ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Maj QEM MARLOS DE **MENDONÇA** CORRÊA

Espaço Cibernético: Análise de um cenário prospectivo e desdobramentos para as Capacidades do Exército Brasileiro

Rio de Janeiro
2020

Maj QEM MARLOS DE **MENDONÇA** CORRÊA

Espaço Cibernético: Análise de um cenário prospectivo e desdobramentos para as Capacidades do Exército Brasileiro

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército como requisito parcial para conclusão do Curso de Especialização em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: Ten Cel Com Rodrigo **Damasceno** Sales

Rio de Janeiro
2020

C824e Corrêa, Marlos de Mendonça

Espaço Cibernético: análise de um cenário prospectivo e desdobramentos para as Capacidades do Exército Brasileiro. / Marlos de Mendonça Corrêa. ─2020.
90 f. : il. ; 30 cm

Orientação: Rodrigo Damasceno Sales.
Trabalho de Conclusão de Curso (Especialização em Ciências Militares) ─ Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.
Bibliografia: f. 81-90

1. ARMA DE CIBERNÉTICA. 2. CIBERNÉTICA. 3. DEFESA CIBERNÉTICA. 4. ESPAÇO CIBERNÉTICO. 5. GUERRA CIBERNÉTICA. 6. GUERRA DO FUTURO. I. Título.

CDD 003.5

MAJ QEM MARLOS DE **MENDONÇA** CORRÊA

Espaço Cibernético: Análise de um cenário prospectivo e desdobramentos para as Capacidades do Exército Brasileiro

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército como requisito parcial para conclusão do Curso de Especialização em Ciências Militares, com ênfase em Defesa Nacional.

Aprovado em 30 de outubro de 2020.

COMISSÃO AVALIADORA

_____
RODRIGO DAMASCENO SALES – TC Com - Presidente
Escola de Comando e Estado-Maior do Exército

_____
CANDIDO CRISTINO LUQUEZ MARQUES FILHO – Cel R/1 Art - Membro
Escola de Comando e Estado-Maior do Exército

_____
ADRIANO DE PAULA FONTAINHAS BANDEIRA – Maj QEM - Membro
Escola de Comando e Estado-Maior do Exército

À minha mãe, Rachel (*in memorian*), pelo amor, carinho e desvelo que me tornaram o homem que sou. Fostes a mais bela e reluzente luz de minha vida.

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus simplesmente por tudo.

Agradeço, também, aos meus avós Nelson (*in memoriam*), Maria (*in memoriam*), Pedro (*in memoriam*) e Zentith (*in memoriam*) pelos exemplos de dignidade e humanidade que balizaram meu caminhar.

Aos meus pais, Nelmari e Rachel (*in memoriam*), minha irmã Ívy e minha sobrinha Maria Eduarda, agradeço pelo sempre sólido e irrestrito apoio.

À Glaucia, minha companheira e amiga por uma década, e à Glória, cujo apoio e compreensão de ambas foram essenciais para que esse objetivo fosse alcançado, obrigado por terem tornado meus dias melhores.

Ao “velho”, meu sincero agradecimento.

Aos meus amigos do Curso de Direção para Engenheiros Militares, pelo convívio salutar e amizade, requisitos indispensáveis para a realização de um bom trabalho.

Agradeço ao meu orientador TC Damasceno pela compreensão e orientação, as quais foram vitais para a realização dessa pesquisa.

Ao Maj Bandeira, Coordenador do Curso de Direção para Engenheiros Militares, meu agradecimento pelo apoio na elaboração dessa pesquisa.

A todos os instrutores da Escola de Comando e Estado-Maior do Exército, cuja tutela nos estudos foi fundamental para me conduzir a este momento, meu reconhecimento e gratidão.

Ao Comandante da Escola de Comando e Estado-Maior do Exército e a seus integrantes, meus agradecimentos por terem tornado possível a realização desse trabalho.

A todos os professores que, ao longo da minha existência, pacientemente lapidaram a pedra bruta da ignorância até que dela saísse a inteligência capaz de produzir esse estudo, muito obrigado.

Por fim, agradeço a todos que de alguma forma, direta ou indiretamente, contribuíram para que esse trabalho fosse bem-sucedido.

Sê escravo do saber se queres ser verdadeiramente livre.
(SÊNECA)

RESUMO

A evolução tecnológica trouxe novas características para a guerra moderna. Longe de mudar sua natureza, às inovações terminaram por infundir o campo militar com a mesma fluidez vista nas demais áreas da atividade humana. Uma dessas inovações, a Guerra Cibernética, manifesta-se como um novo desafio ao estamento militar. Esse trabalho, então, se propões a estudar a Guerra Cibernética e seus impactos para o cumprimento da missão constitucional do Exército Brasileiro. Para tal, o trabalho inicia com uma introdução que posiciona a Guerra Cibernética no cenário evolutivo mundial, define o problema a ser resolvido e os objetivos a serem alcançados e formula a hipótese a ser verificada. Em seguida, a metodologia é apresentada, apontando-se as limitações do método empregado. Uma extensa revisão de literatura é, então, conduzida. Primeiro aborda-se aspectos gerais relativos à área de Defesa Cibernética. Uma vez que esses aspectos sejam explorados, o trabalho se detém na análise documental referente aos EUA. Seu pensamento militar, sua estrutura e sua forma de atuação são submetidas ao escrutínio, buscando-se compreender a visão norte-americana sobre a questão da Defesa Cibernética. Esse estudo, então, estende-se à China. Apesar da falta de transparência do país, são analisados estudos produzidos sobre o mesmo. Assim, o pensamento militar e a concepção estrutural de cibernética chinesa podem ser incorporados à análise. O Brasil também tem sua estrutura de defesa cibernética e pensamentos analisados, fazendo parte da análise documental. Ao término dessa análise, obtém-se um retrato com bom nível de detalhes das condições de defesa cibernética dos três países, assim como o cenário atual do espaço cibernético. Esse retrato é usado como base na construção de um cenário prospectivo sobre a Guerra do Futuro. Esse cenário, por sua vez, junto com a análise documental, é submetido à uma análise SWOT que, finalmente, alimenta a elaboração de três propostas de transformação capazes de impulsionar a capacidade de cibernética do Exército Brasileiro. Finalmente o trabalho termina apresentando as principais conclusões, fruto do estudo conduzido.

Palavras-chave: Arma de Cibernética, Cibernética, Defesa Cibernética, Espaço Cibernético, Guerra Cibernética, Guerra do Futuro.

ABSTRACT

Technological evolution has brought new characteristics to modern warfare. Far from changing its nature, innovations ended up infusing the military field with the same fluidity seen in other areas of human activity. One of these innovations, the Cyber War, presents itself as a new challenge to the military. This work, then, proposes to study the Cyber War and its impacts for the fulfillment of the constitutional mission of the Brazilian Army. To this end, the work begins with an introduction that places Cyber War on the world evolutionary scenario, defines the problem to be solved and the objectives to be achieved and formulates the hypothesis to be verified. Then, the methodology is presented, pointing out the limitations of the method used. An extensive literature review is then conducted. First, general aspects related to the Cyber Defense area are addressed. Once these aspects are explored, the work performs documentary analysis regarding the USA. Its military thinking, structure and way of acting are subjected to scrutiny, seeking to understand the American view on the issue of Cyber Defense. This study, then, extends to China. Despite the lack of transparency in the country, studies on it are analyzed. Thus, military thinking and the structural design of Chinese Cyber Defense can be incorporated into the analysis. Brazil also has its Cyber Defense structure and thinking analyzed, being part of the document analysis. At the end of this analysis, a picture with a good level of details about cyber defense conditions of the three countries is obtained, as well as the current scenario of cyberspace. This picture is used as a basis for the construction of a prospective scenario about the Future War. This scenario, in turn, together with the documentary analysis, is submitted to a SWOT analysis that, finally, feeds the elaboration of three transformation proposals capable of boosting the cybernetics capacity of the Brazilian Army. Finally, the work ends with the main conclusions resulting from the study conducted.

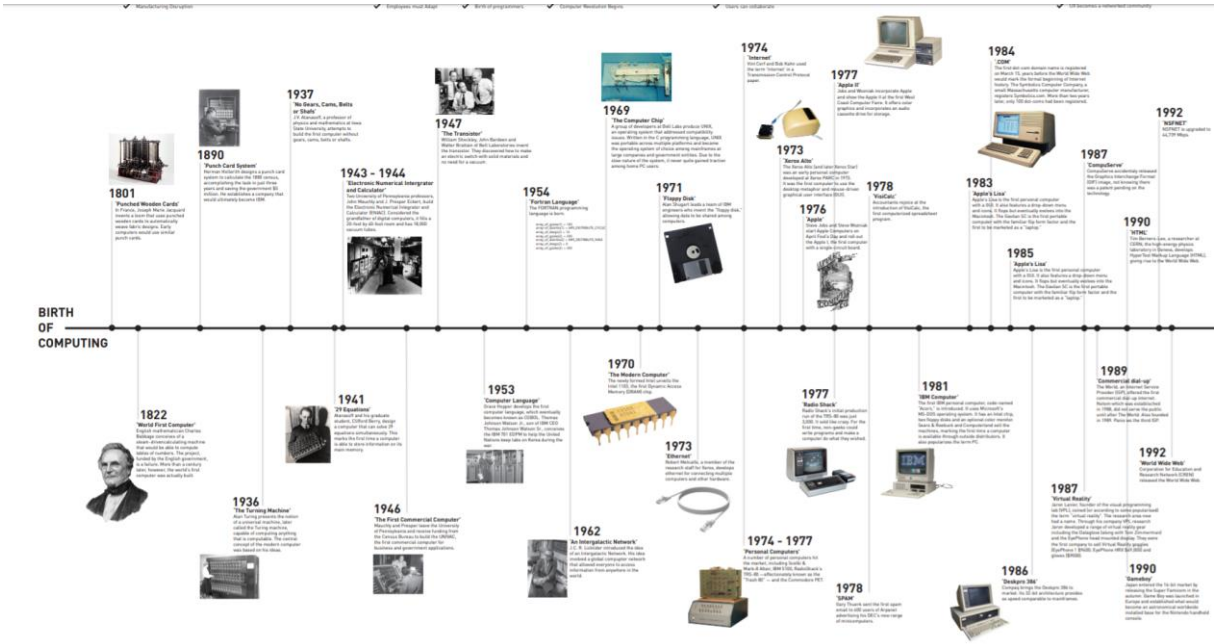
Keywords: Cybernetic Branch, Cybernetics, Cyber Defense, Cyberspace, Cyber War, Future War.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia sempre foi um fator relevante nos conflitos armados. No passado, diferenças nas tecnologias dos escudos, espadas, arcos e armaduras se revestiam em vantagem tática. A evolução tecnológica e do pensamento militar se deram num sistema de influência mútua, ora com a tecnologia alterando a doutrina, ora ocorrendo o inverso. Por séculos a evolução se deu num clima de relativa harmonia. Modificações no pensamento militar, conforme aponta Luttwak (LUTTWAK, 2009), costumam ser lentas por motivos diversos. Porém, por muito tempo, as evoluções tecnológicas também seguiram essa lógica. Entretanto, a partir da década de 1960, com a Revolução Tecnológica, as mudanças começaram a acelerar e a se avolumar, marcando um descompasso com a evolução do pensamento militar. A Figura 1 mostra a evolução das inovações na área de computação.

Figura 1: Evolução das inovações tecnológicas na área de computação.



Fonte: (BANKAI, [S.d.]).

As mudanças vividas pelo mundo atuaram de diversas formas sobre o estamento militar. Por um lado, o cenário de atuação das forças de defesa mudou. Com o avanço da Tecnologia da Informação e Comunicações (TIC), o teatro de operações se tornou mais complexo. Conceitos como a Guerra Centrada em Redes (ALBERTS e colab., 2000) marcaram as alterações ocorridas no pensamento

militar por imposição do avanço tecnológico. Contudo, as inovações tecnológicas continuaram se crescendo e se acelerando e novas tecnologias como Redes e Rádios Definidos por Software, a Internet das Coisas, o uso de *Deep Learning* e outras técnicas de Inteligência Artificial (IA) e os Veículos Aéreos Não Tripulados (VANT) fizeram com que a realidade ser transformasse mais rápido do que o pensamento militar.

Uma outra característica da Era da Informação, iniciada com a Revolução Tecnológica, é a popularização do conhecimento científico-tecnológico. Agora, o conhecimento não está mais restrito a um pequeno grupo de notáveis ou de países, mas encontra-se distribuído entre nações - algumas sem qualquer destaque no campo científico, entre grupos terroristas, empresas e indivíduos. Algo que Nye (NYE, 2012) chama de “difusão do poder”. Com isso, novos atores foram inseridos tanto na geopolítica global, quanto na tática das operações militares. O já complexo campo da guerra, ficou, então, ainda mais incerto e confuso. Um ambiente verdadeiramente VICA (Volátil, Incerto, Complexo e Ambíguo).

A Revolução Tecnológica proporcionou significativo avanço nas áreas de comunicações, computação e eletrônica após 1960. Esses avanços transformaram a maneira como as relações se processam, interconectaram pessoas, organizações e países, aceleraram as comunicações e criaram novas formas de interação. Assim surgiu um novo espaço, chamado Espaço Cibernético, o qual é formado pelos limites do mundo virtual criado com a interconexão, atores e sistemas. O Espaço Cibernético logo tornou-se um novo palco de disputa e conflito, atraindo a atenção dos pensadores de Defesa e militares.

Esse novo espaço aprofundou o processo de transformação da sociedade chamado globalização. Através do espaço cibernético, as Nações-Estado passaram a interligar seus sistemas financeiros e, graças à velocidade da comunicação, a aproximarem as suas populações. As influências de uma cultura sobre a outra se ampliaram e modificaram e uma nova realidade surgiu no Sistema Internacional. Junto a esse processo de interconexão, estruturaram-se relações de interdependência que aumentaram a complexidade do cenário mundial.

Com a difusão do poder e a globalização, indivíduos em qualquer parte do globo passaram a ter acesso às corporações, governos e sistemas que, agora são integrados à grande rede chamada Internet. Se por um lado, isso trouxe facilidades, por outro expôs entidades, organismos e estados ao uso maléfico do espaço

cibernético. Atores individuais – pessoas – passam agora a ter a capacidade de atingir alvos estratégicos no interior profundo de um país, como o sistema financeiro ou órgão governamentais. Igualmente expostas encontram-se as grandes corporações e os bancos. Durante a pandemia da COVID-19, por exemplo, o número de ciberataques à Organização Mundial de Saúde chegou a dobrar ("Global cyber attacks on the increase during COVID-19 crisis | SecurityWorldMarket.com", [S.d.]).

Logo, esse novo espaço alça indivíduos e entidades – que no mundo real não possuem protagonismo – a elementos relevantes para o Sistema Internacional. Nesse diapasão, o Espaço Cibernético adiciona elementos a geopolítica das nações, cujos efeitos ainda estão sendo aprendidos.

O estamento militar foi, assim, desafiado pela inovação tecnológica em diversos aspectos. Sua forma de atuação foi contestada, seu espectro de ações alargado, seu domínio de atuação ampliado e, até mesmo a formação dos recursos humanos passou a demandar novas capacidades. A Guerra do Futuro passa, então, a denominar o cenário prospectivo para os conflitos construído através das tendências identificadas. Esse esforço em se prospectar o futuro dos conflitos é uma tentativa de reação dos militares e pensadores de defesa, que buscam se antecipar ou ao menos se preparar para as mudanças que a evolução tecnológica vem impondo.

Ao se configurar num ambiente de ações geopolíticas e ser um definidor de tendência na Guerra do Futuro, o Espaço Cibernético mostrou-se relevante para a expressão Militar do Poder. Com efeito, o cenário atual aponta para a militarização desse novo espaço, com ações diversas visando tanto a operações defensivas quanto ofensivas. Isso pode ser evidenciado pela criação do *NATO*[1] *Cooperative Cyber Defense Centre of Excellence* em Talli, na Estônia, cuja a missão é "suportar nossas nações membro e a OTAN com expertise interdisciplinar única no campo da pesquisa em defesa cibernética, treinamento e exercícios cobrindo as áreas foco de tecnologia, estratégia e lei" (CCDCCOE, [S.d.]). Nos Estados Unidos da América, pode-se citar também os seguintes órgãos dedicados à Guerra Cibernética: *United States Cyber Command*, *US Army Cyber Command*, *Army Cyber Institute* e o *US Army Cyber Center of Excellence*.

