limites. Um deles seria que os documentos, por exemplo, não conseguem mensurar com exatidão a quantidade de capital necessária para sanar as debilidades de cada área. Assim, seria necessário um nível de investigação maior sobre cada debilidade específica. O segundo limite seria o legislativo. Como documentos estratégicos[25], os documentos citados não são capazes por si só de encaminhar soluções, mas somente sugeri-las. Seria necessário transformar os resultados documentais em prática (TILLY, 2007) e em capacidades cibernéticas reais.

---

[24] Como será melhor visto no capítulo três, o mesmo não ocorre com questões de defesa cibernética, o que gera vulnerabilidades ao país.

[25] Aqui, é necessário lembrar que os 4 documentos da seção 3.4 são políticos estratégicos, e não legislativos. Logo, não haveria necessidade de cumpri-los em sua integridade, já que não são vinculativos.

4 CAPACIDADE DE INFLUÊNCIA DO BRASIL: UMA REALIDADE?

Cabe a este capítulo analisar se, as vulnerabilidades diagnosticadas pelos documentos da seção 3.4 vem sendo sanadas, no sentido de gerar as capacidades cibernéticas tão relevantes na garantia dos instrumentos físicos e de informação dos quadros 2 e 3 (NYE JR, 2010). Para tanto, será feita uma análise da capacidade cibernética do país, para no final julgá-la como adequada ou não. Para que isso ocorra, será necessário em primeiro lugar explicitar a divisão de competências sobre segurança e defesa cibernética nos órgãos públicos brasileiros.

A partir daí, serão qualificadas as capacidades cibernéticas do país. Com este propósito, serão analisadas variáveis que influem diretamente na formação de capacidades cibernéticas: capital investido, P&D, recursos humanos e sistemas de defesa. Acredita-se que estas variáveis sejam essenciais para que as vulnerabilidades do pais sejam superadas, sendo possível que o país exerça seu poder globalmente. Para sustentar tal análise, serão compilados diferentes trabalhos acadêmicos e também os próprios documentos já analisados, que versam sobre o assunto.

4.1 ATRIBUIÇÕES DE SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL

Basicamente, a divisão de atribuições do Brasil em matéria de defesa e segurança cibernética segue uma divisão em níveis. No primeiro nível (o político) está a segurança cibernética. Ela é competência expressa da Presidência da República e do GSI (BRASIL, 2014a), que envolve:

> I - Estabelecer norma sobre a definição dos requisitos metodológicos para a implementação da gestão de risco dos ativos da informação pelos órgãos e pelas entidades da administração pública federal; II - aprovar diretrizes, estratégias, normas e recomendações; III - elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores públicos federais e da sociedade (BRASIL, 2018b, não paginado).

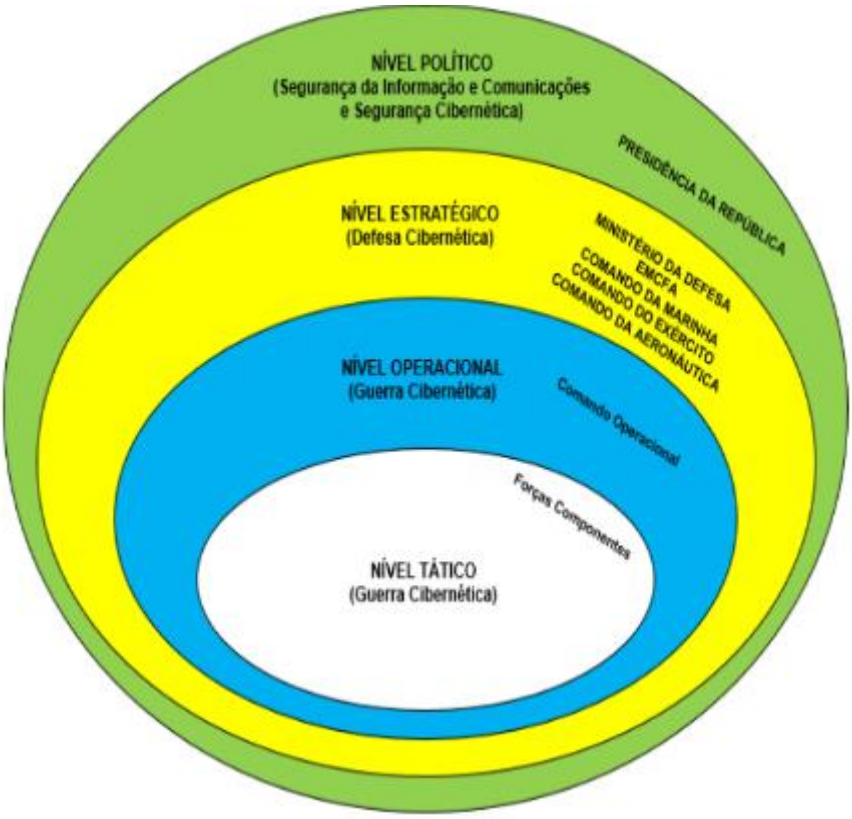
Já o segundo nível (o estratégico) faz referência a defesa cibernética, que é efetuada pelo MD e o comando das Forças Armadas (BRASIL, 2014a). São suas atribuições:

> I - apoiar o Gabinete de Segurança Institucional da Presidência da República nas atividades relacionadas à segurança cibernética II - elaborar as diretrizes, os dispositivos e os procedimentos de defesa que atuem nos sistemas relacionados à defesa nacional contra ataques cibernéticos (BRASIL, 2018b, não paginado).

Os níveis seguintes (terceiro e quarto) são ambos referentes à guerra cibernética (BRASIL, 2014a). O terceiro nível (o operacional) é administrado pelo comando operacional,

enquanto o quarto (o tático) é comandado pelas forças componentes (BRASIL, 2014a). Nota-se também que os níveis tendem a ficar cada vez mais técnicos. O comando operacional e as forças componentes, por exemplo, atuariam militarmente no caso de guerra cibernética, enquanto o GSI apenas politicamente.

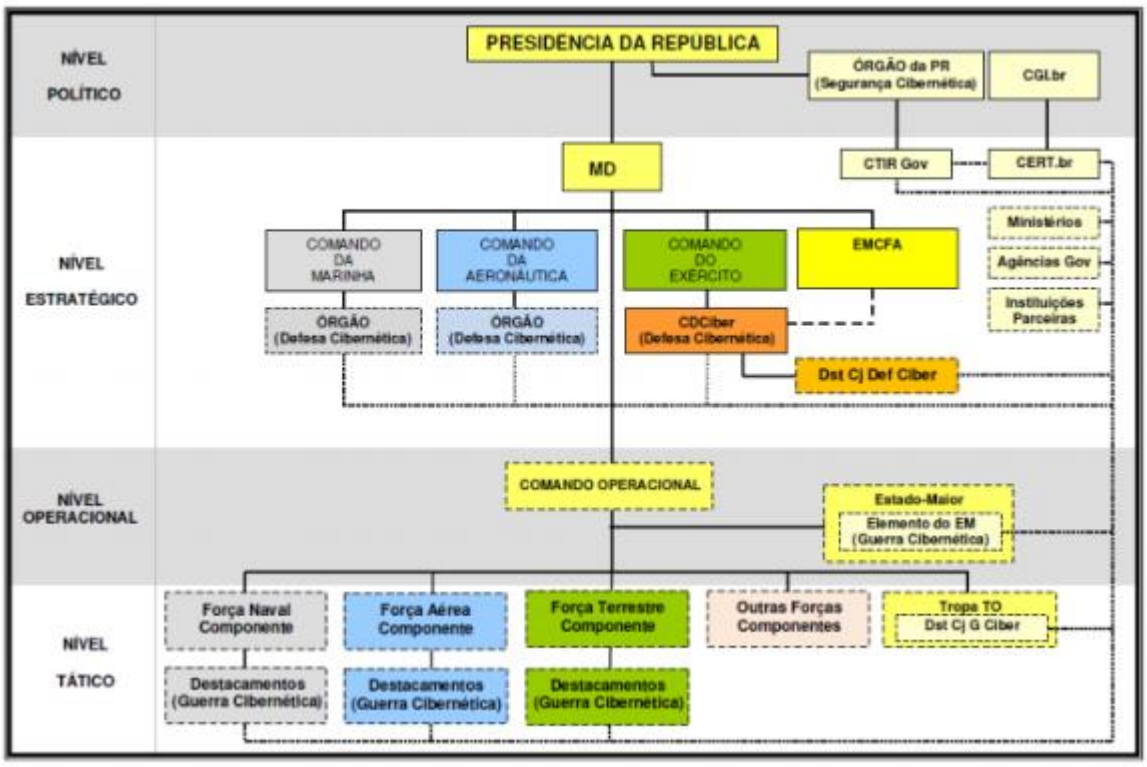
Figura 11 - Níveis de atuação



Fonte: BRASIL, 2014a

A figura acima ilustra também a hierarquia necessária entre os diferentes níveis. As esferas inferiores são sempre dominadas pelas as superiores. Ou seja, o GSI pode determinar que o MD atue de certa forma, mas o GSI não se submete ao MD. A mesma mecânica ocorre nos outros níveis. A dominância da presidência da república sobre a atuação das forças armadas é um princípio constitucional (BRASIL, 1988) e é visível na figura a seguir:

Figura 12 - Hierarquia dos níveis de atuação



Fonte: BRASIL, 2014a

4.2 ANÁLISE DAS CAPACIDADES CIBERNÉTICAS BRASILEIRAS

Explicadas as competências de cada órgão, neste subtópico será examinado se as vulnerabilidades citadas pelos documentos foram sanadas, através da criação de capacidades cibernéticas. Para efetuar esta análise qualitativa, foram selecionadas quatro variáveis: capital investido, recursos humanos, P&D, e os sistemas de defesa do país. Espera-se que cada uma destas variáveis possa ajudar a definir a real competência do país e ver se as vulnerabilidades ainda persistem.