[1] NATO (North Atlantic Treaty Organization) é a sigla em inglês da Organização do Tratado do Atlântico Norte (OTAN)

A China também vem desenvolvendo suas capacidades de Guerra Cibernética. A Estratégia Militar Chinesa em 2015 reconhecia as novas ameaças oriundas do Espaço Cibernético, colocando-o como um novo domínio da segurança nacional (CHINA e DEFENSE, 2015). No mesmo caminho seguem outros países, como Reino Unido, França e Austrália.

O Brasil, por sua vez, não está alheio às mudanças que o mundo vem passando. O Exército Brasileiro (EB) vem empreendendo esforços no sentido de se manter atualizado com relação às novas tecnologias e à dinâmica da guerra moderna. Para tal, o EB deu início ao Processo de Transformação do Exército, através de Diretriz do Ch EME (BRASIL. ESTADO-MAIOR DO EXÉRCITO, 2010) e tem como objetivos, dentre outros, os destacados a seguir:

> a. Promover a transformação do Exército, trazendo-o de uma **concepção ligada à era industrial para a era do conhecimento**.
>
> ...
>
> e. Implantar uma **mentalidade de inovação**. (grifo do autor) (BRASIL. ESTADO-MAIOR DO EXÉRCITO, 2010)

A diretriz em questão estabelece, ainda, que a área temática de Ciência e Tecnologia é um dos vetores de transformação do Exército. Dessa forma, o processo de transformação é a resposta do EB para buscar se manter atualizado, acompanhado as evoluções da Guerra do Futuro.

O presente estudo se baseia, então, nos fundamentos mostrados anteriormente. Em resumo, tem-se o Espaço Cibernético como tendência conformadora dos conflitos futuros, a reflexão do EB carreada através de seu processo de transformação e o fortalecimento da influência da expressão científico-tecnológica no Poder Militar. Assentado nessa tríade, o estudo conduzido busca compreender os impactos do espaço cibernético na dinâmica militar e, olhando para casos concretos, refletir sobre os impactos dessa tendência na transformação do EB em curso.

Este trabalho se restringirá à uma análise sucinta do Espaço Cibernético. Serão, também, estudados dois casos representativos: Estados Unidos da América e China. Com o entendimento obtido, buscar-se-á identificar oportunidades e desafios

para o Exército Brasileiro e será sugerida uma abordagem nacional, no escopo da transformação do Exército.

Para executar a tarefa proposta, far-se-á, nas subseções seguintes desse capítulo, a formalização do problema a ser abordado, os objetivos a serem atingidos e a formulação da hipótese. A última seção apresentará a metodologia. No capítulo 2 será apresentada a fundamentação teórica. O capítulo 3 abordará dois estudos de caso realizados de forma a subsidiar a proposta de contribuição elaborada no capítulo 4. Finalmente o capítulo 5 apresentará as conclusões e sugestões de trabalhos futuros.

1.1 PROBLEMA

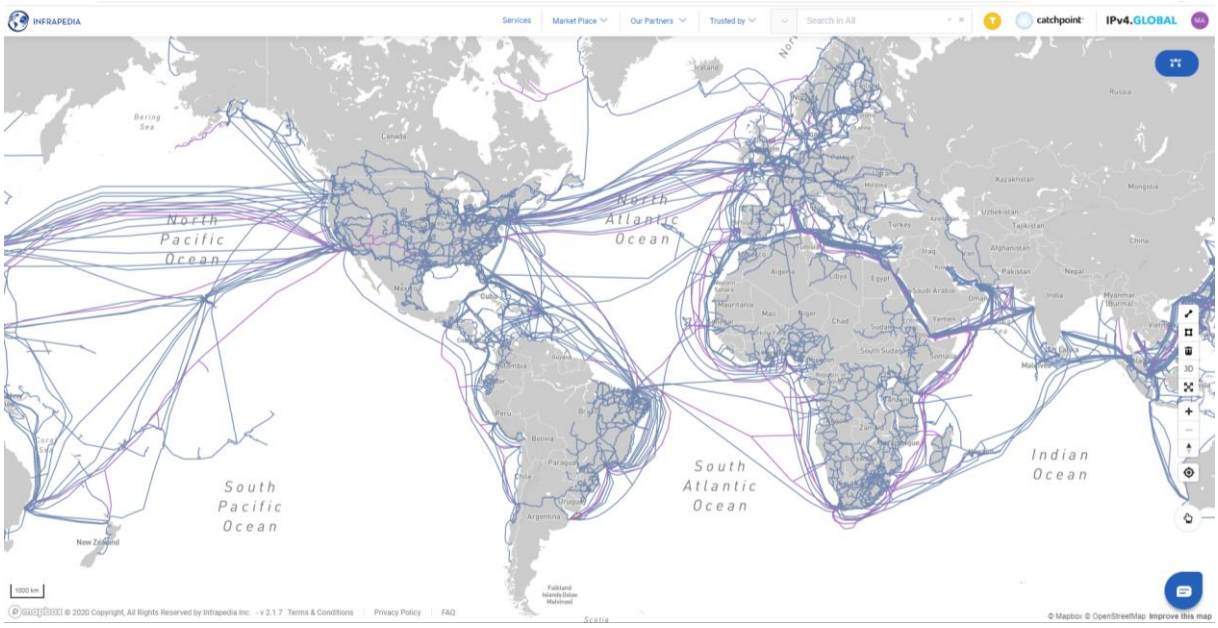
O Espaço Cibernético possui características que o distingue dos demais espaços físicos nos quais os conflitos se desenrolam. Este novo espaço, puramente virtual, originado com a Revolução Tecnológica, é marcado pela ausência de limites claros. Através dele, nações foram interligadas desprezando os limites geográficos que as delimitam. Em verdade, ele foi além, estabelecendo conexões diretas ao interior profundo dos Estados-Nação e empoderando atores não estatais improváveis.

É possível atravessar os limites geográficos das fronteiras nacionais através do Espaço Cibernético. Assim, um indivíduo ou organização pode, por meio de ações virtuais, cometer crimes e ataques em um país sem estar fisicamente no seu território. E a ausência de limites claros fica patente quando se percebe que ações virtuais podem ter consequências reais. Um célebre exemplo disso foi a ação do malware Stuxnet que desativou centrífugas de enriquecimento de urânio, atrasando o programa nuclear Iraniano, além de atacar outros sistemas (“Stuxnet: As origens”, 2014) e (“Os ciberataques mais famosos dos últimos tempos”, 2018). Essa situação é ilustrada pela Figura 2, que mostra *backbones*, submarinos e terrestres enquanto a Figura 3 mostra a cobertura de alguns satélites de comunicação. Já a figura Figura 4 exibe a cobertura celular na região da tríplice fronteira entre Brasil, Argentina e Paraguai.

As figuras mostram como o Espaço Cibernético aumenta a permeabilidade das fronteiras. Mas a complexidade do mundo virtual não se limita às fronteiras nacionais. Talvez sua característica mais marcante seja perpassar todos os campos do poder. As ações cibernéticas têm consequências no campo Político.

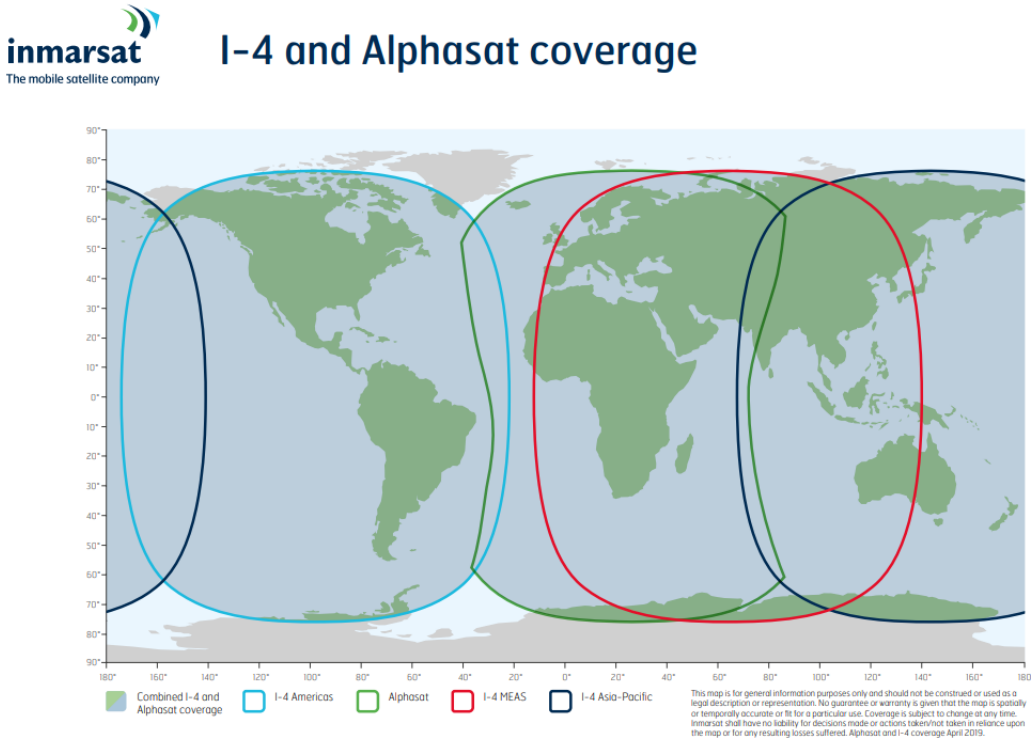
Exemplo disso pode ser encontrado na eleição presidencial dos EUA de 2016, na qual a Rússia foi acusada de tentar interferir no resultado, dando origem à uma investigação do Senado dos EUA (“REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE WITH ADDITIONAL VIEWS”, [S.d.]). Outro exemplo, que marca um desdobramento nos Campos Político e Psicossocial foi o escândalo sobre o compartilhamento de dados da rede social Facebook com a consultoria política Cambridge Analytica (BBC, 2018). Esses dados podem, em tese, ter sido utilizados para campanhas de influência em eleitores.

Figura 2: Ligações de comunicação submarinas e terrestres.



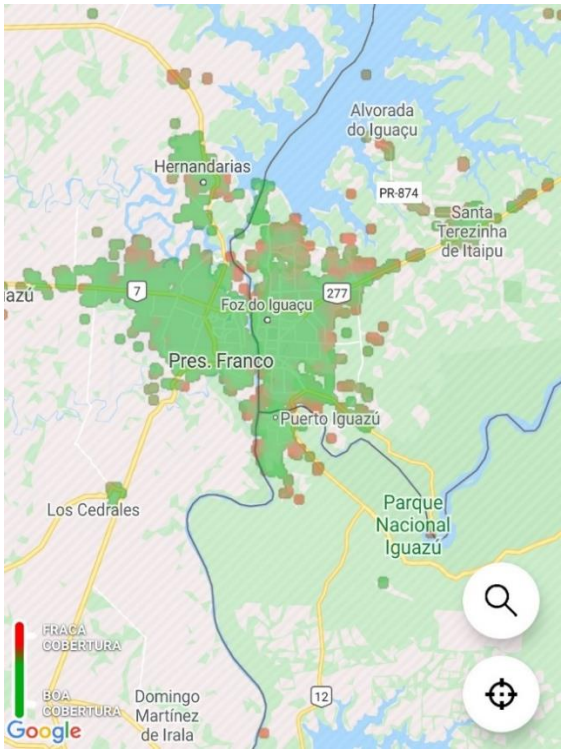
Fonte: (“Infrapedia | Global Internet Infrastructure Map”, [S.d.]).

Figura 3: Cobertura dos satélites I-4 Américas, Alphasat, I-4 MEAS e I-4 Ásia-Pacífico.



Fonte: (INMARSAT, 2019).

Figura 4: Cobertura celular na região da tríplice fronteira entre Brasil, Argentina e Paraguai.

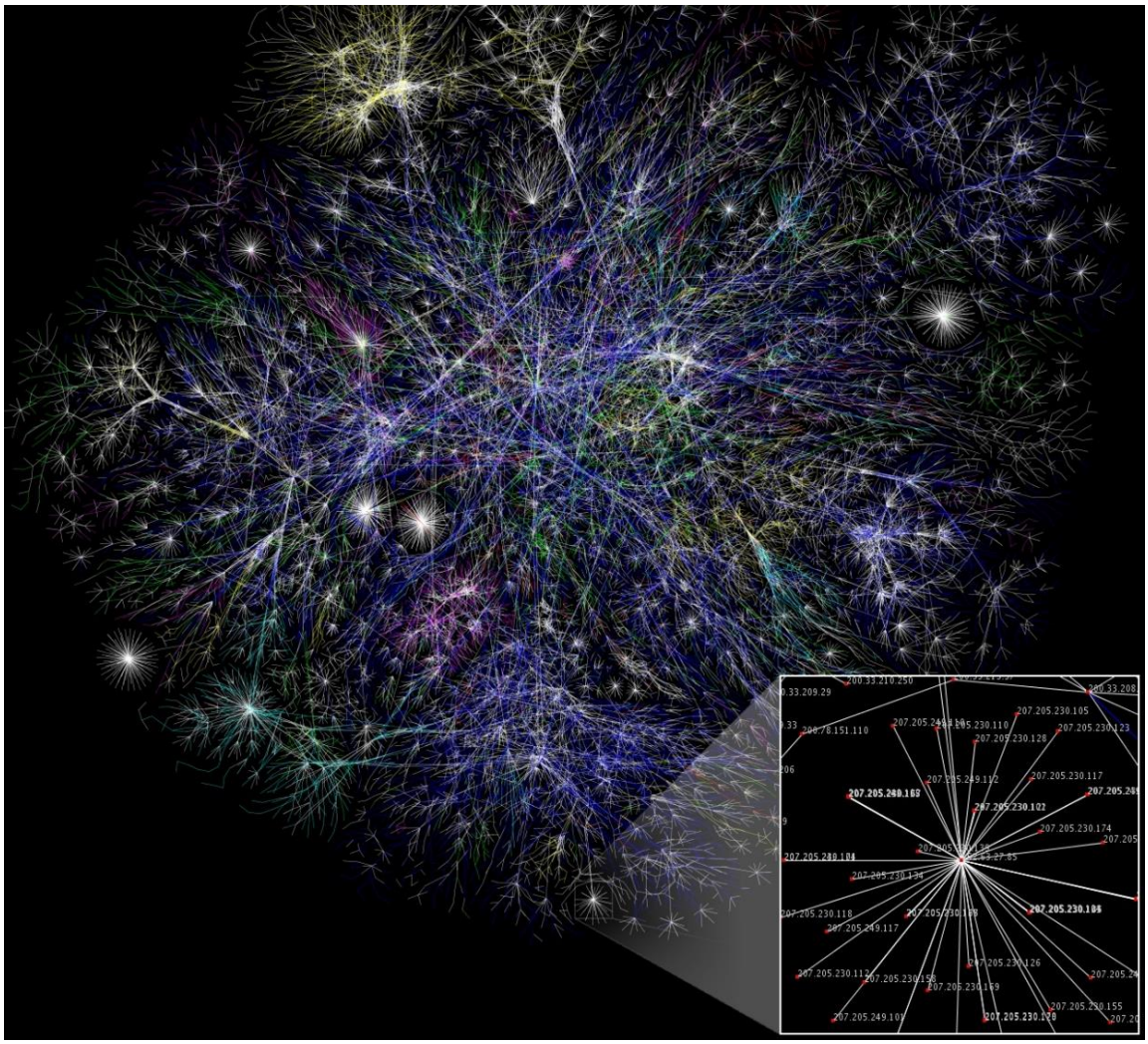


Fonte: o autor a partir do aplicativo Opensignal [2].

[2] https://www.opensignal.com/

Essas figuras apresentam diferentes meios de comunicação (integradores) – fibra ótica, satélites e rede celular que formam o tecido do Espaço Cibernético. Há outros meios, contudo, como as linhas de sistemas públicos de telefonia fixa e sistemas de rádio frequência. Assim, a representação mais acurada do Ciberespaço é dada na Figura 5. Nessa figura, mostra-se um retrato parcial das interconexões do Ciberespaço, obtido em 15 de janeiro de 2005 (WIKIPEDIA, [S.d.]). Conforme se observa na ampliação, cada nó é um endereço de *Internet Protocol* (IP). Cabe observar que não há relação direta entre um endereço IP e um equipamento. Isto é, um equipamento usado para acessar o Ciberespaço pode ter mais de um endereço IP e vice-versa, o que acentua a complexidade das ações cibernéticas.

Figura 5: Retrato parcial de interconexões no Espaço Cibernético, de 15 de janeiro de 2005.



Fonte: (THE OPTE PROJECT, 2005).

Assim, o problema que se impõe é: “Como a tendência da Guerra Cibernética e seu desdobramento na Guerra do Futuro afetam o cumprimento das missões Constitucionais do EB, conforme constam do artigo 142 da Constituição Federal (BRASIL, 2016), em especial, a Defesa Nacional?”.

1.2 OBJETIVOS

Os objetivos buscados serão divididos entre objetivo geral e específicos. O objetivo geral norteará o trabalho de forma resolver-se o problema formulado. Já os objetivos específicos definem passos intermediários a serem percorridos no progresso em direção ao objetivo geral.

1.2.1 **Objetivo geral**

Este estudo tem como objetivo geral analisar a Guerra Cibernética num cenário prospectivo.

1.2.2 **Objetivos específicos**

Os objetivos específicos desse trabalho são:

a) estudar as principais características do Espaço Cibernético do ponto de vista de Defesa;
b) analisar a abordagem de outros países relativamente à Guerra Cibernética;
c) analisar a Guerra Cibernética para o caso brasileiro; e
d) identificar oportunidades no escopo do processo de transformação do Exército Brasileiro à luz da Guerra do Futuro.

1.3 HIPÓTESE

Ao fim desse estudo, a seguinte hipótese deverá ser verificada: A criação da Arma de Cibernética é resposta adequada à tendência da Guerra Cibernética e seu desdobramento na Guerra do Futuro.

2 METODOLOGIA

O propósito desse capítulo é apresentar a metodologia empregada neste trabalho com a finalidade de resolver o problema proposto. A definição de um plano metodológico, que envolve a sistematização da produção do conhecimento, é um dos fundamentos da produção científica. Esse plano será enunciado pela definição do tipo de metodologia, do método de pesquisa e das técnicas de coleta e análise de dados.

2.1 TIPO DE METODOLOGIA

Segundo Gil (GIL, 2019), os tipos de metodologia de pesquisa são a pesquisa exploratória, a pesquisa descritiva e a pesquisa explicativa. O tipo de pesquisa que será empregado será a pesquisa exploratória, cujo foco é o levantamento de informações sobre determinado fenômeno ou problema. Esse levantamento visa a aprofundar o conhecimento sobre um problema, permitindo que sejam elaboradas hipóteses e conclusões com maior refinamento.

2.2 MÉTODO DE PESQUISA

Para (CIRIBELLI, 2003), método científico é um conjunto de etapas e instrumentos que o pesquisador emprega para conduzir seu trabalho, calcado em critérios científicos. Através desse processo, ele obtém dados que podem ou não suportar sua teoria inicial.

Gil (GIL, 2019) considera, ainda, que os métodos de pesquisa são a pesquisa experimental, a bibliográfica, a documental, a *ex-post-fact*, o levantamento de campo e o estudo de caso. Já (RODRIGUES, 2007), apresenta como métodos de pesquisa comumente empregados no levantamento de dados as entrevistas, a observação e o questionário, adotados segundo a o tipo de pesquisa científica conduzido, a saber, a pesquisa experimental, a exploratória, a acadêmica, a empírica, a de campo, a laboratorial e a teórica. No estudo em questão, a pesquisa conduzida situa-se no campo teórico, mas o emprego dos métodos sugeridos por (RODRIGUES, 2007) não se mostra viável. Assim, serão empregados os métodos de pesquisa bibliográfica e estudo de caso.

A pesquisa bibliográfica consiste no levantamento de informações sobre um tema, de forma a se adquirir ou aprofundar o conhecimento. É conduzida através

do estudo de fontes bibliográficas já tratadas, isto é, publicadas e por isso contendo a visão de um ou mais autores. Para este estudo, a pesquisa bibliográfica é uma ferramenta adequada justamente porque o que se busca é primeiramente identificar a visão que os principais formadores de tendência têm sobre a Guerra Cibernética e sobre a forma de abordá-la.

Já o estudo de caso busca ampliar o conhecimento sobre um fenômeno através da investigação dele no seu contexto. Ou seja, produz-se informações acerca de um fenômeno a partir da análise de um caso representativo. No trabalho ora conduzido, o estudo de caso se coloca como forma de validar os conhecimentos levantados na pesquisa bibliográfica. É um método válido para esta pesquisa, pois permite identificar o alinhamento entre a abordagem teórica do problema posto pela Guerra Cibernética, com a prática, que é sempre o último e definitivo validador das teorias.

2.3 TÉCNICA DE COLETA DE DADOS

Dentre as técnicas de coleta de dados apresentadas por Gil (GIL, 2019), a selecionada para emprego neste trabalho é a de documentação indireta. Essa técnica consiste na pesquisa documental e bibliográfica e se concentrará em identificar o estado da arte do pensamento sobre Guerra Cibernética. Para tal, consultar-se-ão, sobretudo, documentos oficiais e periódicos, além de artigos científicos sobre o tema. Reunidas as informações, será construído um cenário prospectivo que será alvo de análise a fim de se identificar os elementos componentes do resultado final.

2.4 TÉCNICA DE ANÁLISE DE DADOS

A técnica de análise de dados será a qualitativa. Será conduzida uma ampla e aprofundada pesquisa de literatura em torno do tema Guerra Cibernética.

2.5 LIMITAÇÃO DO MÉTODO

Uma limitação da metodologia empregada é relativa à capacidade de se analisar toda as fontes de informação disponíveis sobre o tema. Essa limitação será contornada pela restrição do presente estudo a análise de dois casos considerados significativos para o trabalho: EUA e China.

Adicionalmente, limitações menores se impõem. De forma geral, tratar de Defesa e do estado-da-arte de tecnologias como a Cibernética resvalará, inevitavelmente, em informações e documentos sigilosos. No caso particular da China, esse problema se acentua face o tradicional fechamento do governo chinês. Soma-se, ainda, nesse caso, o fato de muitas vezes não haver versões em inglês ou outro idioma de documentos oficiais. Já essas limitações serão superadas pela extrapolação a partir do conhecimento inferido quando absolutamente necessário. Caso contrário, as lacunas encontradas serão indicadas, para futuro aprofundamento.

3 REFERENCIAL TEÓRICO

O presente capítulo dedica-se a fundamentar o estudo ora conduzido através de ampla revisão bibliográfica e documental. Para isso, o mesmo será divido em quatro partes. A primeira seção versará principalmente sobre aspectos gerais relativos ao tema. Na segunda seção, será apreciada a abordagem dos Estados Unidos da América, enquanto a terceira trará a visão chinesa. Já a última seção apresentará o levantamento feito para o Brasil, concluindo assim o embasamento teórico do trabalho.

3.1 ASPECTOS GERAIS

Falar sobre guerra impõe rever Clausewitz. Apesar de mais de um século separar a obra desse teórico e o moderno conceito chamado Guerra Cibernética, o mesmo é o ponto de partida para a análise em tela. A esse propósito, Teixeira Jr (JÚNIOR, 2018) traz importantes considerações. Em primeiro, o autor ressalta o caráter imutável da natureza da guerra, apontando que esta pode, entretanto, ter características e manifestações influenciadas pelo momento e o local aonde se processam. Na análise prospectiva que faz da Guerra do Futuro, Teixeira Jr identifica que o retorno da competição entre as grandes potências tente a cooptar e alinhar atores não estatais em entornos estratégicos contestados, num verdadeiro processo de *proxy war*. Sua análise revela, ainda, que o campo cibernético se soma de fato aos domínios terrestre, marítimo e aéreo, exigindo que as forças armadas modifiquem sua doutrina e estrutura, abarcando o conceito de operação multidomínio. O autor salienta, também, a contestação da interpretação política da guerra, mas opina que “é no cenário internacional interestatal que estão os elementos que apontam para as configurações futuras da guerra” (JÚNIOR, 2018). Prosseguindo, Teixeira Jr afirma que:

> Nesse quadro, a Guerra do Futuro, ao envolver esses atores terá maior capacidade de alterar a distribuição global de poder tal como a hierarquia entre as grandes potências. (JÚNIOR, 2018)

Ao conjecturar as tendências de conduta da guerra no século XXI, o autor identifica:

> a. As forças armadas das grandes potências tenderão a competir pelo controle de seus entornos estratégicos, para isso se estruturarão (organização, doutrina e tecnologia) para operar em todos os domínios de operações ou apoio.
>
> b. A incorporação do espaço cibernético aos domínios terrestre, marítimo, aéreo e espacial poderá evidenciar mudanças estruturais na condução das operações. [...] (JÚNIOR, 2018)

Igualmente importante é a reflexão lançada no artigo de Teixeira Jr para o Exército Brasileiro:

> O entendimento da guerra como um fenômeno político e social deverá contribuir para uma reflexão por parte do Exército sobre os objetivos políticos nacionais, as missões das forças armadas, nosso modelo de força e capacidades construídas e adquiridas. A guerra e em particular os instrumentos desta forma de política tenderão a sentir o peso das necessidades de um ambiente global em transformação violenta em detrimento das preferências institucionais e tradições burocráticas endógenas à força. [...] (JÚNIOR, 2018)

Finalmente, o artigo conclui sobre o desafio particular do Brasil:

> [...] O país sofre com o gap tecnológico e terá esse desafio aumentado pelo desenvolvimento de novas tecnologias e os impactos vindouros da modernização militar de potências de status quo e revisionistas. [...] (JÚNIOR, 2018)

Muito do cenário descrito anteriormente é abordado no documento intitulado *The Third Offset Stretegy*, do *Center for Army Lessons Learned* EUA (HILLNER, 2019). O documento reconhece a China e a Rússia como competidores militares com alcance transregional e multidomínio, assim como o desenvolvimento de sistemas de guerra eletrônica e cibernética, dentre outros. Mais ainda, o documento aponta que a proliferação de sistemas e métodos de guerra para outros países, provavelmente levará o Exército dos EUA a enfrentá-los. A estratégia delineada é apresentada resumidamente da seguinte forma:

> A meta fundamental da estratégia de compensação é a dissuasão e, caso a dissuasão falhe, possuir um poder militar aumentado com

> superioridade tecnológica para destruir um adversário em qualquer domínio (terrestre, aéreo, marítimo, ciberespacial e espacial). (tradução do autor) (HILLNER, 2019)

Em sua análise da *Third Offset Strategy*, o relatório (ELLMAN e colab., 2017) elaborado para o *Center for Strategic & International Studies* aponta que o foco tecnológico se dá em 5 (cinco) áreas chave; sistemas de aprendizagem autônomos, tomada de decisão colaborativa homem-máquina, operações humanas assistidas, operações avançadas de sistemas não tripulados, armas autônomas habilitadas para rede e projéteis de alta velocidade. Para tal abordagem, necessita-se que "a organização do DoD[3] faça duas coisas pelas quais tradicionalmente não é conhecida: aceitar o risco de fracasso que é inerente à inovação e **demonstrar a capacidade de "falhar rapidamente"**" (grifo do autor) (ELLMAN e colab., 2017).

A *Third Offset Strategy*, porém, foca no fortalecimento da dissuasão convencional. Todavia, nota-se a presença do componente cibernético, assim como a influência do desenvolvimento tecnológico.

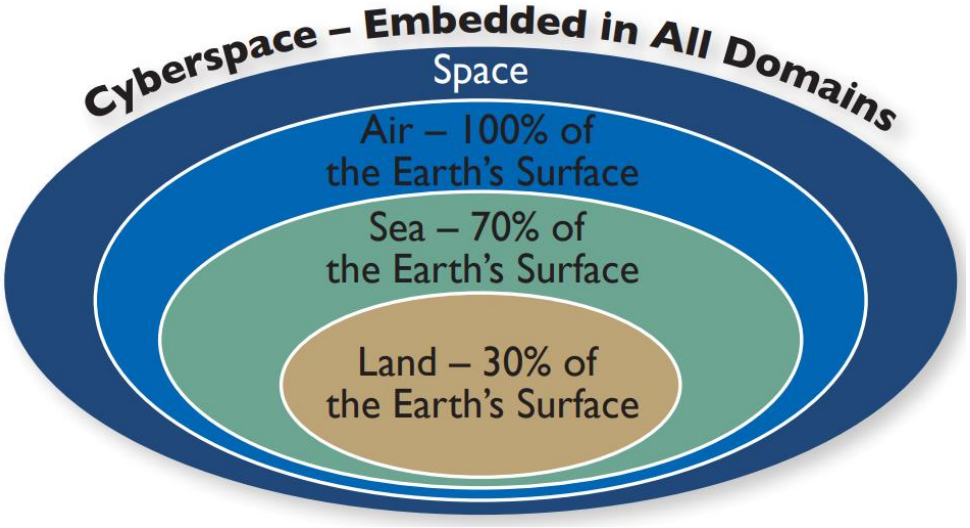
Interessante análise sobre a guerra cibernética é apresentada no artigo *Cyber Warfare: Terms, Issues, Laws and Controversies* (SEVIŞ e SEKER, 2016). O artigo inicia ressaltando o deslocamento do campo de batalha tradicional para o virtual, com a consequente criação de forças cibernéticas pelos países. Com isso, os autores discutem alguns conceitos de ciberespaço (espaço cibernético). Merece destaque que os conceitos definidos pelos EUA (STAFF, 2020) e pela OTAN diferem essencialmente quanto à considerar os seres humanos incluídos ou não nesse espaço. Um olhar mais detido sobre o entendimento da OTAN (KLIMBURG, 2012), mostra que a razão da inclusão de seres humanos é devido à interação social e a forma de atuação dos indivíduos nesse espaço. O manual de Doutrina Militar de Defesa Cibernética do Ministério da Defesa do Brasil, porém, define Espaço Cibernético como "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas" (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

No prosseguimento da discussão, o artigo (SEVIŞ e SEKER, 2016) destaca que a Guerra Cibernética é considerada a quinta zona de combate, visão essa

[3] United States Department of Defense (USDoD ou apenas DoD)

ratificada pelo Gen Larry D. Welch (Ret) da USAF (WELCH, 2011). O militar traça sua análise enfatizando as similaridades que existem na abordagem são desafios nos domínios terrestre, marítimo, aéreo, espacial e cibernético. No seu entender, o propósito de sua avaliação não é “minimizar os desafios do ciberespaço, mas ao contrário, enfatizar a necessidade de desenvolver sobre capacidades comprovadas [...]” (WELCH, 2011), ou seja, embasar os processos de guerra cibernética nos processos já bem estabelecidos em outros domínios. Entretanto, o autor destaca que, ao contrário dos outros domínios que possuem uma hierarquia geofísica bem estabelecida, o ciberespaço perpassa a todos, sendo um domínio embutido nos demais, como mostra a Figura 6. A consolidação do espaço cibernético como um domínio no entendimento dos militares dos EUA pode ser observada, por exemplo na instituição de condecorações exclusivas para ações realizadas nesse domínio (“Pentagon creates new medal for cyber, drone wars - U.S. - Stripes”, [S.d.]).

Figura 6: Domínios operacionais.



Fonte: (WELCH, 2011).

A razão de se deter na análise do ciberespaço é que seu entendimento é crucial para a compreensão sobre o que é Guerra Cibernética. Todavia, identificar quando uma atividade maliciosa pode ou não ser considerada guerra cibernética é difícil (SEVIŞ e SEKER, 2016). Basta recordar que ações cibernéticas podem ter origem e destino não estatais. A Guerra Cibernética “*refere-se a um assalto digital massivamente coordenado a um governo por outro, ou vasto grupo de cidadãos. É a ação de um Estado-nação para penetrar os computadores e redes de outra nação com o propósito de causar danos ou interrupção*” (tradução do autor) (SEVIŞ e

SEKER, 2016). Mas talvez o mais relevante sobre essa discussão é o entendimento de que "*se houver dano ou prejuízo decorrentes de ataques cibernéticos, então isso pode ser caracterizado como Guerra Cibernética*" (tradução do autor) (SEVIŞ e SEKER, 2016).

Outro ponto a ser considerado é que ataques cibernéticos podem facilmente destruir sistemas empregados na guerra convencional, com o agravante de que as armas cibernéticas – computadores, hardwares e softwares, são muito mais baratos do que munições reais. Ou seja, mais informações críticas e mais danos significativos podem ser infligidos a um custo razoável (SEVIŞ e SEKER, 2016).