4.2.1 Investimentos

Uma variável fundamental para nosso estudo é o investimento. É simples perceber que há uma relação direta entre investimento e criação de capacidades. Enquanto maior for o investimento, maior será a geração de capacidades de defesa. Neste sentido, faz-se necessário

investir em “recursos de ordem material e imaterial” (FARIAS; FERRAZ, 2018, p.7), como: “sistemas informatizados, redes de transmissão de informações, softwares, hardwares, além de conhecimentos especializados sobre informática e programação de computadores” (FARIAS; FERRAZ, 2018, p.7).

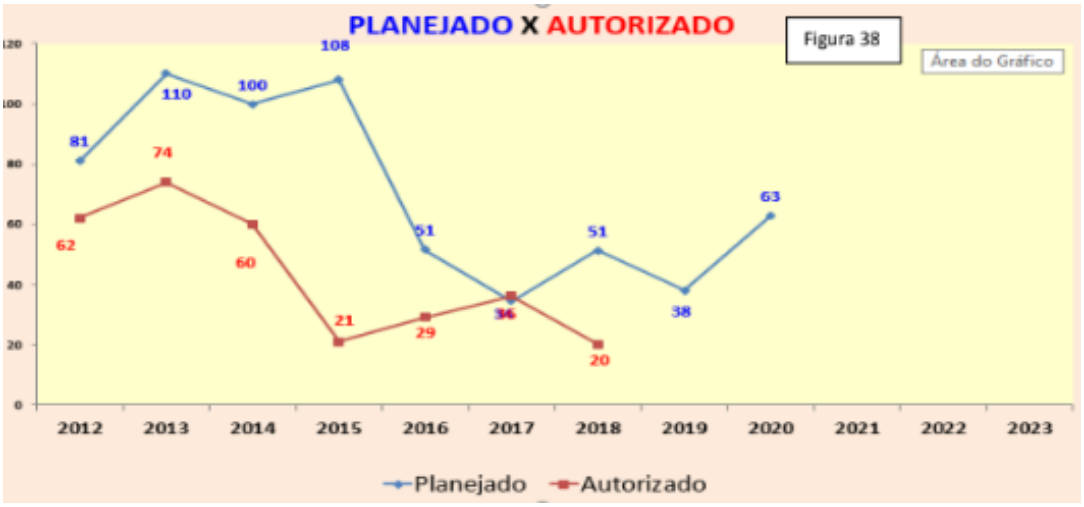
Um exemplo visível desta relação entre capacidade e investimento é tratado por Carneiro (2016). Fazendo um estudo sobre as estruturas defasadas de guerra cibernética, o autor conclui que tais estruturas não são eficientes, sendo necessária sua atualização e investimento (CARNEIRO, 2016). Concordam com esta visão os autores Portela (2020) e Lopes e Silva (2020) quando discutem que apenas o investimento em inteligência cibernética aumentaria a capacidade de dissuasão do país.

Assim, seria interessante comparar o investimento brasileiro na área cibernética com a maior potência do sistema internacional, os Estados Unidos:

> Para ter uma comparação, enquanto se prevê R$839 milhões de gastos no período de 20 anos [no brasil] , nos EUA o valor proposto dentro do orçamento do Departamento de Defesa somente para 2014 é de cerca de R$10,7 bilhões (AGOSTINI, 2014, P.78).

Uma outra comparação seria entre Espanha e Brasil, que teriam posições mais semelhantes no sistema internacional. A Espanha investiu cerca de 67 milhões de reais em defesa e segurança cibernética em 2020, enquanto o Brasil apenas 6 milhões. Seria necessário ao menos 60 milhões para modernizar o setor no Brasil (TCU, 2020). A título de comparação, o Livro Branco de 2012 (BRASIL, 2012a) previa gastos de cerca de 839 milhões de reais na área até 2031, o que hoje em dia parece um horizonte distante. O gráfico a seguir reforça esta impressão e demonstra os gastos do exército brasileiro com o programa estratégico defesa cibernética entre 2012 e 2018:

Figura 13 - Despesas planejadas e autorizadas para o programa estratégico defesa cibernético entre 2012 e 2018



Fonte: BRASIL, 2018a

A análise deste gráfico traz outra questão: o desafio da perspectiva orçamentária. Como é possível perceber na grande maioria dos anos, o exército recebeu menos capital do que esperava (BRASIL, 2018a). Como não é possível seguir o calendário de desenvolvimento do projeto com menos capital, o exército decidiu prorrogar a finalização do programa defesa cibernética para 2023, além de tentar realizar corte de custos (BRASIL, 2018a).

A geração de capacidades parte da premissa que o orçamento de defesa deve ser estável e contínuo (BRASIL, 2018a), o que possibilita investimento de médio e longo prazo. São principalmente os investimentos de longo prazo que possibilitaram ao país desenhar estratégias sólidas. Aliado a investimentos constantes, a dependência tecnológica do país e a debilidades de recursos humanos poderia ser superada.

A própria inconstância de investimentos configura um problema comum que precisa ser combatido (BRASIL, 2020c). A inconstância vista a partir de 2015 pode parcialmente ser explicada pela crise econômica vivida no país (informação verbal)[26]. Em momentos de contração econômica o investimento tecnológico estatal tende a ser diminuído, favorecendo demandas teoricamente mais urgentes, como saúde e educação. O próprio exército reconhece este desafio: “Manter a bom termo o andamento do Programa Defesa Cibernética, a despeito do cenário econômico desfavorável e das restrições financeiras” (BRASIL, 2018a, p.91). Além

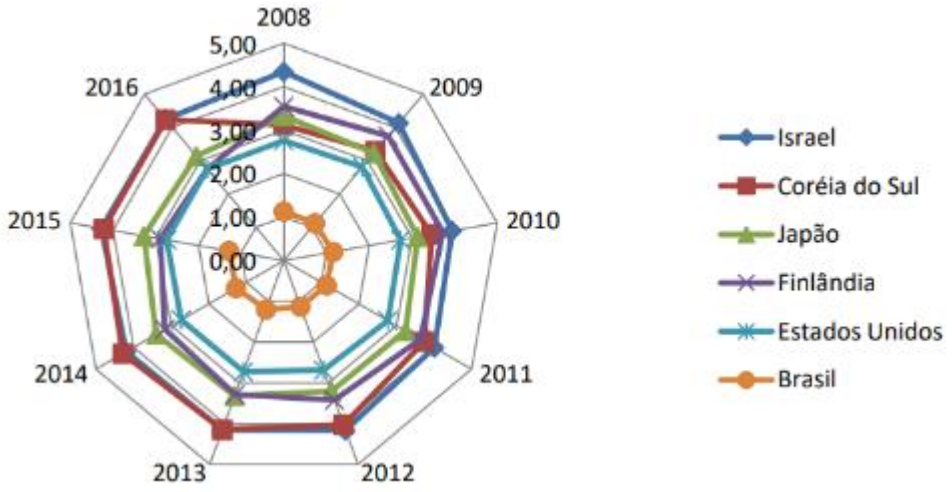
[26] Fala da profª Danielle Jacon Ayres Pinto na disciplina de Relações Internacionais e Tecnologia, UFSC, em 19 mai. 2021

disso, é necessário lembrar que o repasse ao ministério da defesa é feito pelo poder legislativo. Logo, movimentos políticos podem favorecer ou prejudicar o setor.

4.2.2 Tecnologias: P&D

Outra variável chave a ser analisada é a questão tecnológica. Isto é, observar a pesquisa e desenvolvimento tecnológico (P&D) do país na área e suas possíveis dependências tecnológicas. Em primeiro lugar, é possível comparar os gastos em P&D do Brasil com outros países:

Figura 14 - Brasil e os países que mais investem (em porcentagem do PIB), 2008-2016



Fonte: FONSECA, 2018

O gráfico acima demonstra que o Brasil investe bem menos em P&D que outros países da Organização para Cooperação e Desenvolvimento Econômico (OCDE). Os países do gráfico acima são aqueles que estão mais próximos ao estado da arte em matéria tecnológica do mundo. Portanto, compará-los ao Brasil demonstraria a distância do país com seus concorrentes mais eficientes (e que dominam a fronteira tecnológica). O investimento brasileiro chega a ser metade do investimento do penúltimo colocado da lista, demonstrando a distância do país da fronteira tecnológica mundial (FONSECA, 2018).

O número de publicações expressivas brasileiras no tema está crescendo, mas ainda se encontram em um patamar insuficiente (ARANHA; BARCELOS, 2018). A própria falta de infraestrutura adequada a pesquisa acaba sendo um limitante da produção acadêmica

(ARANHA; BARCELOS, 2018). Além disso, a pesquisa sobre o tema da cibernética em território nacional não é geograficamente bem distribuída. (ARANHA; BARCELOS, 2018). Não se pode também pensar que há consonância entre os projetos de estudo entre universidades públicas e privadas (BRASIL, 2020f). Seria primordial encabeçar um esforço para que as pesquisas conversassem mais claramente entre si.

Mesmo nos melhores centros de pesquisa do país, pouca inovação aplicável ao setor é gerada. Ainda falando sobre inovação, a E-ciber afirma que:

> É preciso que o País disponha de uma indústria de segurança cibernética inovadora, apoiada por pesquisas e por produções científicas de alto nível, capaz de reter talentos que possam contribuir com a indústria (BRASIL, 2020f, p.26).