No que toca à popularização do conhecimento relacionado à ataques cibernéticos, *frameworks* de armas digitais encontram-se disponíveis, como por exemplo o Regin. Conforme um estudo mencionado em (SEVIŞ e SEKER, 2016), esse framework tem sido usado para atacar diversos países, como o Brasil. Acredita-se que tais ataques tenham por trás o *the Five Eyes Alliance*, que inclui EUA, Reino Unido, Canadá, Austrália e Nova Zelândia.

As dificuldades em se estabelecer conceitos e definições claros e o elemento inovador que a cibernética representa impactam também o campo jurídico. Segundo o Lt. Gen. Keith B. Alexander, do Exército dos EUA, há um descompasso entre a capacidade de conduzir ações cibernéticas e as leis e políticas governamentais (SHANKER, 2010). Já os autores do artigo *Perspectives for Cyber Strategists on Law for Cyberwar*, advogam que a legislação sobre conflito armado é capaz de abarcar os aspectos mais relevantes da Guerra Cibernética (DUNLAP, 2011). Segundo o artigo, o principal problema não é a falta de legislação, mas a dificuldade de se determinar os elementos capazes de originar um processo legal. Entretanto os autores reconhecem que a aplicação dos princípios legais aos fatos envolvidos num ataque cibernético é tarefa difícil.

A questão legal é relevante, pois, além das considerações relativas à abrangência do Direito Internacional do Conflito Armado, há questões práticas do ponto de vista estratégico, como os tratados de aliança. Frequentemente tais tratados consideram agressão a um Estado-membro uma agressão a todos os Estados. A OTAN, por exemplo, estendeu essa cláusula de agressão para incluir ataques cibernéticos (NATO, 1949), (STOLTENBERG, 2019) e (BBC, 2019). Fruto dessa preocupação, a Aliança elaborou o *Tallinn Manual on the International Law Applicable to Cyber Warfare* (SCHMITT, 2013), largamente assentado sobre o

Direito Internacional Humanitário (*jus ad bellum*) e o Direito na Guerra (*jus in bello*). Em sua regra 30, o manual estabelece:

> "Um ataque cibernético é uma operação cibernética, seja ofensiva ou defensiva, da qual é razoável esperar-se que cause ferimentos ou morte de pessoas ou dano ou destruição de objetos." (tradução do autor) (SCHMITT, 2013)

É interessante observar a previsão de danos físicos como decorrência do ataque virtual.

Apesar dos entendimentos anteriores, (SEVIŞ e SEKER, 2016) ressalta que para a Organização das Nações Unidas um ataque cibernético não é considerado um ataque armado, não ensejando assim o direito de autodefesa. A Convenção de Genebra, todavia, possui uma definição de ataque mais abrangente, considerando-o como atos de violência contra um adversário (INTERNATIONAL COMMITEE OF THE RED CORSS, [S.d.]). Dessa maneira, o enquadramento de um ataque cibernético como ato de guerra mostra-se incerto, mas possível.

A questão legal envolvendo a Guerra Cibernética não se limita ao regramento jurídico dos conflitos. As ações cibernéticas ocorrem mesmo em tempo de paz, situação essa que coloca as ações legais como medida de retaliação e, mesmo, de dissuasão. A existência de um arcabouço legal que atue dessa maneira está registrada, por exemplo, na página 46 do relatório (US CYBERSPACE SOLARIUM COMMISSION, 2020) como a primeira camada de dissuasão da estratégia chamada Dissuasão Cibernética em Camadas.

3.2 A ABORDAGEM DOS ESTADOS UNIDOS DA AMÉRICA DO NORTE

Ao definir o problema que as forças armadas dos EUA enfrentam, o *U.S. Army Training and Doctrine Command* identificou quatro tendências definidoras da Guerra do Futuro: contestação em todos os domínios; campo de batalha cada vez mais letal e ativo; maior dificuldade das nações imporem sua vontade e desafios a estratégia de dissuasão (TRADOC, 2018). Ainda segundo o Comando:

> "Adversários como a China e a Rússia, alavancaram essas tendências para expandir o campo de batalha no tempo (turvando a

> distinção entre paz e guerra), em domínios (espaço e ciberespaço) e na geografia (agora estendido para a Área de Suporte Estratégico, incluindo a pátria) para criar um impasse tático, operacional e estratégico.” (tradução do autor) (TRADOC, 2018)

Como resposta ao desafio representado pela Guerra Cibernética, o Departamento de Defesa (DoD) dos EUA criou o *United States Cyber Command* – USCYBERCOM, cuja missão é “dirigir, sincronizar e coordenar as operações e planejamentos do ciberespaço para defender e promover os interesses nacionais em colaboração com parceiros domésticos e internacionais” (tradução do autor) (U.S. CYBER COMMAND, [S.d.]). O USCYBERCOM teve seu surgimento gestado pela *National Security Agency* (NSA), que o apoiou em termos de infraestrutura, pessoal e ferramentas (POMERLEAU, Mark, 2019), tendo suas origens em novembro de 2008.

Em 18 de agosto de 2017, o USCYBERCOM foi elevado por decisão presidencial a Comando Combatente Unificado, deixando de se subordinar ao USSTRATCOM. Tal mudança refletiu o papel cada vez mais central que a Cibernética passou a ter para a Defesa e o reconhecimento das mudanças da guerra (U.S. CYBER COMMAND, [S.d.]).

São elementos componentes do USCYBERCOM: do 2º Exército, o U.S. Army Cyber Command (ARCYBER); da 24ª Força Aérea, o Air Forces Cyber (AFCYBER); da 10ª Frota, o Fleet Cyber Command (FLTCYBER); e do Corpo de Fuzileiros Navais dos EUA, o U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER). Por sua vez, o USCYBERCOM possui três Forças Cibernéticas, a saber (U.S. ARMY CYBER COMMAND, [S.d.]):

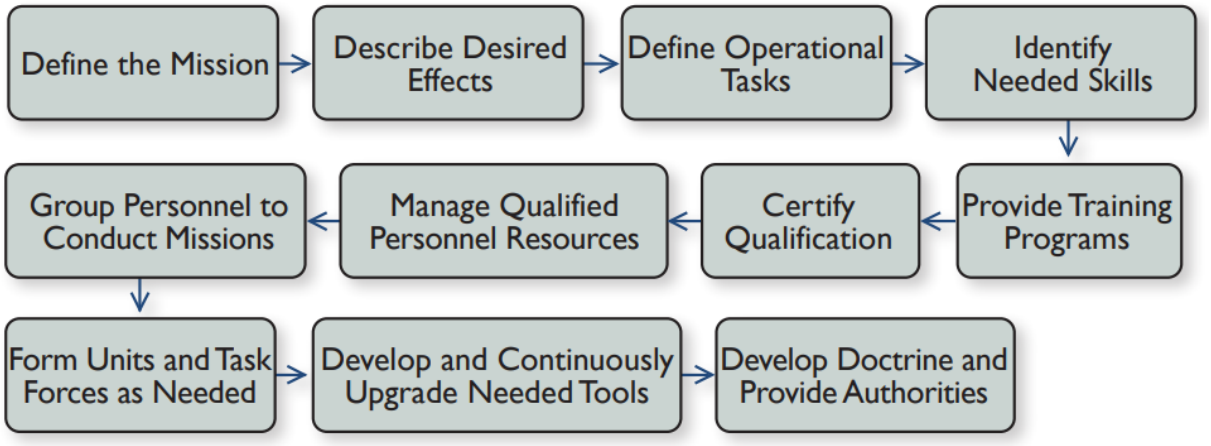
a. *Cyber National Mission Force*: possui, atualmente, 133 equipes (Cyber Mission Teams). É o braço operativo do USCYBERCOM, tendo a finalidade de monitorar atividades adversárias, bloquear ataques e manobrar para derrotar as ameaças;

b. *Cyber Combat Mission Force*: suas equipes conduzem operações cibernéticas em apoio aos Comandos Combatentes; e

c. *Cyber Protection Force*: suas equipes têm a finalidade de defender a rede de informações do DoD, proteger missões prioritárias e cuidar do preparo das forças cibernéticas para o combate.

Em 2018, o USCYBERCOM atingiu a Capacidade Operacional plena, finalizando a geração de poder de combate e entrando em estado de prontidão operacional (U.S. DEPARTMENT OF DEFENSE e DEFENSE DEPARTMENT NEWS, [S.d.]). O processo de construção de forças cibernéticas (figura Figura 7), segundo (WELCH, 2011), é similar ao processo usual de construção de capacidades para uma Brigada modular.

Figura 7: Processo de Construção de Força.



Fonte: (WELCH, 2011).

A forma de atuação do USCYBERCOM se dá pela designação de equipes para atuarem junto aos demais Comandos Combatentes, além de possuir sua própria força de combate. O Comando realiza operações Ofensivas, Defensivas e operações adstritas à rede de informação do DoD, com os objetivos de projeção de poder no espaço cibernético, proteção de dados, preservação das capacidades cibernéticas, da rede de dados e das capacidades redecêntricas (como Comando e Controle) e proteção e garantia de pleno uso da rede de informações do DoD (U.S. ARMY CYBER COMMAND, [S.d.]).

Como visto, a existência de um Comando Conjunto Cibernético, o USCYBERCOM, não prescinde da existência de seus equivalentes nas forças singulares, como é o caso do ARCYBER. A constituição desse é mostrada na Figura 8.

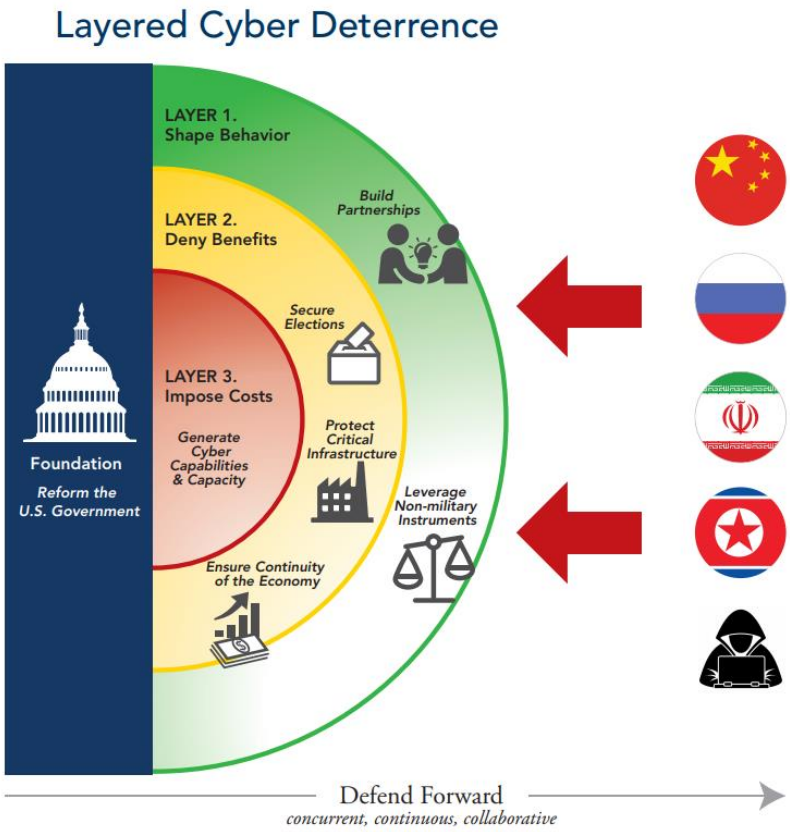
Figura 8: Cyber Mission Forces do ARCYBER.

Fonte: (U.S. ARMY CYBER COMMAND, [S.d.]).

Do ponto de vista estratégico, os EUA desenvolveram um conceito de operação para o campo cibernético chamado Defesa Avançada (*Defense Forward*). Esse conceito faz parte da estratégia de Dissuasão Cibernética em Camadas (*Layered Cyber Deterrence*) (US CYBERSPACE SOLARIUM COMMISSION, 2020). A figura ilustra os princípios dessa estratégia, enquanto a figura mostra como cada camada é envolvida ao longo da escalada do conflito.

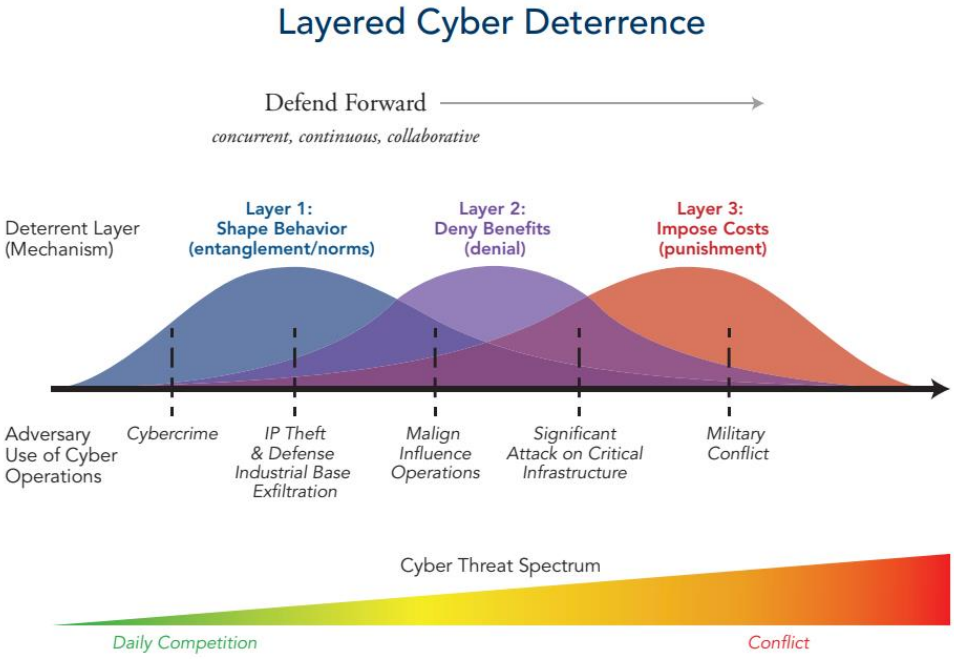
Essa estratégia tem uma abordagem ampla. A camada externa envolve abordagens tradicionais para modificar o custo-benefício de adversários aliadas a formas de influência com vistas a era da informação (US CYBERSPACE SOLARIUM COMMISSION, 2020). A promoção de normas que restrinjam ou potencializem a responsabilização jurídica de ações no espaço cibernético é um exemplo de medida desta camada e explica por que o USCYBERCOM possui, no seu quadro operacional, equipes de advogados (POMERLEAU, Mike, 2016).

Figura 9: Dissuasão Cibernética em Camadas.



Fonte: (US CYBERSPACE SOLARIUM COMMISSION, 2020).

Figura 10: Envolvimento das camadas da Defesa Cibernética em Camadas segundo a evolução do conflito.



Fonte: (US CYBERSPACE SOLARIUM COMMISSION, 2020).

A camada seguinte engloba as ações envolvendo o setor privado e a coordenação da resposta nacional às ameaças emergentes. Tem o fito de proteção das infraestruturas, economia e demais áreas da vida nacional, assim como a capacidade de atacar preventivamente atores que ameacem o ciberespaço dos EUA (US CYBERSPACE SOLARIUM COMMISSION, 2020).

Já a última camada é aquela responsável por impor custos ao atacante, decidir o conflito e dissuadir ameaças. Limita a atuação de adversários no nível abaixo do conflito armado. Numa guerra envolvendo ações cinéticas, busca prevalecer pelo emprego de todo o espectro de capacidades. Nessa camada, a Defesa Avançada tem importante papel, contribuindo para a dissuasão (US CYBERSPACE SOLARIUM COMMISSION, 2020).

Esse conceito de Defesa Avançada, originalmente estabelecido pelo DoD, “foca no instrumento militar de poder para impor custos para interromper ou parar atividades cibernéticas maliciosas na sua origem, incluindo atividades que ocorram abaixo do nível de conflito armado” (tradução do autor) (U.S. DEPARTMENT OF DEFENSE, 2018). Na Defesa Cibernética em Camadas, esse princípio envolve proatividade e a **capacidade de se empregar todos os instrumentos de poder**. **No nível mais extremo dessa abordagem, está o próprio emprego do poder militar convencional** (tradução do autor) (US CYBERSPACE SOLARIUM COMMISSION, 2020). Essa situação pode ser observada na figura Figura 10.

Da Defesa Cibernética em Camadas e do conceito de Defesa Avançada decorre uma condicionante, chamada pelo USCYBERCOM de Engajamento Persistente. Tal condicionante é entendida como o engajamento pleno com adversários, o tempo todo (LOPEZ, 2019), o que se deve pelo permanente estado de conflito vivido no espaço cibernético.