Um índice usado para medir quão inovador e competitivo é um país é o ranking do World Competitiveness Yearbook. Em 2010, o Brasil se encontrava na 38ª posição de 63 posições (IMD, 2010), enquanto em 2022 apenas na 59ª (IMD, 2022). Esta queda considerável de posições reforça que, ao invés de ser cada vez mais inovador, o país faz o caminho contrário. A própria economia nacional deveria ser impulsionada pela inovação e digitalização crescente, o que geraria dinamismo econômico e mais conhecimento (BRASIL, 2018f).

Partindo do pressuposto que o Brasil não é um país inovador em tecnologias e não tem índices elevados de pesquisa e desenvolvimento, é razoável supor que o país é importador de tecnologias. A PND (BRASIL, 2020c) desenvolve esta ideia:

> propósito de alcançar e consolidar a capacidade de desenvolver e fabricar produtos de defesa, minimizando-se a dependência da importação de componentes críticos, de produtos e de serviços, incentivando a aquisição e a transferência de tecnologias (BRASIL, 2020c, p.42).

Não se pode, porém, pensar que qualquer tecnologia é passível de importação. Como setor estratégico, tecnologias relacionadas à defesa nacional são vitimizadas frequentemente por barreiras comerciais (POTT; RAMOS, 2016). Ou seja, países centrais (e exportadores de tecnologias) impõem entraves propositais para a exportação de certas tecnologias, visando o monopólio de seu uso. Tal monopólio pode se transformar em vantagem militar em momento de combate, por exemplo. Portanto, é urgente que o Brasil produza tais tecnologias internamente e não dependa de sua importação.

O assunto da dependência tecnológica é tratado pelo documento Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica (BRASIL, 2020e). O documento cita claramente a necessidade do país de reduzir sua dependência tecnológica, o que seria vital para garantir o poder militar nacional (BRASIL, 2020e). Uma medida mitigadora seria justamente o aumento de investimento em pesquisa e desenvolvimento, além da aquisição

de recursos e softwares (BRASIL, 2020e). Ainda sobre a questão da dependência tecnológica e as vulnerabilidades por elas causadas, Fernandes (2015a) afirma que estes são obstáculos tão sérios que impedem que o Brasil se torne soberano ciberneticamente.

4.2.3 Recursos Humanos

Outra variável central seriam os recursos humanos. Provavelmente, o principal gargalo deste setor é a falta de profissionais qualificados (BRASIL, 2018f). Essa carência ocorre tanto no setor público quanto no privado. É comum, por exemplo, que empresas privadas treinem seus funcionários internamente (OEA, 2020). A procura por profissionais da área é grande (OEA, 2020) e a quantidade de profissionais formados não é suficiente para abastecer o setor (BRASIL, 2020f).

O governo brasileiro ciente desta problemática, criou a escola de Defesa Cibernética (ENaDCiber) na tentativa de gerar recursos humanos especializados na área de defesa cibernética. Porém, autores como Canongia e Mandarino Jr (2011) acreditam que iniciativas deste tipo só seriam realmente efetivas se a educação e capacitação de recursos humanos ocorressem desde a educação básica. Isso ocorre porque a deficiência de alfabetização digital é um problema generalizado no país (BRASIL, 2020f). Assim, o governo brasileiro poderia manter estratégias pontuais como a ENaDciber, mas também desenvolver estratégias específicas para outros níveis de ensino. Esta seria uma forma de resolver a difícil situação na qual o país se encontra: falta do uso seguro da internet, de profissionais formados no setor e poucos programas educacionais na área (BRASIL, 2020f).

Outra maneira de contornar tal deficiência formativa (ao menos no nível superior) seria através do uso de simuladores, como o Simulador Nacional de operações cibernéticas (SILVA *et al.*, 2018). Desenhado especificamente para uso estratégico brasileiro, o SIMOC (Simulador de Operações de Guerra Cibernética) possibilita que:

> além de serem bem mais baratos do que fazer um treinamento, os jogos e simuladores disponibilizam a opção de os participantes/alunos fazerem várias vezes a mesma "fase", melhorando suas capacidades e forçando a não memorização, e sim o aprendizado, além de poderem testar novos meios de resolução de problemas, sendo mais flexível (SILVA, 2018, p.5).

É falacioso pensar que, mesmo com as estratégias do uso de simuladores e criação da ENaDciber, o nível de formação no nível superior é adequado:

> ainda é muito incipiente o desenvolvimento de [...] cursos em universidades que possibilitam uma mão-de-obra nacional capacitada e especializada para atuar nessa área e poucas são as empresas capacitadas para lidar com a segurança cibernética (WANDERLEY, 2019, p.14).

Por fim, vale lembrar que a falta de mão de obra ocorre também em países desenvolvidos (BRASIL, 2018f), dada às mudanças contínuas ocasionadas pela internet. Os países mais ricos, porém, podem se beneficiar de uma vantagem: atração de mão de obra externa. Ou seja, parte de sua demanda é suprimida pela imigração de mão de obra altamente qualificada, muitas vezes oriunda de países em desenvolvimento. Desta forma, os países em desenvolvimento sofrem uma pressão permanente de emigração de sua escassa mão de obra qualificada. Portanto a manutenção de mão de obra qualificada é necessária (BRASIL, 2020e), e sem ela é impossível operar os sistemas e as infraestruturas (FARIAS; FERRAZ, 2018).

4.2.4 Sistemas de Defesa

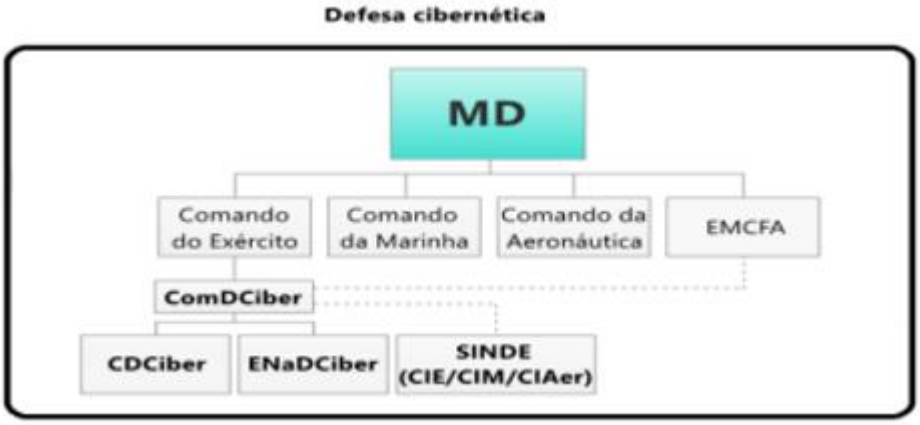
Nesta seção serão analisados o órgão CDCiber (Centro de Defesa Cibernética) e outros sistemas de defesa cibernética brasileiros, como Sistema Integrado de Monitoramento de Fronteira (SISFRON) e o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC).

4.2.4.1 - CDCiber

O CDCiber (Centro de Defesa Cibernética do Brasil) é o principal órgão de defesa cibernética da nação. O CDCiber foi criado em 2010 e vinculado ao exército, com a crescente necessidade de se defender de ataques cibernéticos, que ficavam cada vez mais frequentes (COSTA, 2019). O CDCiber é o principal órgão do Comando de Defesa Cibernético (ComDCiber)[27]:

[27] Como dito no subcapítulo 3.2.3, o ComDCiber é vinculado ao SMDC, a partir da criação do último em 2020 (BRASIL, 2020d)

Figura 15 - Divisões de Defesa cibernética do Ministério da Defesa



Fonte: TCU, 2020

O CDCiber tem como funções:

> Desenvolvimento de capacidades reais para guerra cibernética (comando e controle, armas, vigilância), segurança cibernética, defesa cibernética e de forma geral para atuação em situações de crise, bem como atuação em situações de conflito armados (FERNANDES, 2015b, p546).

O CDCiber é um instrumento que agregaria poder de combate em operações militares, e tem três capacidades operativas: o ataque cibernético, a exploração cibernética e a proteção cibernética (COSTA, 2019). O CDCiber poderia também:

> atuar [...] no sentido de obter informações, identificar lideranças digitais, identificar perfis falsos, levantar e analisar vínculos, realizar campanhas de informação e também atuar sobre a informação para manipular o que destruir, atuar sobre a infraestrutura, etc. (COSTA, 2019, p. 83)

Ainda segundo Costa (2019): o CDCiber: "é uma força de emprego estratégica. Ou seja, uma força de emprego estratégico empregada por módulos. O CDCiber nunca será empregado como um todo como as brigadas." (p.77). O centro é também colaborativo, ajudando em ações da marinha e aeronáutica e não apenas do exército (COSTA, 2019).

Tendo em vista os mega eventos ocorridos no Brasil em 2012 (Rio+20), 2014 (Copa do Mundo) e 2016 (Olimpíadas), o governo se preocupou em fortalecer a defesa cibernética brasileira. Portanto, o governo injetou recursos no CDCiber. Ainda em 2012, por ocasião da

conferência Rio +20, o CDCiber se deslocou ao Rio de Janeiro e passou a ser composto por 110 pessoas, frente a 24 no ano anterior[28] (COSTA, 2019).

Podemos dizer que o órgão foi eficiente em combater as ameaças cibernéticas ocorridas no evento (ABDALLA FILHO *et al.*, 2019; CAMELO; CARNEIRO, 2014). De qualquer forma, vale destacar que durante os eventos, o Centro de Defesa Cibernética teve posição apenas ofensiva (FERNANDES, 2015b).

Voltando à análise da figura 13, é possível relacionar a queda dos investimentos em defesa cibernética com outros motivos, e não apenas com a crise econômica a partir de 2015. Outra justificativa plausível para a queda do investimento é uma possível visão de curto prazo por parte do governo brasileiro. Ou seja, após a realização dos megaeventos, o CDCiber deixou de ser tão relevante na agenda política de defesa do país. Logo, os investimentos direcionados ao CDCiber deixaram de ocorrer com o mesmo volume. Novamente, esse viés de investimento de curto prazo se choca com a importância dos investimentos de longo prazo necessários para vencer as vulnerabilidades do setor cibernético brasileiro.

4.2.4.2 - Outros sistemas

O sistema integrado de monitoramento de fronteira (SISFRON) apareceu pela primeira vez na END de 2008 (BRASIL, 2008). O sistema foi idealizado para combater os crimes transnacionais e o narcotráfico nas fronteiras do país (IPEA, 2019). A enorme dimensão da fronteira brasileira é um multiplicador de riscos neste cenário, sendo complexo guarnecê-la de maneira adequada (IPEA, 2019). De forma geral, o SISFRON é um projeto ousado e promete ser "o maior sistema de monitoramento de fronteiras do planeta" (IPEA, 2019, p. 18) aumentando a capacidade de dissuasão do país (IPEA, 2019).

O SISFRON tem como propósito: "fortalecer a presença e a capacidade de monitoramento e de ação do Estado na faixa de fronteira terrestre, potencializando a atuação dos entes governamentais com responsabilidades sobre a área (EPEX, 2019)". Sua instalação será gradual, dividida em três fases. O projeto piloto (primeira fase) está em fase de implementação, na região fronteiriça do Mato Grosso do Sul, área com grande presença de narcotraficantes (IPEA, 2019). Na segunda fase, o sistema será expandido para toda a região

[28] Não foi encontrada nenhuma outra fonte que indique o número de funcionários do CDCiber atualmente ou sua variação durante os anos.

fronteiriça com Bolívia e Paraguai e só então para toda a área fronteiriça do território nacional (IPEA, 2019).

O SISFRON se relaciona também com o espaço cibernético:

> um sistema de Comando e Controle, Comunicações, Computação, Inteligência, Vigilância e Reconhecimento (C4IVR) que visa dotar a Força Terrestre de meios habilitadores a uma presença efetiva na faixa de fronteira brasileira (BUFOLO, 2014, p. 23).

Entre seus métodos de monitoramento, destacam-se:

> sensores óticos e optrônicos, radares de vigilância terrestre (RVT), sistemas de vigilância, monitoramento e reconhecimento (SVMR), sistemas de comunicação tática e centros de comando e controle (CC2) [...] garantir os meios necessários à segurança das informações e comunicações, à defesa cibernética (IPEA, 2019, p. 22)

O SISFRON teria custo de cerca de 12 bilhões de reais, e sua implementação se daria entre 2013 e 2023 (IPEA, 2019). Porém, como muitos outros projetos, o SISFRON sofreu com cortes orçamentários. A conclusão do projeto já foi adiada para 2035 (MONTEIRO, 2015). Caso a restrição de orçamento continue a ocorrer, ele poderia ser concluído apenas em 2065, o que inviabilizaria o projeto (MONTEIRO, 2015).

Um fator que se deve destacar no projeto é o percentual de 75% de conteúdo nacional. Ou seja, 75% de todos os bens utilizados no projeto (sensores, radares e softwares) devem ser nacionais (IPEA, 2019). Assim, espera-se que o projeto possa induzir a indústria de tecnologia nacional, gerando empregos na área e gerando desenvolvimento (IPEA, 2019). Esta seria também uma forma de diminuir a dependência tecnológica do país.

O SISFRON teria também algum papel social, passando informações para governos locais no combate a crimes transnacionais e tráfico de drogas (IPEA, 2019). Além disso, o sistema pode funcionar em favor da cooperação do Brasil com os vizinhos, cooperando no combate ao tráfico de drogas. Portanto, o SISFRON não deve ser pensado apenas como um instrumento de defesa da nação (IPEA, 2019), já que permite a conexão do exército com outros órgãos públicos.

Além do SISFRON, na tentativa de minimizar a dependência tecnológica brasileira, foi lançado o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), já em atividade. O satélite é integralmente controlado pelo Brasil (Ministério da Defesa e Telebrás) (IPEA, 2019). Desta forma, o país não ficaria dependente de satélites estrangeiros para circular

sua própria informação. Em um momento de combate, essa comunicação poderia ser cortada pelo país inimigo[29].

A tecnologia utilizada no SGDC advém da *joint venture* entre Embraer e Telebrás (Telecomunicações Brasileiras S. A.), e a construção foi feita por empresas internacionais (IPEA,2019). Além de se conectar com o SISFRON, outra de suas funções seria estender áreas onde não há infraestrutura de internet por banda larga (BRASIL, 2018f).

Por fim, podemos citar o supercomputador Santos Dumont, do laboratório nacional de computação científica (LNCC) (BRASIL, 2018f). Infelizmente, infraestruturas como o referido supercomputador são escassas no país, e 60% da infraestrutura dos centros de pesquisa não passa dos 500 mil reais (BRASIL, 2018f).

4.2.5 Considerações sobre as capacidades cibernéticas ofensivas do país

Finalmente, devemos fazer considerações sobre as capacidades cibernéticas ofensivas do Brasil. Segundo Gonzales e Portela (2018) não há disputa de poder cibernético na América do Sul. De qualquer forma, este pensamento não pode levar a crer que os vizinhos do Brasil sejam incapazes de lançar ofensivas contra o país (IZYCKI, 2018). Izycki (2018) aponta que é primordial que o Brasil não desenvolva apenas capacidades cibernéticas defensivas, mas também ofensivas. A capacidade dissuasória real dependerá tanto de capacidades de ataque quanto de defesa (IZYCKI, 2018).

Voltando a análise dos quadros de poder de Nye do segundo capítulo, é possível identificar em quais casos o país poderia lançar mão de capacidades ofensivas. Três dos resultados do quadro 2 (implicações do poder cibernético na forma hard) se configuram como "ataques". Desta forma, seria necessário que as capacidades ofensivas também fossem explicativas para se mensurar a capacidade cibernética brasileira.

Porém, analisar a capacidade cibernética ofensiva do Estado brasileiro é mais complexo. O primeiro motivo é que há sistemas voltados somente para a defesa nacional, como o SISFRON. O segundo é que a análise pregressa da atuação do CDCiber foi basicamente focada em capacidades defensivas, e com poucas menções aos ataques perpetrados pelo órgão

[29] Não necessariamente são os próprios estados estrangeiros que operam seus satélites. É muito comum que empresas privadas estrangeiras administrem satélites. De qualquer forma, o corte de comunicações também poderia ocorrer nestes casos.

(FERNANDES, 2015b). Em terceiro lugar, é difícil precisar especificamente as capacidades ofensivas de destacamento de guerra cibernética das três forças (exército, marinha e aeronáutica) e do próprio CDCiber. Caso houvesse fontes que precisassem melhor as capacidades de ataques do Brasil, seria interessante que essa variável se juntasse às outras deste subcapítulo.

Contudo, também há autores que marginalizam a centralidade dada a ataques cibernéticos lançados por Estados Nacionais. Rid (2013) afirma que: "Ataques cibernéticos podem certamente trazer informações de inteligência valiosas. Mas do ponto de vista político, sua utilidade é questionável" (RID, 2013, p.173, *tradução nossa*)[30]. Ao longo de seu livro, Rid (2013) vai demonstrando que, por afetar majoritariamente sistemas e softwares (e não pessoas), os ataques cibernéticos costumam ser instrumentos políticos limitados. De alguma forma, a violência perde relevância quando não é direcionada a humanos (RID, 2013). Para corroborar com sua visão, o autor se utiliza do caso Stuxnet. O ataque (de autoria desconhecida) tinha como objetivo "minar a habilidade do governo iraniano de desenvolver armas nucleares" (RID, 2013, p. 172, *tradução nossa*)[31]. O ataque conseguiu atrasar o programa nuclear iraniano, mas não o impediu (RID, 2013).

4.3 O BRASIL PODE EXERCER SEU PODER GLOBALMENTE?

Para analisar se o Brasil tem capacidade de exercer seu poder globalmente, devemos voltar a análise das variáveis elencadas neste capítulo: o capital investido, potencial de recursos humanos, P&D e os sistemas de defesa. Podemos condensar os resultados na tabela abaixo:

Quadro 8 - Análise das variáveis essenciais para o poder cibernético

	Investimento	**P&D**	**Recursos Humanos**	**Sistemas de Defesa**
Adequado(s)?	Não	Não	Não	Não

Fonte: Elaboração própria

[30] No original: "Cyber attacks could yield very valuable intelligence, no doubt. But from a political vantage point their coercive utility is far more questionable"

[31] No original: undermine the Iranian government's trust in its ability to develop a nuclear weapon

Como é possível identificar, nenhuma das variáveis acima se mostrou adequada. Logo, podemos entender que as vulnerabilidades atestadas pelos documentos diagnósticos ainda não foram superadas.

Não é difícil perceber a importância destas quatro variáveis no desenvolvimento de capacidades cibernéticas e no próprio poder cibernético. Lyu (2019) por exemplo, chama a atenção para a necessidade do desenvolvimento tecnológico e aptidões de inovação do país. Batista (2016) afirma que: "A questão de investimento orçamentário e de pessoal também são abundantes, levando a crer que essas são as possíveis motrizes para o desenvolvimento da estrutura cibernética em si" (p. 101), o que converge com a visão de Oliveira e Portela (2017). A PND, por sua vez, afirma que: "A Expressão Militar do Poder Nacional está intimamente associada ao grau de independência tecnológica e logística do País" (BRASIL, 2020c, p.39).