Segundo (MYRE, 2019), no Teatro de Operação Cibernético as operações não podem realizar pausas operativas. Trata-se de um ambiente altamente contestado, no qual qualquer passividade pode ter consequências imprevisíveis. O contato com o adversário nunca é rompido.

Na guerra, a iniciativa é o caminho para a vitória e a defesa deve ser usada para recuperar a iniciativa. No teatro de operações cibernético, isso exige ações ofensivas mais do que em qualquer outro domínio. A postura dos EUA pode ser

muito bem entendida na seguinte declaração de Anne Neuberger, oficial Sênior da National Security Agency (NSA) sobre o engajamento persistente:

> "Sabendo que nós não estamos aguardando pelo incidente, estamos rastreando, estamos entendendo, estamos degradando suas capacidades, sua habilidade de operar de uma forma que, esperamos, evite um ataque crucial." (MYRE, 2019)

Mas a abordagem dos EUA não se limita a instituição de um Comando Operacional Conjunto de cibernética, o USCYBERCOM. O próprio Exército dos EUA possui um Comando Cibernético, o U.S. Army Cyber Command[4] (ARCYBER). Apesar de o ARCYBER contribuir para a missão do USCYBERCOM, ele possui sua própria missão que é:

> "integrar e conduzir operações cibernéticas de amplo espectro, guerra eletrônica e operações de informações, assegurando liberdade de ação para forças amigas no e através do domínio cibernético e do ambiente informacional, enquanto nega o mesmo aos adversários." (U.S. ARMY CYBER COMMAND, 2020a).

O U.S. Army Cyber Command tem como funções educar, treinar, organizar, administrar e financiar, entre outras, além de manter forças cibernéticas capazes de conduzir operações no espaço cibernético. Ele se originou da percepção do Exército dos EUA de que as operações cibernéticas estavam aumentando globalmente e sua criação foi aprovada pelo Estado-Maior em 2010 (U.S. ARMY CYBER COMMAND, 2020c).

O ARCYBER possui três unidades, NETCOM[5], 1st IO Command[6] e a 780th MI Brigade (Cyber)[7], além de 5 centros regionais – Arizona, Havaí, Alemanha, Korea e Kwait (U.S. ARMY CYBER COMMAND, 2020a, b), num total de 16.500 militares e civis (U.S. ARMY CYBER COMMAND, [S.d.]). A Figura 11 mostra a distribuição do ARCYBER.

[4] https://www.arcyber.army.mil/
[5] https://netcom.army.mil/
[6] http://www.1stiocmd.army.mil/
[7] https://www.inscom.army.mil/msc/780mib/index.html

Figura 11: Unidades participantes do ARCYBER.

Fonte: (U.S. ARMY CYBER COMMAND, 2020a).

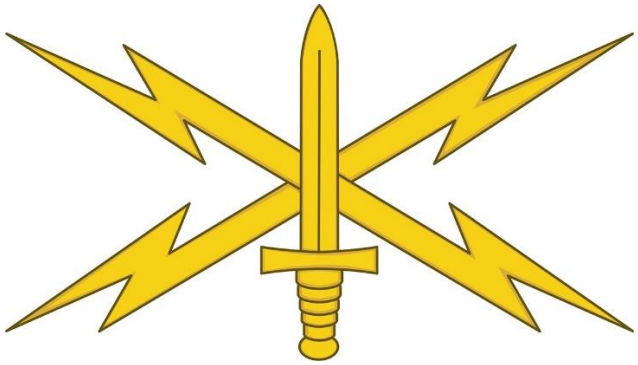
A estrutura de cibernética dos EUA envolve, ainda, uma parte acadêmica composta pela U.S. Army Cyber School[8], Army Cyber Institute[9], College of Information and Cyberspace[10], Air Force Institute of Technology[11], Cyber Training Academy[12], U.S. Army Cyber Centre of Excellence[13] e o programa universitário Hacking for Defense[14] (H4D).

Além do ARCYBER, outra importante medida tomada pelo Exército dos EUA foi a criação da Arma de Cibernética em 1 de setembro de 2014, quatro anos após a criação do ARCYBER. A Arma de Cibernética foi inovadora, não absorvendo nem o ramo de Sinais e nem o de Inteligência Militar (“Army’s Cyber branch marks its fifth anniversary | Article | The United States Army”, [S.d.]), com os quais está estreitamente ligada. Em 2018, a carreira de Guerra Eletrônica foi absorvida pela Arma de Cibernética, resultando em melhoria das capacidades operacionais em

[8] https://cybercoe.army.mil/CYBERSCH/index.html
[9] https://cyber.army.mil/
[10] https://cic.ndu.edu/
[11] https://www.afit.edu/index.cfm
[12] https://www.dcita.edu/
[13] https://cybercoe.army.mil/
[14] https://www.h4d.us/

todos os níveis (U.S. ARMY, [S.d.]). O distintivo que representa o ramo de Cibernética é mostrado na Figura 12.

Figura 12: Distintivo de Cibernética, ramo do Exército dos EUA.



Fonte: (“Army’s Cyber branch marks its fifth anniversary | Article | The United States Army”, [S.d.]).

A Arma de Cibernética do Exército dos EUA possui posições para *Enlisted Soldiers*, *Officers* e *Warrant Officers*, os quais recebem diversos treinamentos especializados, como os do *Cyber Technical College* (*Cyber Common Technical Core*, *Advanced Cyber Operations Specialist Training*, *Cyber Basic Officer Leadership Course*, *Cyber Warfare Technician Training*), *Cyber Leadership Courses* (*Cyber Captains Career Course*, *Advanced Cyber Warfare Technician*) e *Electronic Warfare College* (*Advanced Electronic Warfare Officer Qualifications Course*, *Company Crew Specialist Course*, *Electronic Warfare Technician Basic* e *Advanced*, *Electronica Warfare – Senior Leader’s Course*) (U.S. ARMY, [S.d.]). O Exército dos EUA mantém, também, um programa destinado a atrair talentos civis ou membros ativos para a carreira de cibernética, chamado *Cyber Direct Commissioning Program*. Esse programa busca atrair pessoal especializado e com experiência em Engenharia de Software, DevOps, *Machine Learning*, Cientista de Dados e Engenharia Reversa de Sistemas, Tecnologias Cibernéticas, Engenharia de Redes e Engenharia de Hardware, dentre outras competências eminentemente técnicas (U.S. ARMY, [S.d.]), (U.S. ARMY CYBER COMMAND, 2018). Além dessas habilidades, é desejada Especialidade em Operações de Campo (Capacidade Clandestina).

Apesar de o programa se concentrar na busca por talentos altamente qualificados do ponto de vista técnico, exige ainda o atendimento dos padrões físicos (teste e condicionamento físico) impostos pelo Exército. Entretanto, num

artigo publicado no sítio de internet War on The Rocks[15], Burke defende que as exigências físicas para os militares que atuam na Guerra Cibernética, em qualquer força, sejam relaxadas. Sua defesa tem como argumentos o fato de que é cada vez mais difícil para as forças armadas dos EUA recrutarem candidatos, que aproximadamente um quarto dos americanos não atingem os padrões de recrutamento e que as características da Guerra Cibernética são diferentes. Embora o autor faça tal defesa, ele aponta a necessidade de se haver guerreiros cibernéticos com bom condicionamento físico e habilidades operacionais como salto de paraquedas (BURKE, 2018).

3.3 A ABORDAGEM DA REPÚBLICA POPULAR DA CHINA

Voltando-se o olhar para a República Popular da China (RPC), é importante observar que o Regime que governa o país é pouco transparente e, por conseguinte, as fontes de informação são escassas e, muitas vezes, duvidosas. Tome-se como exemplo a publicação *China's Military Strategy* (CHINA e DEFENSE, 2015), a qual no início desse trabalho estava disponível em dois sites de notícias chineses e, a essa altura, pode ser encontrada apenas em um site internacional que o reproduziu. Logo, muito do presente estudo utilizou fontes ocidentais não-primárias para colher informações sobre a política, a estratégia e a estrutura cibernética da China.

No artigo *China's use of Cyber warfare: espionage Meets Strategic Deterrence* o autor aponta inicialmente três razões pelas quais um estado mantém e emprega uma capacidade cibernética agressiva: para dissuadir outros estados, infiltrando sua infraestrutura crítica; para conduzir ações de espionagem; e obter ganhos econômicos (HJORTDAL, 2011). Conforme fontes citadas pelo autor, a estratégia militar chinesa enxerga na capacidade cibernética uma oportunidade assimétrica com potencial para uma estratégia de dissuasão. Ou seja, a estratégia da China para rivalizar com os EUA é o fortalecimento e a exploração de suas capacidades cibernéticas. Essa visão é suportada, por exemplo, pelo o ataque cibernético contra o Google em 2009, que foi parte de um amplo ataque direcionado a mais de 34 (Yahoo, Symantec, Northrop Grumman, Morgan Stanley e outras) companhias e instituições norte-americanas (EUA) e membros do congresso. Esse

[15] https://warontherocks.com/

ataque, chamado de Operação Aurora, levou os especialistas a acreditarem no envolvimento do ELP e da indústria chinesa (SEVIŞ e SEKER, 2016), (HJORTDAL, 2011).

A visão estratégica da RPC assenta-se, segundo (DOMINGO, 2016), numa visão neorrealista de mundo. Assim, a busca do país por segurança inevitavelmente o leva à uma competição com os EUA. Diferenças fundamentais na estratégia de competição de ambos os países - China e EUA – são apontadas, mas destaca-se a interpretação de que a China considera efetivamente o uso do poder militar para decidir disputas, revelando um posicionamento mais hostil no concerto das nações.

O artigo (DOMINGO, 2016) avalia que no caso da China o uso de ações militares no ciberespaço conta com o aval do nível político e de autoridades militares. As atividades ofensivas e defensivas estariam a cargo do Terceiro e Quarto Departamento do Exército de Libertação Popular (ELP), além de possuir Escritórios de Reconhecimento Técnico (ERT) em várias regiões. As ações cibernéticas chinesas contam muitas vezes com *hackers*, universidades e outros atores não ligados diretamente ao ELP, permitindo que a RPC use de negação plausível às acusações de ataques cibernéticos (DOMINGO, 2016). Essas negações são possíveis porque, mesmo que um ataque se origine em solo chinês, o governo pode alegar que foram realizados por cidadãos patriotas sem ligação com o governo. Tal ocorreu em ataques à Geórgia e Estônia e também em ataques aos EUA com origem no território chinês (HUNKER, 2010).

Segundo relatos não confirmados publicados em (BELYAEV, 2013) e reproduzidos em (PETUKHOV e colab., 2014), a China alocava em 2013, US $ 2,7 milhões por ano para custeio de *hackers* e ações cibernéticas e tinha 100.000 (cem mil) pessoas no seu exército cibernético. De qualquer maneira, a “China possui uma notável infraestrutura de TI e armas cibernéticas avançadas” (SEVIŞ e SEKER, 2016).

A China mostra-se uma ótima estrategista na competição no Ciberespaço.

> “A persistência da RPC em melhorar suas capacidades de Operações Computadorizadas em Rede (OCR) durante os estágios iniciais da competição e, subsequentemente, testar as capacidades contra os EUA destaca a capacidade da RPC de pensar estrategicamente e fazer

> uso da OCR para desafiar a superioridade militar dos EUA". (tradução do autor) (DOMINGO, 2016)

O planejamento e o emprego de medidas cibernéticas com a finalidade de atingir infraestruturas críticas e informações de países estrangeiros são conduzidos por agências responsáveis pela segurança militar chinesa e pelos Ministérios da Defesa e da Segurança Estatal. O Estado-Maior do ELP coordena a organização da guerra de informação em redes de computadores e tem controle sobre centros especializados que analisam as possibilidades de exploração de redes computadorizadas, operações psicológicas e outras (PETUKHOV e colab., 2014).

A visão estratégica chinesa sobre o ciberespaço revela que:

> "O ciberespaço tornou-se um novo pilar do desenvolvimento econômico e social e um novo domínio da segurança nacional. À medida que a competição estratégica internacional no ciberespaço se torna cada vez mais acirrada, vários países estão desenvolvendo suas forças militares cibernéticas. **Sendo uma das maiores vítimas de ataques de hackers**, a China enfrenta graves ameaças à segurança de sua infraestrutura cibernética. À medida que o ciberespaço pesa mais na segurança militar, a China agilizará o desenvolvimento de uma força cibernética e aumentará suas capacidades de consciência da situacional no ciberespaço, defesa cibernética, apoio aos esforços do país no ciberespaço e participação na cooperação cibernética internacional, de modo a conter as principais crises cibernéticas, garantir a rede nacional e a segurança da informação e manter a segurança nacional e estabilidade social. (grifo e tradução do autor) (CHINA e DEFENSE, 2015)

Apesar de alegar ser uma vítima de ataques cibernéticos, há um enorme número de ataques perpetrados pela China contra os EUA. Os EUA chamam um assalto militar cibernético chinês pelo código *Titan Rain*, uma vez que a quantidade de ataques recebidos da china é tão grande que muitas vezes não são nomeados (SEVIŞ e SEKER, 2016).

Assim, a China espera:

> "vencer as guerras informacionais até a metade do século XXI e, segundo análises dos EUA, está desenvolvendo uma avançada capacidade de guerra de informação cujo objetivo afirmado é de

> estabelecer controle sobre o fluxo de informações do adversário e manter dominância no ciberespaço" (HUNKER, 2010)

Seguindo sua visão estratégica sobre o ciberespaço, a RPC desenvolveu um programa de inteligência de comunicações chamado *Golden Shield* que usa tecnologias inovadoras e avançadas para obter inteligência interna e externamente. Em 2014, a China criou uma brigada "Blue Force", com capacidade de ataque a dados e redes de computadores (SEVIŞ e SEKER, 2016). Em 2015 foi criada a *Strategic Support Force* (SSF), cuja finalidade é o domínio do espaço, do ciberespaço e do domínio eletromagnético (KANIA e COSTELLO, 2018). Entretanto, detalhes do funcionamento da SSF, sua estrutura e organização são pouco conhecidas, pois as informações são vagas ou sigilosas (NG, 2020), (NI e GILL, 2019). Uma visão geral foi apresentada em 2016 pelo Coronel Sênior Yang Yujun, porta-voz do Ministério da Defesa chinês:

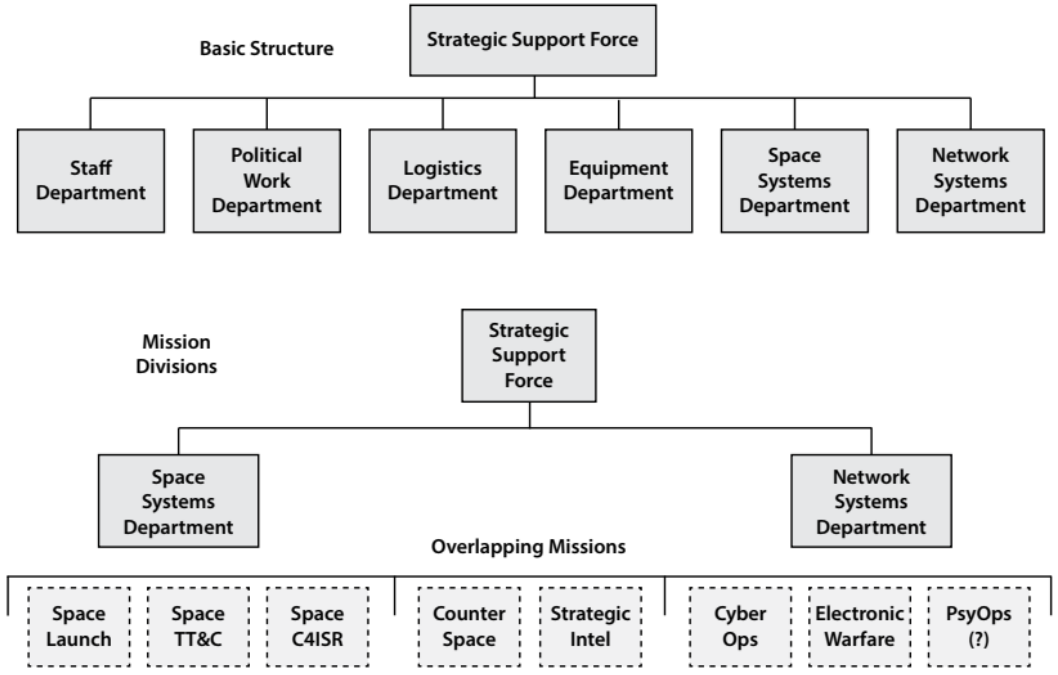
> "A Força de Apoio Estratégico é um novo tipo de força de combate para salvaguardar a segurança nacional. É um importante ponto de crescimento da nova capacidade de combate dos militares. É formado principalmente pela integração funcional de vários tipos de forças de apoio com fortes funções estratégicas, fundamentais e de apoio. O estabelecimento da Força de Apoio Estratégico é propício para otimizar a estrutura da força militar e melhorar as capacidades de apoio integrado. [O ELP] irá persistir com a integração de sistema, integração militar-civil, a construção de novas forças de combate e se esforçará para construir uma força de apoio estratégico forte e moderna." (tradução do autor) (NI e GILL, 2019)

A SSF busca o "aproveitamento das capacidades espaciais, eletromagnéticas e de redes como elementos chave habilitadores de operações conjuntas integradas através de múltiplos domínios" (NI e GILL, 2019). Trata-se de uma força que provê apoio informacional e estratégico para todo o Exército, atuando como um "guarda-chuva informacional" integrada ao ciclo operacional completo das demais forças: terrestre, naval, aérea e de foguetes. É vista como uma força crucial para a vitória (GUANGHUI, 2016).