Provavelmente, entre as variáveis elencadas neste capítulo (investimento, P&D, recursos humanos e sistemas de defesa) a mais relevante seja o investimento. Caso o país apresentasse bons níveis de investimento no setor cibernético, seria natural que o investimento fosse canalizado para as vulnerabilidades do país em matéria de P&D, recursos humanos e sistemas de defesa.

Ainda sobre o capital investido, é simples perceber que o Brasil investe muito menos na área do que deveria (FONSECA, 2018; MACHADO, 2017; TCU, 2020). A mesma conclusão é perceptível ao se comparar o investimento brasileiro com o da Espanha ou o dos EUA. Essa falta de capital disponível ampliou o prazo de implantação de sistemas de defesa como o SISFRON (MONTEIRO, 2015) e o projeto de defesa cibernética (BRASIL, 2018a). A diferença entre o orçamento autorizado e o planejado é visível na figura 13 em todos os anos, mas atinge seu maior índice no ano de 2015 (BRASIL, 2018a). Como já dito anteriormente, seriam necessários cerca de 60 milhões para modernizar o setor cibernético, (TCU, 2020) levando a crer que o país possua tecnologias defasadas.

O nível de P&D no Brasil sobre o tema também é baixo. Além de não haver infraestrutura adequada para as pesquisas, é produzida pouca inovação (ARANHA; BARCELOS, 2018). A E-ciber (BRASIL, 2020f) também informa que não há linha de continuidade entre pesquisa de instituições públicas e privadas. O país também vem caindo no índice de inovação em praticamente todos os anos desde 2010 (IMD, 2022). Nestas condições não resta ao país outra saída que não seja a importação de tecnologias, se tornando tecnologicamente dependente de nações centrais.

Não muito diferente é o cenário brasileiro no quesito de recursos humanos. Há déficit de profissionais formados na área (BRASIL, 2018f) e atração da escassa mão de obra qualificada brasileira aos países centrais. Estratégias como a ENaDCiber, uso de simuladores (SILVA *et al.*, 2018) e os cursos técnicos e de graduação não são suficientes para suprir a demanda doméstica.

Sobre os sistemas de defesa nacionais, podemos citar como os principais o CDCiber e o SISFRON. Embora o CDCiber tenha sido eficiente no combate às ameaças presentes nos megaeventos (ABDALLA FILHO *et al.*, 2019; CAMELO; CARNEIRO, 2014), é provável que o cenário de baixo investimento que o setor vive atualmente comprometa suas capacidades no presente. Ao mesmo tempo, um exemplo categórico de falta de investimento no setor de defesa cibernético é o SISFRON. Com um volume de recursos muito menor que o esperado, o projeto corre o risco real de ser impossível na prática (MONTEIRO, 2015).

De qualquer forma, é difícil imaginar que um país que não invista adequadamente em seu setor cibernético e em P&D; não disponha de mão de obra qualificada e não tenha sistemas de defesa robustos esteja tratando de minimizar suas vulnerabilidades. Com tantas debilidades ainda latentes, é difícil imaginar que o Brasil possa exercer seu poder cibernético globalmente.

Adensando a discussão sobre as capacidades dos Estado, Tilly (2007) diz que:

> A capacidade do estado significa até que ponto as intervenções de agentes estatais em recursos, atividades e interconexões pessoais não estatais alteram a distribuição de tais recursos, atividades e conexões interpessoais, assim como as relações destas distribuições. (TILLY, 2007, p.16, *tradução nossa*)[32]

Deste modo, esperar-se-ia que, com o mapeamento das vulnerabilidades pelos documentos diagnósticos, o Estado Brasileiro tivesse condições de alterar a distribuição de recursos, diminuindo suas debilidades. Como demonstrou este capítulo, isto não ocorre, e a partir de Tilly (2007) podemos entender que o Brasil é um país de baixas capacidades.

Assim, seria impossível alcançar as definições de poder de Nye Jr (2010) e consequentemente a criação de recursos materiais e imateriais (FARIAS; FERRAZ, 2018), tão relevantes ao país. Como já visto a partir de Nye Jr (2010) o poder cibernético pode ser exercido dentro ou fora do ciberespaço, na forma hard ou soft. O poder pode também ter três faces, como já comentado. Porém, dada as debilidades brasileiras, é difícil acreditar que qualquer forma e

[32] No original: "State capacity means the extent to which interventions of state agents in existing non-state resources, activities, and interpersonal connections alter existing distributions of those resources, activities, and interpersonal connections as well as relations among those distributions."

face do poder cibernético seja possível ao país, já que as suas capacidades cibernéticas não são desenvolvidas.

Caso houvesse uma disputa de poder no espaço cibernético entre o Brasil e seus vizinhos, poderia haver maior interesse do Brasil em desenvolver as variáveis supracitadas. Mas como não há uma disputa clara no domínio cibernético entre as nações sul-americanas (GONZALES; PORTELA, 2018), isso não ocorre. Para estes autores, as políticas em matéria de cibernética dos países Sul Americanos são geralmente voltadas para questões nacionais e não para o enfrentamento com os vizinhos.

5 CONCLUSÃO

Em primeiro lugar, vimos a revolução tecnológica e informacional em consequência da internet. A partir daí, surgiram vários conceitos, tão importantes para o setor. Conceitos que não necessariamente são consensuais na literatura. Dos conceitos mais relevantes, temos a diferenciação entre segurança e defesa cibernética. Outro conceito de suma importância é o poder cibernético, que pode ocorrer na forma hard ou soft, e pode ter implicações dentro e fora do espaço cibernético. Foi visto também as três faces do poder cibernético e suas peculiaridades. Por fim foram destacados os atores que atuam no espaço cibernético além suas vantagens e vulnerabilidades.

No terceiro capítulo foi mostrado o mapeamento dos documentos sobre cibernética no Brasil. A partir daí, foram analisados a maioria dos documentos do período, os dividindo quanto a sua adequação para responder à pergunta de pesquisa. A maioria dos documentos eram vagos e abertos, e não necessariamente específicos do tema da cibernética. Deve-se reiterar que a maioria dos documentos analisados são excessivamente genéricos e padecem de uma estratégia robusta e pragmática de atuação do Brasil no espaço cibernético, visão também compartilhada por De Rê (2021). A minoria dos documentos (os mais completos, da seção 3.4) são documentos eficientes em diagnosticar as vulnerabilidades do país sobre o tema. Mas, por não terem força normativa, não conseguem de fato superar tais vulnerabilidades citadas, e acabam dependendo de vontade política para serem colocados em prática.

Por fim, no capítulo quatro, é feita uma análise das capacidades cibernéticas brasileiras, que foram subdivididas como: capital investido, P&D, recursos humanos e sistemas de defesa. Todas essas variáveis se mostraram inadequadas, levando a crer que o país não está sendo capaz de superar as vulnerabilidades citadas pelos documentos diagnósticos.

Após a leitura integral deste trabalho, conclui-se que a hipótese foi verdadeira. O arcabouço documental criado pelo país entre 2018 e 2020 não foi suficiente para que o país aumentasse qualitativamente seu poder, e consequentemente, sua influência global em termos de capacidades cibernética. Os documentos são em sua maioria vagos, diagnósticos e não vinculativos, o que impossibilita por si só a criação de capacidades. As capacidades cibernéticas existentes não são elevadas, dado que o investimento, P&D, recursos humanos e sistemas de defesas são inadequados, o que dificulta a utilização do poder cibernético por parte do país.

Com capacidades reduzidas, é ainda mais urgente um arcabouço legislativo que garanta a criação de capacidades e acabe reduzindo as debilidades do Brasil. Uma saída para tal questão seria transformar os documentos em matéria de lei, que designasse precisamente a quantia de recursos para superar cada vulnerabilidade. Assim, os documentos deveriam ser obrigatoriamente colocados em prática. Portanto, em nenhum momento pode-se perder de vista a importância da produção documental, tão relevante para formular estratégias e diagnosticar debilidades do país. Uma produção documental de qualidade poderia determinar a inserção do país no espaço cibernético e possibilitar a utilização de seu poder cibernético.

Esta conclusão se aproxima de trabalhos como o de Santos Jr (2019), quando reitera a necessidade de um arcabouço documental preciso e pragmático. Fica também registrado este grande desafio: "O Brasil precisa formular uma estratégia nacional abrangente para defesa e segurança cibernética, bem como planos de mobilização para os diferentes níveis e esferas de governo" (BRASIL, 2018f, p.42). Só assim seria possível entender como o Brasil trabalharia a cibernética como fonte de poder efetivo.

Outra questão fundamental é a ausência do documento "E-defesa" já citado como necessário no ano de 2018 pela PNSI (BRASIL, 2018b). Enquanto a segurança cibernética no país já tem sua própria estratégia nacional, a E-ciber (BRASIL, 2020f), o mesmo não ocorre com a defesa cibernética. Este poderia ser um indício de certa prevalência da agenda de segurança cibernética em detrimento da de defesa cibernética. Outro fator que reforça tal pensamento é a E-digital (BRASIL, 2018f) e ENSIC (BRASIL, 2020a), também focados em segurança cibernética. Vale lembrar que a questão das infraestruturas críticas pode fazer referência tanto à segurança como à defesa. Mas como demonstra a ENSIC, no Brasil as infraestruturas críticas estão sendo entendidas como atribuição do GSI, o órgão responsável pela segurança cibernética no país.

Mas esta visão de que a defesa cibernética no Brasil é marginalizada não é um consenso. Autores como Diniz, Muggah e Glenny (2014) acreditam que com a injeção de recursos no CDCiber nos anos dos megaeventos, a defesa cibernética no Brasil ficou melhor desenvolvida que a segurança cibernética:

> Embora as ameaças principais ao ciberespaço nacional estejam provavelmente ligadas ao crime econômico e deverão resultar em iguais aumentos na alocação de recursos para a segurança pública, as forças armadas vem recebendo a maior parcela de apoio. Por exemplo, além dos custos de seu lançamento, o CDCiber recebeu US$ 60 milhões em 2012 e receberá mais US$ 200 milhões no decorrer de 2015. (DINIZ; MUGGAH; GLENNY, 2014, p.101).

Como já visto na figura 13, essa projeção de recebimento de 200 milhões ao CDCiber em 2015 não foi efetivada (BRASIL, 2018a). Os autores se preocupam que essa possível hipertrofia da defesa cibernética seja nociva a sociedade, caso reduzissem liberdades individuais na utilização do ciberespaço (DINIZ; MUGGAH; GLENNY, 2014). Acreditam também que desta forma, poderia haver certa militarização do espaço cibernético nacional.

Ao contrário dos autores supracitados, este trabalho não acredita que haja uma hipertrofia na defesa cibernética brasileira, se baseando principalmente na quantidade de capital investido na área e as debilidades dos sistemas de defesas brasileiros. É possível que em 2014, as quantidades de capital investido no CDCiber pareceriam constantes nos anos seguintes. Mas como já foi examinado, a disponibilidades de recursos para o órgão caiu com o passar dos anos. Por consequência, parece mais provável que a segurança cibernética esteja melhor desenvolvida que a defesa cibernética no país, e não o contrário.

Outra questão que deve ser tratada é sobre a abrangência dos documentos. Não é porque a maioria dos documentos sejam vagos, que se deve ter a ingenuidade de acreditar que bons documentos seriam aqueles que explicitam as estratégias nos mínimos detalhes. É esperado que a defesa nacional, como área estratégica, tenha algum nível de confidencialidade. Caso contrário, parte das estratégias brasileiras perderiam eficácia, a partir do momento que os alvos de ataques do país já conhecessem o *modus operandi* brasileiro em sua totalidade.

Ainda sobre esta discussão, se poderia levantar a seguinte ressalva: a maioria dos documentos brasileiros são genéricos propositalmente, para que a verdadeira estratégia brasileira não fosse revelada. Como consequência, os "verdadeiros documentos" estratégicos existem, mas são não públicos. Esta visão rompe claramente com o princípio da transparência, tão caro e necessário à democracia. Seguindo essa posição, os documentos "verdadeiros" não estariam à disposição para guiar a nação e o campo político, na tentativa de superar as vulnerabilidades cibernéticas. Logo, a sociedade brasileira e as próprias forças armadas seriam vitimizadas com tal estratégia.

Por último, é notório perceber os alertas dados pelo Livro Verde de segurança cibernética ainda em 2010 (BRASIL, 2010b). Há 12 anos atrás, o documento destacava a necessidade de se encarar a cibernética como grande prioridade para o país, sendo ela uma condição para seu desenvolvimento (BRASIL, 2010b). Infelizmente, a falta de capacidades cibernéticas do país e de documentos robustos demonstram que após mais de uma década, pouco foi feito.

REFERÊNCIAS

ABDALLA FILHO, Eduardo et al. **Defesa Cibernética no Brasil:** Análise da Atuação do Ministério da Defesa na Copa do Mundo de 2014 e nas Olimpíadas de 2016. XVI CADN. Rio de Janeiro. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/defesaa_ciberneticaa_noa_brasila_analisea_daa_atuacaoa_doa_ministerioa_daa_defesaa_naa_copaa_doa_mundoa_dea_2014a_ea_nasa_olimpiadasa_dea_2016.pdf>. Acesso em fevereiro de 2021

AGÊNCIA SENADO. Política Nacional de Defesa é aprovada no Senado e segue para Câmara. **Senado Federal**, 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/06/02/politica-nacional-de-defesa-e-aprovada-no-senado-e-segue-para-camara>. Acesso em 4 de junho de 2022

AGOSTINI, Marcos Tocchetto. **A cibernética sob a ótica do fenômeno da guerra e da agenda de segurança**. TCC (graduação) - Universidade Federal de Santa Catarina. Centro Sócio-Econômico. Relações Internacionais. 2014. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/124695/Monografia%20do%20Marcos%20Tocchetto%20Agostini.pdf?sequence=1&isAllowed=y>. Acesso em janeiro de 2021.

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações**. Brasília, DF. Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO760LFI_pHFdPDvhssf6GcKAE5_GJovBZUfi7_h9SO4EFu4GZ_rtRSkPAMggKV38swnbODIuh_k2ClcCwWdtg0X>. Acesso em junho de 2021.

ARANHA, Diego F; BARCELLOS, Marinho. Research in Security and Privacy in Brazil. **IEEE Security & Privacy**, v. 16, n. 6, p. 14-21, 2018.

AYRES PINTO, Danielle Jacon. Social Medias and Fake News: a new approach on State Security. In: ISA 62th Annual Convention, 2021. **Anais ISA 2021** Annual Convention Globalization, Regionalism and Nationalism: Contending Forces in World Politics. Disponível em: <www.isanet.org>. Acesso em 1 de junho de 2022

AYRES PINTO, Danielle Jacon; MORAES, Isabela. As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit. **Revista de Estudios Sociales**, n. 74, p. 71-82, 2020.

BACHRACH, Peter; BARATZ Morton. Decisions and Nondecisions: An Analytical Framework. **American Political Science Review**. September 1963, 632-42.

BATISTA, Ana Laíse Ferreira Herculano. **Segurança cibernética:** uma abordagem comparativa das estruturas de defesa cibernética norte-americana e brasileira. ECEME, Rio de Janeiro, 2016.

BIMBER, Bruce. 1998. “The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism”. **Palgrave Macmillan Journals** 31 (1): 133-160.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, 1988 Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 25 de jun. 2022.

_____. Decreto n° 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. 2018c. **Decreto no 9.573**. Brasília, DF: Diário Oficial [da] União de 23 de novembro de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em: 7 de abril de 2021.

_____. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. 2018b. **Decreto no 9.637**. Brasília, DF. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938#:~:text=1%C2%BA%20Fica%20institu%C3%ADda%20a%20Pol%C3%ADtica,da%20informa%C3%A7%C3%A3o%20a%20n%C3%ADvel%20nacional>. Acesso em 07 de abril de 2021.

_____. Decreto n° 10.222 de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. 2020f. **Decreto N 10.222. Brasília**, DF: Diário Oficial da União de 6 de fevereiro de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 7 de abril de 2021.

_____. Decreto n° 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. 2020a. **Decreto no 10.569**. Brasília, DF: Diário Oficial da União de 10 de dezembro de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm>. Acesso em 07 de abril de 2021.

_____. Decreto legislativo Nº 179, de 2018. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem (CN) nº 2 de 2017 (Mensagem nº 616, de 18 de novembro de 2016, na origem). 2018g. **Decreto Legislativo Nº 1**79. Brasília, DF: Diário Oficial da União, 17 dez. 2018. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=4&data=17/12/2018>. Acesso em 22 de junho de 2022.

_____. **E-Digital - Estratégia Brasileira para a Transformação Digital**. Brasília, DF, 2018f. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em maio de 2021

_____. **Cibernética da Administração Pública Federal**. Brasília, DF, 2015. Disponível em: <https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf>. Acesso em janeiro de 2021.

_____. **Estratégia Nacional de Ciência Tecnologia e Inovação (2016-2022)**. Brasília, DF, 2018e. Disponível em: <https://antigo.mctic.gov.br/mctic/opencms/ciencia/SEPED/Publicacoes/ENCTI/PlanosDeAcao.html>. Acesso em maio de 2021

_____. **Estratégia Nacional de Defesa**. Brasília, DF, 2008

_____. Lei complementar no 136 de 25 de agosto de 2010. Altera a Lei Complementar nº 97, de 9 de junho de 1999, que "dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas", para criar o Estado-Maior Conjunto das Forças Armadas e disciplinar as atribuições do Ministro de Estado da Defesa. 2010a. **Lei complementar 136.** Brasília, DF: Diário Oficial da União, 26 de ago. de 2010.Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp136.htm>

_____. Lei Nº12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014b. **Lei Nº12.965**. Brasília, DF: Diário Oficial da União, 24 abr. de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 7 de abril de 2021.

_____. Lei n 13.709, de 14 de agosto de 2018. Lei geral de proteção de dados (LGPD). 2018d. **Lei no 13.709**. Brasília, DF:Diário Oficial da União, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em maio de 2021

_____. **Livro Branco de defesa nacional**. Brasília, DF, 2012a

_____. **Livro Branco de defesa nacional**. Brasília, DF, 2020b

_____. **Livro verde segurança cibernética no Brasil**. Brasília, DF, 2010. 2010b. Disponível em: <https://redectidc.com.br/assets/files/2010%20-%20Livro%20Verde%20-%20Seguran%C3%A7a%20Cibern%C3%A9tica%20no%20Brasil.pdf>. Acesso em janeiro de 2021.

_____. **Norma complementar 04/IN01/DSIC/GSI/PR**. 2013. Brasília, DF. Disponível em: <https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-04IN01DSICGSIPR.pdf>; Acesso em 1 de maio de 2022.