A SSF se reporta à Comissão Militar Central e é uma das forças componentes do ELP, ao lado da Força Terrestre, Marinha, Força Aérea, Força de

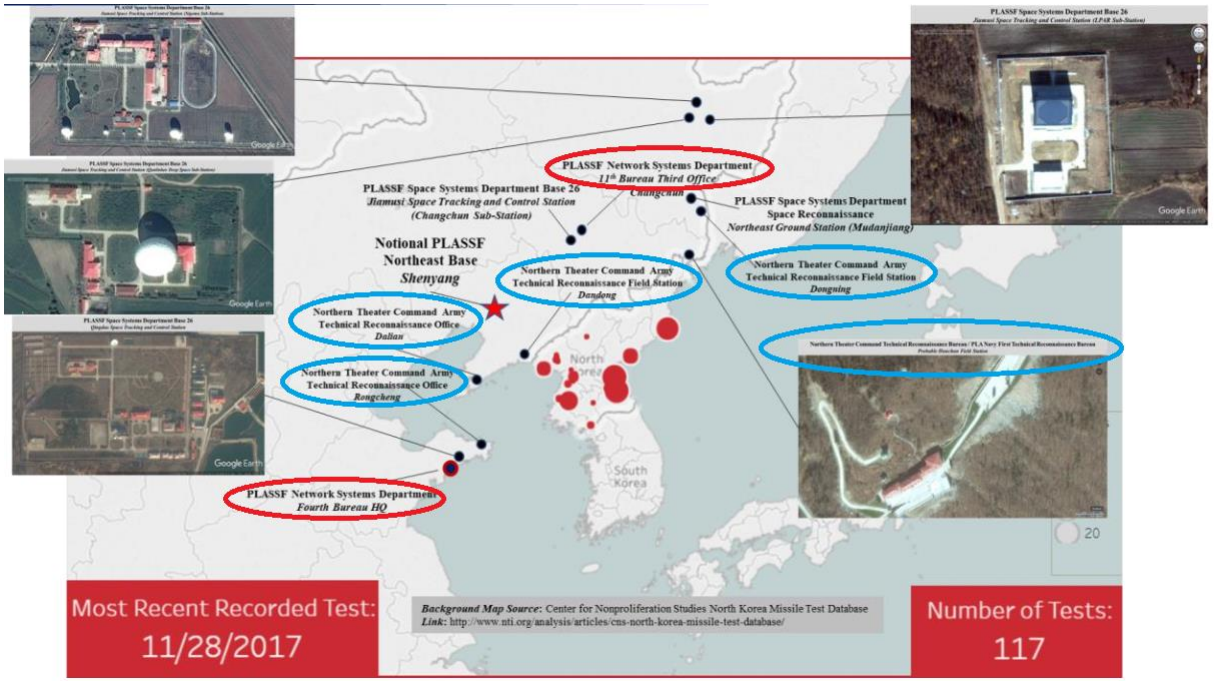
Foguete e Força de Apoio Logístico Conjunto (ZHEN, 2019), (“Category:People’s Liberation Army branches - Wikipedia”, [S.d.]). A SSF supervisiona outras duas vertentes semi-independentes: o Departamento de Sistemas Espaciais (DSE) e o Departamento de Sistemas de Rede (DSR), o qual lidera as forças cibernéticas responsáveis pelas operações de informação e cibernética. O DSR foi estruturado no terceiro Departamento do Departamento Geral de Pessoal do ELP e incorporou as unidades de IO, incluindo as relativas à guerra cibernética, guerra eletrônica e guerra psicológica (COSTELLO e MCREYNOLDS, 2018). A Figura 13 mostra a estrutura da SSF e a Figura 14 mostra a sua distribuição pelo nordeste do país. Nesta última, circulado em vermelho estão as unidades do DSR e em azul os escritórios e estações de reconhecimento técnico.

Figura 13: Estrutura componente da SSF.



Fonte: (COSTELLO e MCREYNOLDS, 2018).

Figura 14: SSF no nordeste da China.



Fonte: (BURTON e STOKES, 2018).

Além dessa estrutura, duas unidades supostamente clandestinas aparecem ligadas às atividades de cibernética conduzidas pelo ELP: a unidade 61398 (“Chinese cyber-attacks: Hello, Unit 61398 | The Economist”, 2013; COUNCIL ON FOREIGN RELATIONS, [S.d.]), (“PLA Unit 61398”, [S.d.]) e a unidade 61486 (CHENG, 2014), (KOVACS, 2014), (“PLA Unit 61486”, [S.d.]). Ambas as unidades são suspeitas de realizar operações cibernéticas e ligação com o EPL, apesar de negação oficial pelo governo da RPC.

3.4 A ABORDAGEM DA REPÚBLICA FEDERATIVA DO BRASIL

Uma vez apreciada a abordagem dos EUA e da RPC, cabe trazer à luz a forma como a Guerra Cibernética tem sido tratada pelo Brasil. Para isso, é preciso compreender como o próprio EB vem se posicionando diante da Guerra do Futuro, buscando se antecipar às mudanças vindouras. Ciente dos desafios impostos, o Exército Brasileiro vem conduzindo um processo de transformação. Essa transformação vai muito além de uma simples alteração de condutas e aquisição de material, conforme constata Duarte (DUARTE, 2018):

> "transformação implica em uma mudança marcante na totalidade da capacidade bélica de uma nação, algo que garanta uma vantagem substancial caso seja realizado, e não somente a melhoria ou aprimoramento de uma de suas capacidades bélicas". (DUARTE, 2018)

É nesse contexto que o EB busca adaptar-se à realidade da guerra moderna, a qual exibe múltiplas facetas - a Guerra Cibernética é uma delas, implementando uma significativa mudança na capacidade bélica nacional. Essa transformação alinha-se com o imposto pelos níveis Político e Estratégico para a Defesa Nacional, segundo se observa na Política Nacional de Defesa – PND (BRASIL, 2012), a qual reconhece a imprescindibilidade do domínio de tecnologias sensíveis relativas ao setor cibernético:

> 3.6. Para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, **cibernético** e nuclear. (grifo do autor) (BRASIL, 2012)

A PND vai além, reconhecendo o setor cibernético como um setor estratégico para a Defesa do País e determinando o seu fortalecimento:

> 7.10. Os setores espacial, cibernético e nuclear são estratégicos para a Defesa do País; **devem, portanto, ser fortalecidos**. (grifo do autor) (BRASIL, 2012)

Juntamente com a PND, o Brasil aprovou sua Estratégia Nacional de Defesa - END (BRASIL, 2012), que define estratégias e ações que visam à consecução dos objetivos descortinados pela PND. A END aborda a questão do setor cibernético, refletindo a mesma importância dada na PND. O documento define diretrizes que envolvem "*Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear*" (BRASIL, 2012) e estabelece oito prioridades para o setor. Dessas, destaca-se as seguintes:

> (a) Fortalecer o Centro de Defesa Cibernética com capacidade de **evoluir para o Comando de Defesa Cibernética das Forças Armadas**;
>
> ...

> (f) **Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico**, em prol das operações conjuntas e da proteção das infraestruturas estratégicas; (grifo do autor) (BRASIL, 2012)

É oportuno notar que a END dá ao Exército a função de conduzir a Defesa Cibernética, missão essa refletida na 32ª Diretriz do Comandante do EB "*Ampliar a atuação do Exército Brasileiro no setor cibernético, tanto no vetor de capacitação, quanto na integração com as demais Forças no âmbito do Ministério da Defesa*" (LEAL PUJOL, 2019).

O tema Cibernética é aprofundado nos demais documentos da Sistemática de Planejamento Estratégico Militar (SPEM). Para a atual análise, contudo, é suficiente destacar a Estratégia Setorial de Defesa (ESD) "*7.2 - Atuar no espaço cibernético de forma efetiva e negar o seu uso contra os interesses da defesa nacional*" e as Ações Setoriais de Defesa (ASD) (BRASIL. MINISTÉRIO DA DEFESA, 2016) listadas na Tabela 1 e vinculadas ao Objetivo Setorial de Defesa (OSD) "*7. Desenvolver os Setores Estratégicos de Defesa*" (BRASIL e MINISTÉRIO DA DEFESA, 2019).

Tabela 1: ASD relativas à ESD 7.2.

ESD 7.2	**Atuar no espaço cibernético de forma efetiva e negar o seu uso contra os interesses da defesa nacional.**
ASD 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.

Fonte: (BRASIL. MINISTÉRIO DA DEFESA, 2016).

O Ministério da Defesa (MD), em linha com a formulação estratégica apresentada, criou em 2014 o Comando de Defesa Cibernética (ComDCiber), sendo um Comando Conjunto permanentemente ativado. O Estado-Maior Conjunto das Forças Armadas (EMCFA) foi designado para coordenar as operações conjuntas do ComDCiber (BRASIL e MINISTÉRIO DA DEFESA, 2014). Na mesma ocasião, foi criada a Escola Nacional de Defesa Cibernética (ENaDCiber), subordinada ao ComDCiber e com caráter dual, unindo civis e militares nos corpos docente e discente. A ENaDCiber foi criada com o fito de qualificar recursos humanos dos três poderes da República, das Forças Armadas e da sociedade em geral (BRASIL e MINISTÉRIO DA DEFESA, 2014), (BRASIL e colab., 2019).

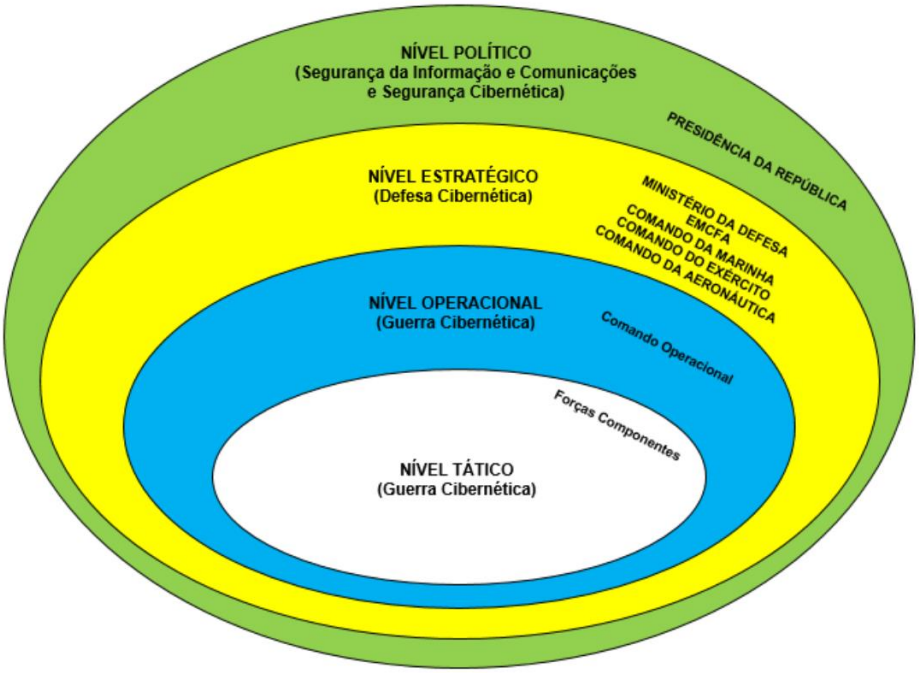
Ainda como parte de sua visão estratégica para o setor de Cibernética, o MD, juntamente com o Ministério da Ciência, Tecnologia e Inovação (MCTI), instituiu o Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética. Esse programa foi criado como uma rede de Pesquisa, Desenvolvimento e Inovação (PD&I), sob a coordenação da Secretaria de Política de Informática do MCTI. Seu principal objetivo é envolver a sociedade civil no tema Defesa Cibernética, ampliando o envolvimento do País com a questão de sua segurança cibernética (BRASIL e MINISTÉRIO DA DEFESA e MINISTÉRIO DA CIÊNCIA, 2014).

O Exército Brasileiro, por sua vez, aprovou a Política Militar Terrestre (PMT), que estipula como um Objetivo Estratégico do Exército – OEE "*atuar no espaço cibernético com liberdade de ação*" (EXERCITO BRASILEIRO, 2019). De fato, EB tem sido protagonista no campo Cibernético, tendo criado em 4 de agosto de 2010 o Centro de Defesa Cibernética (CDCiber) (BRASIL e colab., 2010). O CDCiber serviu de embrião para a criação do ComDCiber (BRASIL e MINISTÉRIO DA DEFESA, 2014) e através da Portaria nº 3.405-MD, o MD atribuiu ao CDCiber a coordenação e a integração das atividades de Defesa Cibernética no âmbito do MD, tendo o EMCFA como órgão de controle operacional em operações conjuntas (BRASIL e MINISTÉRIO DA DEFESA, 2012).

O Brasil aprovou sua Estratégia Nacional de Segurança Cibernética (E-Ciber) em 5 de fevereiro de 2020. A E-Ciber é aplicável ao quadriênio 2020-2023 e traz orientações voltadas tanto para os entes estatais, como para a sociedade civil (com foco nas infraestruturas e serviços críticos). A E-Ciber traz um diagnóstico da situação brasileira, que identifica a situação nacional e reconhece as ameaças de *hackers* e a ocorrência de cibercrimes. A estratégia, contudo, não aprofunda análises relativas a ameaças estatais de Estados competidores do Brasil, focando sua avaliação e orientações em medidas destinadas a proteção rotineira de infraestruturas e serviços (BRASIL e colab., 2020).

Outro documento relevante é a Doutrina Militar de Defesa Cibernética – MD31-M-07, aprovada pelo Ministério da Defesa. Um ponto de destaque são os níveis de decisão identificados no documento, que denotam a percepção de que a Guerra Cibernética estende-se desde o nível político até o táctico, conforme se vê na Figura 15 (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

Figura 15: Níveis de decisão.



Fonte*:* (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

Da doutrina em comento, os conceitos de Defesa Cibernética e de Guerra Cibernética merecem destaque para o presente estudo.

> "2.2.5 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 de Inteligência e **comprometer os sistemas de informação** do oponente.
>
> 2.2.10 Guerra Cibernética - corresponde ao **uso ofensivo e defensivo de informação e sistemas de informação para 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**. 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" (grifos do autor) (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

A Doutrina Militar de Defesa Cibernética apresenta também, na Tabela 2, exemplos de formas de atuação cibernética. É possível notar que o seu emprego nos níveis mais altos envolve significativa complexidade institucional (caráter interministerial e interagências). A divisão apresentada revela, uma clara distinção operacional entre os tempos de paz e de conflito ou crise. A atuação em tempo de paz envolve, inclusive, a autorização do nível político, como se depreende do seguinte trecho do manual em comento:

> "2.8.5.1. Operações de Não Guerra. Por ocasião da execução de Operações de Não Guerra, o emprego de ações de ataque cibernético necessita de autorização expressa de autoridade competente, normalmente em nível político. Para as ações de exploração cibernética, deverão ser observados atos normativos do ordenamento jurídico em vigor. Em caso de dúvidas, caberá ao EMCFA consultar o nível político acerca do emprego das ações anteriormente mencionadas" (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

Tabela 2: Formas de atuação cibernética.