_____. **Planejamento estratégico setorial - 2020-2031**. Brasília, DF, 2019b. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/lai/institucional/diagra_planejamentoa_estrategicoa_17a_04a_2020.pdf>. Acesso em maio de 2021

_____. **Política Nacional de defesa Nacional e Estratégia Nacional de Defesa**. Brasília, DF, 2012b

_____. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF, 2016

_____. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF, 2020c

_____. Portaria No 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação. 2019a. **Portaria no 93**. Brasília, DF. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em maio de 2021

_____. Portaria No 3.781/GM-MD, de 17 de novembro de 2020. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. 2020d. **Portaria no 3.781**. Brasília, DF: Di[ario Oficial da UNião, 19 nov. de 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860>. Acesso em 8 de abril de 2021

_____. Portaria Normativa GSIPR No45 de 8 de agosto de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. 2009. **Portaria Normativa GSIPR N45**. Brasília, DF. Disponível em: <https://www.legisweb.com.br/legislacao/?id=213726>. Acesso em 2 de jun. de 2022.

_____. Portaria Normativa No 9/GAP/MD, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas –MD35-G-01 (5a Edição/2015). 2015. **Portaria Normativa no 9/GAP/MD**. Brasília, DF: Diário Oficial da União, 21 jan. 2016. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf>. Acesso em maio de 2021

_____. Portaria Normativa No 69/GM-MD, de 27 de julho de 2020. Aprova as Diretrizes para a Consecução das Ações Setoriais de Defesa voltadas para a Guerra Eletrônica - MD32-D-01 (1a Edição/2020). 2020d. **Portaria normativa No69/GM-MD**. Brasília, DF. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-normativa-n-69/gm-md-de-27-de-julho-de-2020-269395498>. Acesso em maio de 2021

_____. Portaria Normativa No 196/EMD/MD de 22 de fevereiro de 2007. Aprova o Glossário das Forças Armadas- MD35-G-01 4ª Edição/2007. 2007 . **Portaria Normativa N 196/EMD/MD**. Brasília, DF.

_____. Portaria Normativa No 3010, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. 2014a. **Portaria Normativa no 3.010/Md**. Brasília, DF: Diário Oficial da União, 19 nov. v. 224. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 23 fev. 2021.

_____. Transformação do Projeto Estratégico do Exército de Defesa Cibernética (PEE Def CIBER) em Programa Estratégico do Exército Defesa Cibernética (Prg EE Def Ciber). In: **Relatório de gestão do exércitobrasileiro do exercício de 2018**. Brasília, DF, 2018a. p. 84-91. Disponível em: <http://www.cciex.eb.mil.br/images/pca/2018/cmdopca2018.pdf>. Acesso em maio de 2021.

BUFOLO, R. **O SISFRON e o papel do Exército nas operações em ambiente interagências**. Rio de Janeiro: ECEME, 2014.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, n. 29, p. 21-46, 2010.

CAMELO, J. R. S.; CARNEIRO, J. M. E. A atuação do Centro de Defesa Cibernética na Copa das Confederações Fifa 2013. In: FERREIRA NETO, Walfredo B. GONZALES, Selma L. D. M. MEDEIROS FILHO, Oscar. **Segurança e defesa cibernética da fronteira física aos muros virtuais**. Acesso em janeiro de 2021

CARNEIRO, Marcelino Haddad Aquino. **Os elementos de apoio ao combate Comunicações, Guerra, Eletrônica e Cibernética na composição da Força Terrestre Componente**: uma proposta de estrutura organizacional. 2016. 44 f. TCCP (Especialização em Ciências Militares) - ECEME, Rio de Janeiro, 2016.

CASTRO, Maria Carolina. **As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações**. TCC (graduação) - Universidade Federal de Santa Catarina. Centro Sócio-Econômico. Relações Internacionais. 2020. Disponível em: <https://repositorio.ufsc.br/handle/123456789/218387>. Acesso em julho de 2021

CAVELTY, Myriam Dunn. The Militarization of Cyber Security as a Source of Global Tension. In: Wenger, Andreas; Möckli, Daniel; Mahadevan, Prem. **Strategic Trends 2012: Key Developments in Global Affairs**. Zurique: Center for Security Studies (CSS), 2012b. p. 103-124.

CHOUCRI, Nazli. **Cyberpolitics in international relations**. MIT press, 2012.

CLARK , David D . 2010 . **Characterizing Cyberspace:** Past, Present and Future. MIT Working Paper Series, Version 1.2, March 12.

CLARKE, Richard A; KNAKE, Robert A. Cyber War: **The Next Threat to National Security and What to do About It**. New York: HarperCollins Publishers, 2012.

COSTA, Alan Denilson Lima. Centro de defesa cibernética. IN: BAPTISTA, R.R.C; FERREIRA, J.M.M; RAMOS, C.R.F. **Ciberespaço: a nova dimensão do campo de Batalha.** Disponível em: <http://ompv.eceme.eb.mil.br/images/defcib/cee/Eceme_CEE2019.pdf>. Acesso em janeiro de 2021

DAHL, Robert A. Who Governs: Democracy and Power in an American City. **New Haven:** Yale UP, 1961.

DAHL, Robert. 1989. **Democracy and Its Critics**. Haven: Yale University Press.

DE RÊ, Eduardo. **Ciberespaço e segurança cibernética:** as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil. TCC (graduação) - Universidade Federal de Santa Catarina. Centro Sócio-Econômico. Relações Internacionais. 2021. Disponível em: <https://repositorio.ufsc.br/handle/123456789/223136>. Acesso em abril de 2022

DINIZ, G.; MUGGAH, R.; GLENNY, M. Securitização da cibersegurança no Brasil. **Cadernos Adenauer,** v. 15, n. 4, p. 69-109, 2014.

EUROPOL - EUROPEAN POLICE OFFICE. Internet Organised crime threat assessment (Iocta). 2018. Disponível em:<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018> Acesso em junho de 2019.

EPEX - ESCRITÓRIO DE PROJETOS DO EXÉRCITO. **Integrando capacidades na vigilância e na atuação em nossas fronteiras**. 2019. Disponível em: <http://www.epex.eb.mil.br/index.php/sisfron/>. Acesso em 20 de junho de 2022.

FARIAS, D ; FERRAZ, V. Saber e poder na atualidade: questão cibernética. In: Décimo Encontro Nacional da Associação Brasileira de Estudos de Defesa, 2018. **Anais eletrônicos…** Disponível em: < https://www.enabed2018.abedef.org/resources/anais/8/1534726005_ARQUIVO_Farias,Ferraz-Saberepodernaatualidade-questaocibernetica(ENABED2018).pdf>. Acesso em: janeiro de 2021

FAVERO, Pedro Henrique Paulette. Recursos cibernéticos e defesa nacional: a influência da cibernética no poder dos Middle Powers States. **Relatório Final de iniciação científica.** Universidade Federal de Santa Catarina. 2021.

FERNANDES, J.H. C. A perniciosa armadilha cibernética e uma proposta de mobilização nacional. In: GHELLER, Gilberto Fernando; GONZALES, Selma Lúcia de Moura; MELO, Laerte Peotta d. **Amazônia e Atlântico Sul** : desafios e perspectivas para a defesa no Brasil. IPEA, 2015a. Disponível em: < https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/150831_amazonia_e_atlantico_sul_web.pdf>. Acesso em janeiro de 2021

_____. O espectro de atuação do centro de defesa cibernética (CDCiber) sob o enfoque de uma integração sistêmica baseada nos campos do poder nacional. In: GHELLER, Gilberto Fernando; GONZALES, Selma Lúcia de Moura; MELO, Laerte Peotta d. **Amazônia e Atlântico Sul** : desafios e perspectivas para a defesa no Brasil. IPEA, 2015b. Disponível em: <https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/150831_amazonia_e_atlantico_sul_web.pdf>. Acesso em janeiro de 2021

FERREIRA NETO, W. B. Geopolítica e Território Cibernético: Teoria de Fronteiras, política e estratégia para essa nova dimensão territorial. 2012. In VI Encontro Nacioal da Associação Brasileira de Estudos de Defesa, 2012. **Anais eletrônicos...** Disponível em: <https://www.abedef.org/download/download?ID_DOWNLOAD=74>. Acesso em janeiro de 2021

FERREIRA NETO, W. B. Territorializando o "Novo" e (Re)territorializando os Tradicionais: A Cibernética como Espaço e Recurso de Poder. **Coleção Meira Mattos,** Rio de Janeiro, v. 8, n. 31, p. 7-18, abr./2014.

FONSECA, Leila Oliveira da. **Cibersegurança:** o Brasil e o México em uma perspectiva comparada. TCC (graduação) - Pontifícia Universidade Católica de Goiás. Relações

Internacionais. 2018. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cmdn/2019/5a_ciberseguranaa_oa_brasila_ea_oa_mexicoa_ema_umaa_perspectivaa_comparada.pdf/view>. Acesso em fevereiro de 2021

GIBSON, William. **Neuromancer.** Trad. Fábio Fernandes. 5ª ed. São Paulo: Aleph, 2016

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. a geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética? **Austral: Revista Brasileira de Estratégia e Relações Internacionais**. v.7, n.14, Jul. 2018. Disponível em <https://seer.ufrgs.br/austral/article/download/87994/50497>. Acesso em janeiro de 2021.

IBGE - INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Pesquisa nacional por amostra de domicílios**: síntese de indicadores. Rio de janeiro: IBGE, 2016. Disponível em <https://biblioteca.ibge.gov.br/visualizacao/livros/liv98887.pdf>. Acesso em 2 de fevereiro de 2022.

IMD - INTERNATIONAL INSTITUTE FOR MANAGEMENT DEVELOPMENT. **IMD world competitiveness booklet**: 2010. Lausanne: International Institute For Management Development, 2010. Disponível em: <https://cedakenticomedia.blob.core.windows.net/cedamediacontainer/kentico/media/general/pdf/15152-wcy_scoreboard_2010.pdf> Acesso em: 10 jun. 2022.