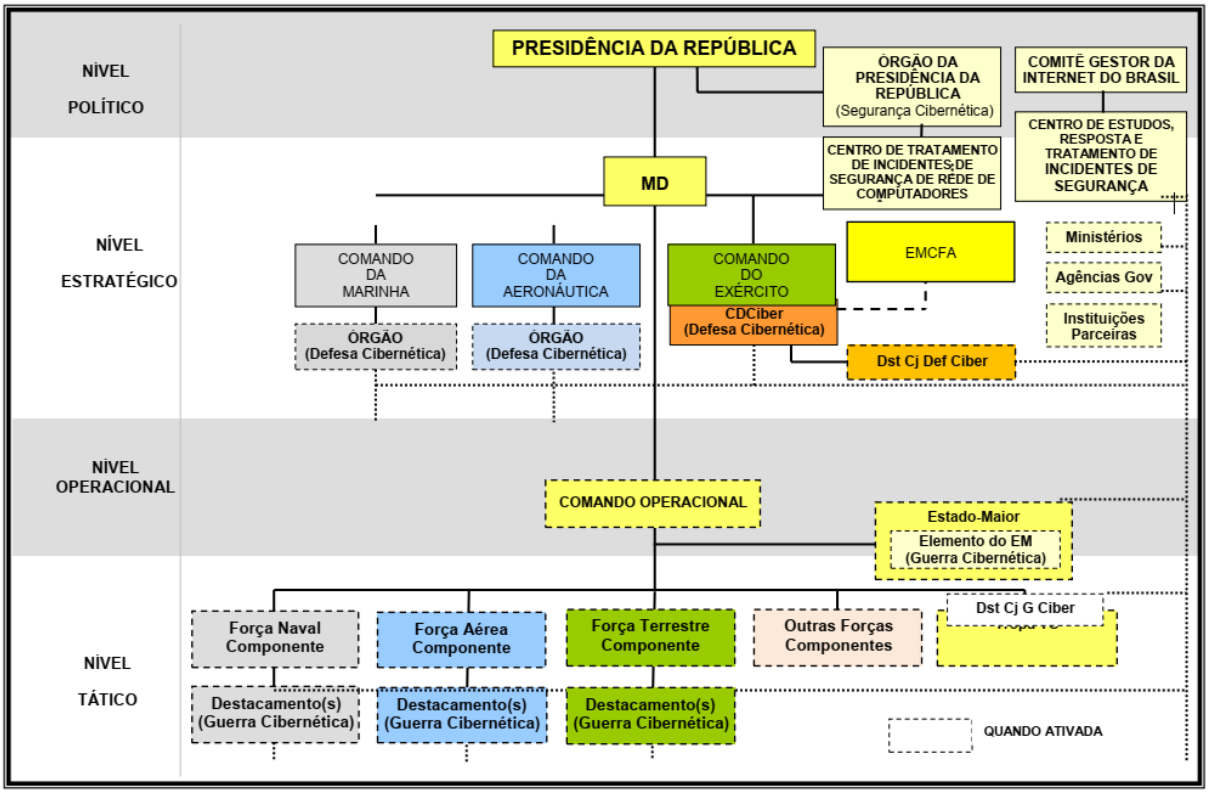
Forma de Atuação Cibernética / **Critérios**	**Política / Estratégia**	**Operacional / Táctica**
Nível dos Objetivos	Políticos e/ou Estratégicos	Operacionais e/ou Táticos
Foco	Obtenção de Inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Normalmente interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, Agência Brasileira de Inteligência - ABIN, Agência Nacional	Normalmente no âmbito do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores

	de Telecomunicações - ANATEL etc.)	
Contexto	Desde o tempo de paz, podendo fazer parte de uma Operação de Informação ou de Inteligência	Em um ambiente de crise ou conflito, apoiando uma ação militar
Nível tecnológico empregado	Normalmente alto ou muito alto	Normalmente médio ou baixo
Sincronização	Dentro do contexto de uma sofisticada Operação de Inteligência, podendo requerer ações diplomáticas anteriores ou posteriores	Dentro do contexto dos sistemas operacionais de uma Operação Militar, sincronizado com a manobra
Tempo de Preparação e Duração	Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento e emprego de técnicas de difícil detecção	Duração limitada, normalmente com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

Fonte: (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

A Figura 16 mostra a concepção do Sistema Militar de Defesa Cibernética, representada na publicação MD31-M-07 (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

Figura 16: Estrutura e órgãos do Sistema Militar de Defesa Cibernética.



Fonte: (BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS, 2014).

No caso do EB, o Manual de Campanha Guerra Cibernética – EB70-MC-10.232 apresenta os fundamentos da Guerra Cibernética e sua integração às funções de combate, as estruturas que compõem o Sistema de Guerra Cibernética do Exército (SGCEx), a integração da capacidade cibernética nas operações terrestres e exemplos de ações cibernéticas (BRASIL. EXÉRCITO. COMANDO DE OPERAÇÕES TERRESTRES, 2017). Esse manual praticamente reproduz os conceitos de Defesa Cibernética e Guerra Cibernética existentes na Doutrina Militar de Defesa Cibernética. Todavia, o manual caracteriza a função da guerra cibernética como de apoio: “as ações cibernéticas não são um fim em si mesmas, sendo empregadas para apoiar a condução das operações militares” (BRASIL. EXÉRCITO. COMANDO DE OPERAÇÕES TERRESTRES, 2017). Essa visão é consistente com os níveis tático e operacional aos quais o manual se destina.

Além desses conceitos, o Manual EB70-MC-10.232 apresenta a estrutura operativa de Guerra Cibernética, com suas respectivas atividades e responsabilidades, conforme se observa na Tabela 3. No Capítulo IV, o documento

expõe a Guerra Cibernética no Contexto das Funções de Combate, mostrando como se integra às últimas. No Capítulo V, é apresentada a Guerra Cibernética nas operações terrestres, definindo como as ações cibernéticas se integram aos diversos tipos de operações (BRASIL. EXÉRCITO. COMANDO DE OPERAÇÕES TERRESTRES, 2017).

Tabela 3: Estruturas operativas de Guerra Cibernética e respectivas atividades e responsabilidades.

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (B Com)			X	Realiza a proteção cibernética dos sistemas de informação do grande comando apoiado. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da FTC.
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu comandante será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)			X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC			X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação

Fonte: (BRASIL. EXÉRCITO. COMANDO DE OPERAÇÕES TERRESTRES, 2017).

Nota-se pela Tabela 3, que a responsabilidade pela condução da Guerra Cibernética está assentada majoritariamente nas organizações da Arma de Comunicações. Contudo, o manual admite que em operações o SCGEx seja reforçado por organizações do Sistema de Telemática do Exército (Centro

Integrado de Telemática, Centros de Telemática de Área e Centros de Telemática), do Centro de Desenvolvimento de Sistemas, ComDCiber, CDCiber e outros (BRASIL. EXÉRCITO. COMANDO DE OPERAÇÕES TERRESTRES, 2017).

Como se observa na portaria que estabelece a condição de funcionamento do Curso de Guerra Cibernética para Oficiais (BRASIL e colab., 2017), a participação de engenheiros militares só é autorizada em caráter excepcional. Logo, o Quadro de Engenheiros Militares (QEM) só é marginalmente aproveitado, a despeito de sua elevada qualificação técnica e da limitação de recursos humanos.

4 TENDÊNCIAS DA GUERRA DO FUTURO: UM CENÁRIO PROSPECTIVO PARA A GUERRA CIBERNÉTICA

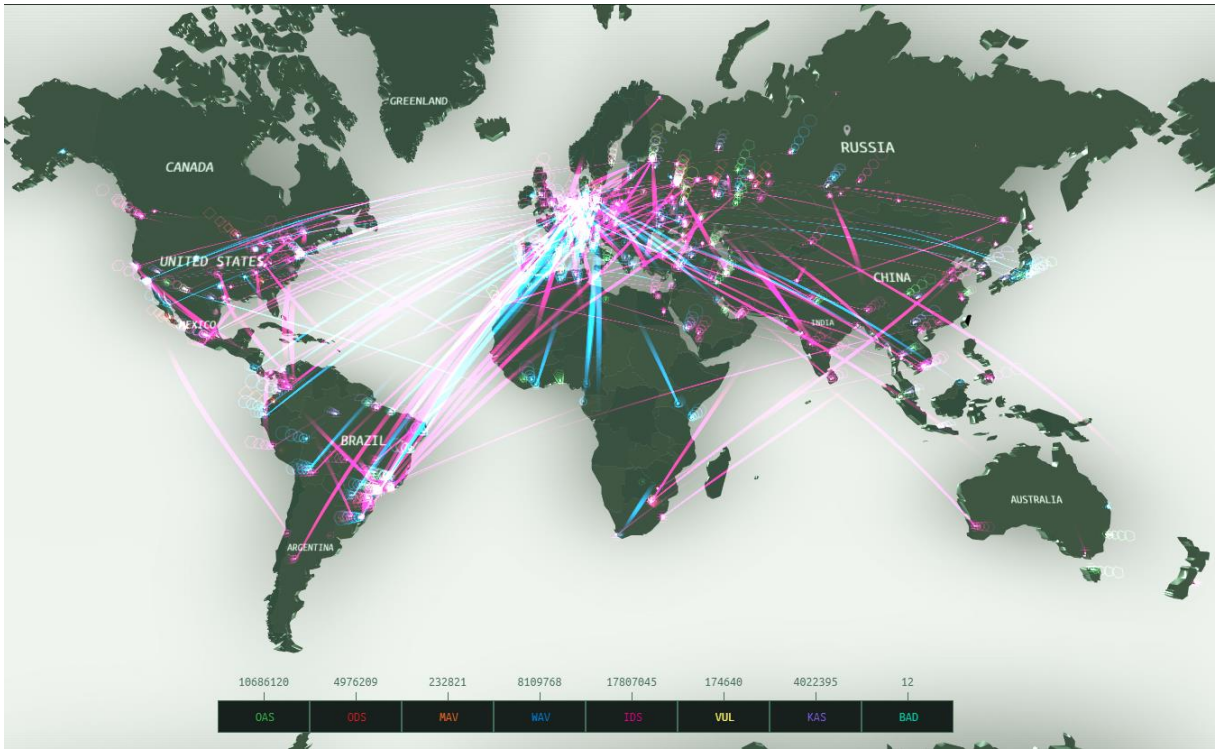
Neste capítulo será conduzida a análise das informações levantadas no Capítulo 3, a fim de se compreender melhor o fenômeno representado pela Guerra Cibernética. Serão estudados o contexto estratégico brasileiro e os casos particulares dos EUA, RPC e Brasil, buscando-se assim o estabelecimento de um cenário prospectivo que subsidie as propostas feitas no Capítulo 5. Logo, a seção 4.1 abordará aspectos gerais essenciais para a formulação do cenário. A seção 4.2 traçará a perspectiva estratégica do Brasil, enquanto a seção 4.3 conduzirá o estudo dos casos selecionados. Para tanto, a subseção 4.3.1 justificará os países selecionados para o estudo. A subseção seguinte, 4.3.2, estudará o caso dos EUA, enquanto a subseção 4.3.3 se deterá no caso da China. Já a subseção 4.3.4 analisará o caso brasileiro em contraste com os demais casos.

4.1 GENERALIDADES

A primeira consideração a ser feita é baseada na constatação de que a natureza da guerra permanece a mesma. Neste sentido, é possível vislumbrar o fenômeno da Guerra Cibernética e sua repercussão para a Guerra do Futuro no contexto da guerra como extensão da política. À essa consideração, soma-se a tendência atual do uso de atores não estatais em ações promovidas pelos estados, a chamada *proxy war*. A união desses dois conceitos pode ser vista na Guerra Cibernética, de forma mais clara, no caso chinês. O uso de *hackers* e atores não estatais para conduzirem ataques cibernéticos contra os EUA, seus principais competidores, materializa perfeitamente o emprego da Guerra Cibernética para obter ganhos políticos.

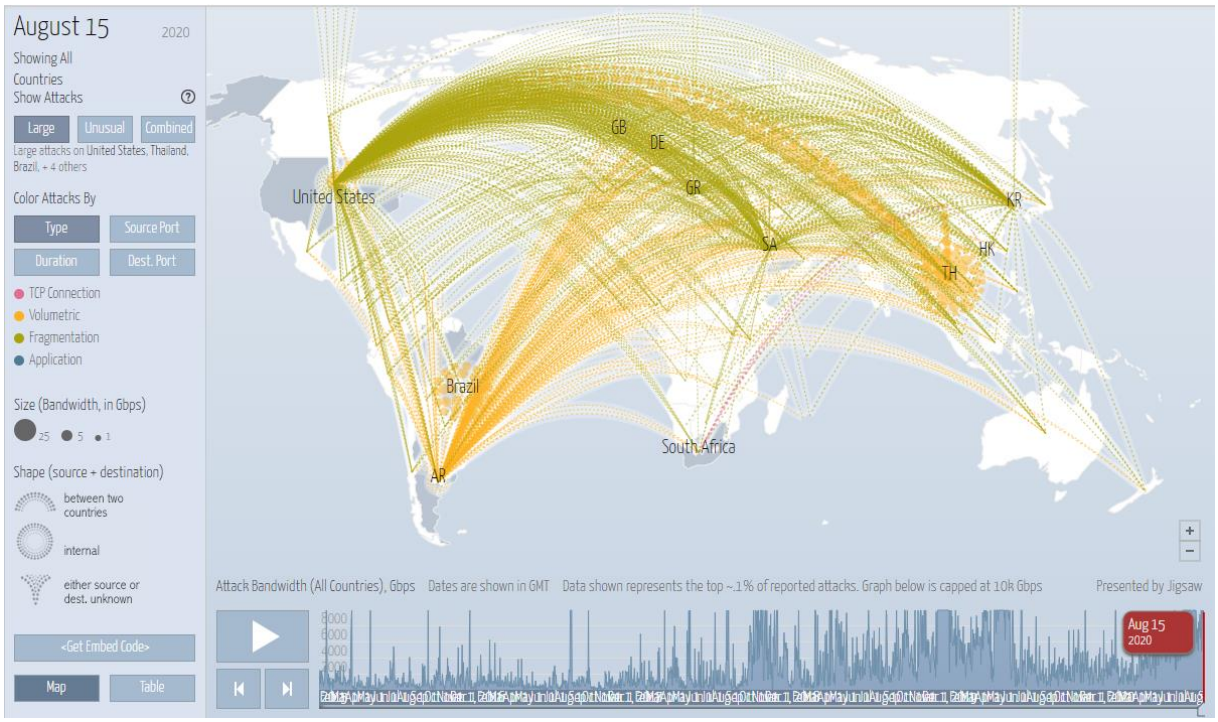
Por outro lado, a postura dos EUA apresentada na seu conceito operacional chamado Defesa Avançada e, em particular, o Engajamento Persistente, defendido pelo USCYBERCOM (LOPEZ, 2019; MYRE, 2019), mostram o Espaço Cibernético como um ambiente permanentemente contestado. Essa visão é corroborada pelos mapas exibidos na Figura 17 e Figura 18 e que mostram uma fotografia parcial e em tempo real dos ataques cibernéticos globais.

Figura 17: Fotografia parcial de ataques cibernéticos em 07/09/2020, às 18h 33 min (horário de Brasília)



Fonte: (KASPERSKY, 2020).

Figura 18: Fotografia parcial de ataques cibernéticos do tipo negação distribuída de serviço (DDoS) em 15/08/2020.



Fonte: (DIGITAL ATTACK MAP, 2020).

O que se observa, portanto, é que o mundo vivencia hoje, no Espaço Cibernético, a guerra cibernética, aqui entendida como o efetivo emprego de ações cibernéticas a fim de se obter ganhos e impor a vontade ao oponente e não como um conceito operacional. Essa guerra tem na *proxy war* uma de suas principais características, já que muitos países preferem não se envolverem diretamente, empregando para isso atores não estatais e evitando assim, as consequências legais de seus atos.

Mais do que constatar que há uma guerra em andamento no Espaço Cibernético, é preciso reconhecer que se trata de uma guerra travada em escala global. Todavia, é preciso compreender que o Espaço Cibernético não é um reflexo preciso do espaço geográfico aonde se assenta, mas sim das relações que integram os diversos estados-nação ao sistema produtivo mundial. Isso se torna evidente pela observação das figuras Figura 2, Figura 17 e Figura 18. A primeira mostra *backbones* que fazem a interligação das comunicações entre as regiões, enquanto as últimas refletem a intensidade de ataques cibernéticos. O que emerge da apreciação dessas figuras é que o Brasil se encontra fortemente integrado ao Espaço Cibernético e que a guerra ora travada tem escala global alcança todos os países que possuem relevância no Espaço Cibernético.