IMD - INTERNATIONAL INSTITUTE FOR MANAGEMENT DEVELOPMENT. **IMD world competitiveness booklet**: 2022. Lausanne: International Institute For Management Development, 2022. Disponível em: <https://imd.cld.bz/IMD-World-Competitiveness-Booklet-2022/4/> Acesso em: 20 jun. 2022.

INSTITUTO IGARAPÉ. **O histórico da cibersegurança.** 2022. Disponível em: <https://ciberseguranca.igarape.org.br/cronologia/>. Acesso em abril de 2021

IPEA - INSTITUTO DE PESQUISA ECONÔMICA APLICADA. **Sistema integrado de monitoramento de fronteiras em perspectiva.** 2019. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/9317/1/td_2480.pdf>. Acesso em janeiro de 2022

ITU - INTERNATIONAL TELECOMMUNICATION UNION. **Global cybersecurity index**. 2018. Disponível em: <Global Cybersecurity Index 2018 ${field:Subtitle report} (itu.int))> . Acesso em fevereiro de 2022

ITU - INTERNATIONAL TELECOMMUNICATION UNION. **Measuring the information society report**. 2017. Disponível em: <https://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf>. Acesso em junho de 2022.

IZYCKI, E.A. Capacidade cibernética na América Latina: análise do histórico e projeção do potencial ofensivo. In: Décimo Encontro Nacional da Associação Brasileira de Estudos de Defesa, 2018. **Anais eletrônicos…** Disponível em:

<https://www.enabed2018.abedef.org/resources/anais/8/1535038576_ARQUIVO_Capacidade_Cibernetica_na_America_Latina.pdf >. Acesso em: janeiro de 2021

LIBICKI, M. **What Is Information Warfare?**. Washington DC: National Defense University Press, 1995.

LINS, Bernardo. Perfil Industrial do Setor de Software. In. : **Conselho de Altos Estudos e Avaliação Tecnológica**. O Mercado de Software no Brasil: Problemas Institucionais e Fiscais. Brasília: Câmara de Deputados.

LOPES, G. V. e SILVA, P.H.G. Impactos da inteligência cibernética nas ações e atividades relacionadas à mobilização nacional no Brasil. In: OLIVEIRA, Marcos Aurélio Guedes de. **Defesa cibernética e mobilização nacional**. Disponível em: <https://redectidc.com.br/assets/files/Defesa-cibernetica-e-mobilizacao-nacional.pdf>. Acesso em janeiro de 2021.

LYU, Jinghua. IPI GLOBAL OBSERVATORY. **What Are China's Cyber Capabilities and Intentions?**. Disponível em: https://theglobalobservatory.org/2019/03/what-are-chinascyber-capabilities-intentions/. Acesso em: 24 jun. de 2020

MACHADO, S. C. B. V. Arthur. **Defesa Cibernética Comparada:** Um Estudo do Brasil e da África do Sul. Artigo publicado conforme em aditamento 001/Esp-DE ao BI/AMAN Nr 140, de 31 de JUL 2017. Disponível em: https://www.academia.edu/36246194/Defesa_Cibern%C3%A9tica_Comparada_Um_Estudo_do_Brasil_e_da_%C3%81frica_do_Sul. Acesso em: 09 de abril de 2021.

MANDARINO JR., Raphael. 2010. **Segurança e Defesa do Espaço Cibernético Brasileiro**. Recife: Cubzac.

MEDEIROS FILHO, Oscar. 2014. Em busca de ordem cibernética internacional. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma Lúcia de M. **Segurança e Defesa Cibernética: da fronteira física aos muros virtuais**. Coleção I - Defesa e Fronteiras Cibernéticas Pernambuco: Editora UFPE

MONTEIRO, T. Há uma crise ética, mas instituições cumprem seu papel. **Estado de S. Paulo**, São Paulo, 2 nov. 2015. Disponível em: <http://politica.estadao.com.br/noticias/geral,ha-uma-crise-etica--mas-instituicoes-cumprem-seu-papel,1789701>. Acesso em: 24 abr. 2018.

NAIM, Moisés. 2006. **Ilícito: o ataque da pirataria, da lavagem de dinheiro e o do tráfico à economia global.** Rio de Janeiro: Ed. Jorge Zahar.

NAVAS-SABATER, J., et al. **Telecommunications and information services for the poor - toward a strategy for universal access**. World Bank, 2002. Disponível em <http://documents.worldbank.org/curated/en/496311468739312956/ Telecommunications-and-information-services-for-the-poor-toward-a-strategy-for-universal-access>. Acesso em dezembro de 2021

NYE JUNIOR, Joseph S. **Cyber Power**. Harvard Kennedy School: Belfer Center for Science and International Affairs. Cambridge, p. 1-24. maio 2010. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf>. Acesso em: 07 de abril de 2021.

NYE, Joseph S. Soft power. **Foreign policy**, n. 80, p. 153-171, 1990.

OEA - ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Revisão da capacidade de Cibersegurança**. 2020. Disponível em: <http://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf>. Acesso em fevereiro de 2021

OLIVEIRA, Marcos A. G.; PORTELA, Lucas Soares. **As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil**. Revista Brasileira de Estudo de Defesa, v. 4, n. 2, p. 77-99, 2017.

PAGLIARI, G.C; AYRES PINTO, D.J.; VIGGIANO, J. Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: Um estudo prospectivo. In: OLIVEIRA, Marcos Aurélio Guedes de. **Defesa cibernética e mobilização nacional**. Disponível em: <https://redectidc.com.br/assets/files/Defesa-cibernetica-e-mobilizacao-nacional.pdf>. Acesso em janeiro de 2021.

PLUM, Mariana Nascimento. Livro Branco de Defesa: Por quê? Para quê? Para quem? **Instituto para Reforma das Relações entre Estado e Empresa**, 2020. Disponível em <https://iree.org.br/defesa/livro-branco-de-defesa-por-que-para-que-para-quem/>. Acesso em 1 de junho de 2022.

PORTELA, L. S. Inteligência cibernética como importante fator de dissuasão para a mobilização nacional In: OLIVEIRA, Marcos Aurélio Guedes de. **Defesa cibernética e mobilização nacional**. Disponível em: <https://redectidc.com.br/assets/files/Defesa-cibernetica-e-mobilizacao-nacional.pdf>. Acesso em janeiro de 2021.

POTT, A.C; RAMOS, V.A.S. Guerra cibernética: a fragilidade das comunicações brasileiras e as implicações para a marinha. In: Nono Encontro Nacional da associação brasileira de estudos de defesa, 2016. **Anais eletrônicos…** Disponível em: < http://www.enabed2016.abedef.org/resources/anais/3/1466347704_ARQUIVO_ArtigoENABED-2016-POTT,A_RAMOS,B.FINAL.pdf>. Acesso em: janeiro de 2021

RATZEL, Friedrich. **La géographie politique**. Paris: Fayard, 1987

RID, Thomas. **Cyber war will not take place**. Oxford University Press, USA, 2013.

RUSSETT, Bruce. Liberalism. In: DUNNE, Tim; KURKI, Milja; SMITH, Steve. **International relations theories: Discipline and diversity**. Oxford University Press, USA, 2021.

SANTOS JUNIOR, J.B.D et al. **Novas ameaças e a cibersegurança:** uma análise do sistema brasileiro de defesa cibernética frente ao caso dea espionagem durante o governo Dilma Rouseff. XVI CADN. Rio de Janeiro. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/novasa_ameacasa_ea_aa_ciberseguranca_umaa_analisea_doa_sistemaa_brasileiroa_dea_defesaa_cibernetica.pdf/view>. Acesso em janeiro de 2021

SILVA, Mayane Bento et al. **Defesa Cibernética Brasileira:** O Uso do SIMOC para a Formação de Combatentes. XV CADN. Pirassununga. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/XV_cadn/defesaa_ciberneticaa_brasileiraa_oa_usoa_doa_simoca_paraa_aa_formacaoa_dea_combatentes.pdf/view>. Acesso em fevereiro de 2021

SINGER, W. P; FRIEDMAN, A. **Cybersecurity and Cyberwar: what everyone needs to know**. Oxford University Press; 1 edition. Janeiro, 2014.

SOLDATOV, A; BOROGAN, I. Russia´s approach to cyber: the best defence is a good offence. Em Hacks, Leaks and Disruptions: Russian Cyber Strategies. Institute for Security Studies. European Union. Paris: **Chaillot Papers**. 2018. Disponível: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf. Acesso em: 30 de maio de 2020.

TCU - TRIBUNAL DE CONTAS DA UNIÃO. **TC 001.873/2020-2.** Disponível em: <http://www.capitaldigital.com.br/wp-content/uploads/2020/12/documentos.pdf>. Acesso em setembro de 2021

TILLY, Charles. **Democracy**. New York: Cambridge University Press, 2007

UNITED NATIONS. **Human Development Report**. United Nations Development Programme. Oxford University Press. New York, 1994. Disponível em: < http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf>. Acesso em: 14 de janeiro de 2021.

VENTRE, Daniel. Ciberguerra. In: Academia General Militar. **Seguridad Global y Potencias Emergentes en un Mundo Multipolar**. XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza. 2012.

WANDERLEY, Ana Beatriz Queiroz et al. **Ciberdefesa em Perspectiva Comparada:** Brasil x Israel. XVI CADN. Rio de Janeiro. Disponível em:<https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/ciberdefesaa_ema_perspectivaa_comparadaa_brasila_xa_israel.pdf/view>. Acesso em fevereiro de 2021

WIENER, Norbert. **Cybernetics:** or the control and communication in the animal and the machine. 2nd ed. Cambridge: MIT Press, 1961.