A identificação de que há uma guerra em andamento é importante para se analisar as posturas dos países. Um dos pilares da guerra convencional é a obtenção da iniciativa. A defesa é vista apenas como um esforço temporário cujo objetivo final é a ofensiva e a recuperação da iniciativa. No campo Cibernético esse pensamento é acentuado ao extremo. Pelas características que envolvem a contenda cibernética, a defesa já é quase uma derrota. Isso ocorre porque a reação a um ataque cibernético só ocorre quando este é detectado, o que pode já ser tarde demais e o ataque ter alcançado seu objetivo. Aliás, essa visão está por trás da postura dos EUA no que toca ao Engajamento Persistente (MYRE, 2019).

Para uma reação capaz de impor custos ao atacante, faz-se necessário o conhecimento das vulnerabilidades do adversário. Isso significa ações ofensivas permanentes, no mínimo para aquisição de informações. Logo, a manutenção da iniciativa é fundamental, o que significa atacar preventivamente adversários potenciais, a fim de retirar-lhes a liberdade de ação.

Outro ponto que merece apreciação, é a visão externada por Domingo (DOMINGO, 2016). Na visão do autor, contrário do que muitos dizem, o poderio cibernético será das grandes potências como EUA, China, Rússia e outras. Portanto, o Espaço Cibernético não se constitui, no entender do autor, numa oportunidade de equilíbrio de forças, mas sim, em mais um campo no qual a assimetria se manifesta. Esse pensamento baseia-se na análise do ataque com o vírus Stuxnet, o qual possui um nível de conhecimento tecnológico envolvido, segundo Domingo, além daquele detido por estados mais fracos. Outro ponto citado é a menor tolerância desses estados menos capazes tecnologicamente às falhas, inerentes à atividade militar. Essa baixa tolerância é justificada, uma vez que tais falhas podem levar a retaliações devastadoras das grandes potências.

Uma importante consequência é que:

> “mesmo se a utilidade de operações militares no Ciberespaço for limitada, outros estados que aspiram a hegemonia regional não têm outra escolha senão desenvolver capacidades cibernéticas como parte integral de uma força militar forte.” (tradução do autor) (DOMINGO, 2016)

Mas o potencial da Guerra Cibernética vai além. Trata-se de um verdadeiro instrumento de imposição de vontade pela força disponível mesmo no tempo de paz. Um dos elementos mais surpreendentes analisados em (BELYAEV, 2013) trata do emprego da manipulação de informações em redes sociais com a finalidade de induzir neuroses, manipular a opinião pública e causar outros efeitos sociais com potencial de enfraquecimento do país. Essa prática é uma combinação perversa de operação psicológica, guerra informacional e ações cibernéticas, oferecendo um meio eficaz e eficiente, ainda que barato, de dominação. É ainda, pela sutileza que lhe caracteriza, um ataque difícil de ser detectado e rechaçado.

4.2 ANÁLISE ESTRATÉGICA DO CONTEXTO BRASILEIRO

A PND (BRASIL, 2012) reconhece que o desenvolvimento do Brasil e sua projeção internacional pode conduzi-lo a um conflito de interesses com atores de diversas naturezas. O documento salienta, ainda, o interesse que a Amazônia brasileira desperta nas demais nações. A internacionalização da Amazônia nacional é assunto que sempre retorna à mídia, contanto com apoio de países

desenvolvidos, ambientalistas, ONG e organismos supranacionais (MATTOS, 2005; NEVES e colab., 2019). Assim, o contexto brasileiro é mercado pela incidência do interesse de potências extrarregionais, em especial as desenvolvidas.

Mas a análise do contexto nacional precisa ser conduzida com base no entorno estratégico do Brasil, conceito esse estabelecido na PND. A Política define-o como uma área “que extrapola a região sul-americana e inclui o Atlântico Sul e os países lindeiros da África, assim como a Antártica” (BRASIL, 2012). No entanto, uma análise dos países formadores do nosso entorno estratégico na América do Sul revela a presença de diversas potências extrarregionais, conforme se observa na Figura *19*.

Figura 19: Principais potências extrarregionais no entorno estratégico do Brasil na América do Sul.

Fonte: o autor.

A Tabela 4 apresenta essas potências, contextualizando-as no entorno nacional.

Tabela 4: Principais potências extrarregionais na América do Sul e seu contexto de atuação.

Países externos à América do Sul	**Presença na América do Sul**	**Contexto da presença**
França	Guiana Francesa	Território ultramarino (“Les territoires ultramarins | Ministère des Outre-mer”, 2016)
Inglaterra	Ilhas Falklands	Território ultramarino (“Falkland Islands (British Overseas Territory) travel advice - GOV.UK”, [S.d.])
	Guiana	Commonwealth (COMMONWEALTH SECRETARIAT, 2018)
EUA	Colômbia	Cooperação militar (permissão de uso temporário de bases militares no país) (FIGUEIRA, 2018)
	Peru	Cooperação militar (permissão entrada de tropas em solo peruano) (FIGUEIRA, 2018)
	Chile	Cooperação militar (permissão entrada de tropas em solo chileno) (FIGUEIRA, 2018)
	Argentina	Cooperação militar (instalação de duas bases militares) (FIGUEIRA, 2018)
	Guiana	Ajuda humanitária (pressão por vantagens militares)
China	Venezuela	Apoio político e empréstimos. (“Quem apoia Maduro ou Guaidó: entenda o xadrez político da crise na Venezuela - Jornal O Globo”, [S.d.])
Rússia	Venezuela	Apoio político, empréstimos e cooperação militar. (“Quem apoia Maduro ou Guaidó: entenda o xadrez político da crise na Venezuela - Jornal O

Países externos à América do Sul	Presença na América do Sul	Contexto da presença
		Globo", [S.d.]) ("Rússia anuncia ampliação de cooperação militar com Venezuela | Notícias internacionais e análises | DW | 08.02.2020", [S.d.])

Fonte: o autor.

O conceito de entorno estratégico, porém, precisa ser expandido para o Espaço Cibernético, no qual se tem, então, o Entorno Estratégico Virtual. Contudo, o conceito precisa ser ajustado. Define-se, assim, Entorno Estratégico Virtual como o conjunto formado pelos atores que atendem à pelo menos uma das seguintes condições:

1. Proximidade física do território nacional;
2. Proximidade virtual do território nacional;
3. Capacidade de conduzir ações cibernéticas contra o País estando distante física ou virtualmente do território nacional.

A primeira condição é relevante pela facilidade que a proximidade física traz para a condução de ações cibernéticas. Uma vez que um ator esteja fisicamente próximo, ele pode se valer tanto da infraestrutura instalada (Figura 4) quanto de sua própria capacidade de comunicação para ultrapassar os limites territoriais e executar ataques cibernéticos.

A segunda condição também está relacionada com a facilidade de se realizar ataques cibernéticos, contudo o que contribui para facilitar os ataques é a existência de linhas diretas de comunicação (infovias) com grande capacidade de tráfego entre o ator e o País (Figura 2 e Figura 3).

A última condição é afeta àqueles atores que, mesmo distantes física ou virtualmente, possuem a capacidade de conduzir ataques cibernéticos ao País e motivos que possam levá-los a desencadear tais ações.

Embora não seja objetivo desse trabalho apresentar uma lista exaustiva dos atores estatais que formam o entorno estratégico virtual brasileiro, pode-se listar como exemplos de países formadores do mesmo o Canadá, EUA, União Europeia, Rússia e China.

Observando-se, novamente, a Figura *19*, percebe-se que tais países se fazem presentes no entorno estratégico brasileiro na América do Sul. Nota-se, ainda, um cinturão de contenção dos EUA envolvendo o Brasil. Sobre os EUA, merece especial registro a declaração do candidato democrata à presidência dos EUA, Joe Biden que afirmou que:

> "começaria imediatamente a organizar o hemisfério e o mundo para prover US$ 20 bilhões para a Amazônia, para o Brasil não queimar mais a Amazônia. (A comunidade internacional diria ao Brasil) aqui estão US$ 20 bilhões, pare de destruir a floresta. E se não parar, **vai enfrentar consequências econômicas significativas**." (grifo do autor) (MORI, 2020)

Portanto, a análise estratégica do contexto brasileiro mostra a presença de potências extrarregionais desenvolvidas e em desenvolvimento no entorno estratégico nacional. Essas nações formam, também, o entorno estratégico virtual do Brasil. Tais potências estão entre as maiores economias mundiais, os maiores poderios bélicos (ver Tabela 5) e algumas deram, em certo momento, declarações defendendo a relativização da soberania brasileira sobre a floresta amazônica.

Dentre as potências listas, todas possuem capacidade cibernética, merecendo destaque os EUA e a China, cujo emprego ofensivo de ações de guerra cibernética mostra-se abundante e livre de amarras. Nesse contexto, o entorno estratégico virtual consiste-se num espaço altamente contestado e marcado por disputas e buscas por projeções de poder.

Finalmente, pode-se concluir que tanto o entorno estratégico brasileiro real quanto o virtual é formado por potências de primeira grandeza externas ao bloco sul-americano. A presença desses países e os interesses conflitantes que alguns possuem com relação ao Brasil posiciona-os, no mínimo, como competidores no campo real. As ações cibernéticas gozam de relativo anonimato e, como visto, os países encontram nesse campo a liberdade de ação que não mais possuem no campo real para impor sua vontade. Logo, estas nações tendem a representar ameaça ao Brasil no campo virtual.

4.3 ESTUDO DE CASOS

Nesta seção serão estudados casos que contribuam para a avaliação da situação brasileira. Os casos serão analisados considerando-se os seguintes fatores: estrutura militar de cibernética, pensamento em defesa cibernética, tendências relevantes para o cenário prospectivo e possíveis impactos para o Brasil.

Esse estudo de caso começará pela apresentação da justificativa dos casos selecionados, feita na subseção 4.3.1. O estudo do caso dos EUA será apresentado na subseção 4.3.2 e o caso chinês na 4.3.3. Finalmente a subseção 4.3.4 traçará um paralelo entre os casos e estudados e a situação brasileira.

4.3.1 **Justificativa da escolha**

Para seleção dos casos a serem estudados, buscou-se selecionar países cuja influência tenha significativo peso na Guerra do Futuro. Isto é, países que sejam delineadores de tendências. A seleção foi feita, então, com base em dois parâmetros: poder militar e produção científica. A escolha do poder militar como indicador decorre da visão de que países com maior gasto militar são mais capazes de definir tendências para a Guerra do Futuro. Além disso, o gasto militar é um grande indutor de P&D (SMITH, 2019) (MORETTI e colab., 2019), o que influi na capacidade cibernética de uma nação, dado o viés massivamente tecnológico da Guerra Cibernética.

Tendo o poder militar como fator dominante, foram selecionados os 11 (onze) países com maior poder militar com base no gasto financeiro a partir da relação elaborada pelo *Stockholm International Peace Research Institute*[16] (SIPRI). Depois, esses países foram correlacionados com o índice do sítio Global Firepower, o qual inclui mais elementos no cálculo do poder militar. Esses países tiveram, então, sua produção científica levantada e o resultado encontra-se na Tabela 5, que mostra as posições de cada país segundo os índices usados. A Tabela 6 mostra os mesmos países de acordo com os valores de cada índice.

O ranque de produção científica foi elaborado incluindo todas as múltiplas áreas do conhecimento. Não obstante, os países em tela são lideranças no desenvolvimento tecnológico atual. Além disso, produtos de defesa usualmente

[16] https://www.sipri.org/

possuem alto valor agregado e grande interdisciplinaridade, daí a conveniência de um olhar abrangente sobre a produção científica.

A seleção dos EUA é imediata e óbvia. Trata-se da maior potência militar e econômica do mundo, e uma das maiores no campo científico. A seleção do segundo país, contudo, demanda discussão. Inicialmente, deve-se observar que a China é o segundo país com maior gasto militar do mundo, caindo para a terceira posição quando se considera o índice amplo do sítio Global Firepower[17]. Neste último, é a Rússia que ocupa a segunda colocação. Todavia, como se observa na Tabela 6, o gasto militar da Rússia é aproximadamente um quarto do gasto chinês. Assim, do ponto de vista militar, considerando-se que o gasto é relevante para essa análise, a China é o melhor candidato para ter seu caso estudado.

Tomando-se a produção científica, a China se consolida como segundo caso a ser estudado, pois a Rússia ocupa a décima (Scimago Journal & Country Rank[18]) ou a décima oitava posição (Nature Index[19]).

Tabela 5: Ranque de países segundo o poderio militar e produção científica.

País	**Poder Militar**		**Produção Científica**	
	SIPRI (2019) (PERLO-FREEMAN e colab., 2016)	**Global Firepower (2020)** (GLOBAL FIRE POWER, 2020)	**Nature Index (2019)** (SPRINGER NATURE LIMITED, 2019)	**Scimago Journal & Country Rank (2019)** (SCIMAGO JOURNAL AND COUNTRY RANK, 2019)
EUA	1	1	1	2
China	2	3	2	1
Índia	3	4	13	4
Rússia	4	2	18	10
Arábia Saudita	5	17	29	29
França	6	7	6	8
Alemanha	7	13	3	5
Reino Unido	8	8	4	3
Japão	9	5	5	6
Coreia do Sul	10	6	9	13
Brasil	11	10	23	14

Fonte: o autor.

[17] https://www.globalfirepower.com/
[18] https://www.scimagojr.com/
[19] https://www.natureindex.com/

Tabela 6: Valores dos índices do poderio militar e produção científica.

País	Poder Militar		Produção Científica	
	SIPRI (2019) (bilhões de dólares) (PERLO-FREEMAN e colab., 2016)	**Global Firepower (2020)** (menor, melhor) (GLOBAL FIRE POWER, 2020)	**Nature Index (2019)** (SPRINGER NATURE LIMITED, 2019)	**Scimago Journal & Country Rank (2019)** (nº de documentos indexados) (SCIMAGO JOURNAL AND COUNTRY RANK, 2019)
EUA	732	0,0606	28.329	678.197
China	261[20]	0,0691	15.589	684.048
Índia	71,1	0,0953	1.513	187.014
Rússia	65,1	0,0691	1.447	11.820
Arábia Saudita	61,9[21]	0,3034	495	27.715
França	50,1	0,1702	4.896	118.951
Alemanha	49,3	0,2186	8.776	183.640
Reino Unido	48,7	0,1717	7.636	212.519
Japão	47,6	0,1501	4.918	132.308
Coreia do Sul	43,9	0,1509	2.285	89.544
Brasil	26,9	0,1988	949	84.887

Fonte: o autor.

Do exposto, os países selecionados para estudo foram os EUA e a China. Tal seleção corrobora de forma objetiva que ambos os países são os principais competidores militares, produtores de tecnologia e influenciadores da Guerra do Futuro.

4.3.2 **Análise do caso dos Estados Unidos da América do Norte**

Analisar o caso dos EUA não é nenhuma surpresa. O país é a maior potência econômica e militar da atualidade e a única com capacidade de atuação global. O uso dos Estados Unidos como caso de estudo de interesse do Brasil pode ser objetado pela crença de que a enorme disparidade entre ambos os países torna o estudo inadequado para a realidade brasileira. Tal argumento, porém, não merece prosperar, pois além de revelar uma visão obsoleta, típica da era industrial, deixa de considerar uma série de fatores. Brasil e EUA guardam, por um lado, diversas similaridades, em termos de riqueza e extensão territorial, ausência de conflitos no seu entorno, formação cultural diversificada e outros. Mas, ainda mais importante, fruto da análise estratégica do contexto brasileiro, os EUA devem ser considerados

[20] Valor estimado
[21] Valor estimado

um provável competidor do Brasil em sua aspiração de estabelecer-se como líder regional. Exemplos em que os EUA frustraram ambições do Brasil fogem ao propósito desse trabalho, mas podem ser facilmente encontradas em buscas pela Internet.

Se os EUA são competidores no campo real, no campo virtual certamente são ameaças, justamente pelo fato de poderem, no espaço cibernético, atuar com mais liberdade de ação. Nesse caso, a situação tem alguma semelhança com a defesa antiaérea. Se nela, só se tem soberania sobre o espaço aéreo que pode ser defendido, na Cibernética só se é soberano se há capacidade de se identificar e retaliar ações cibernéticas. E como visto, a correta identificação da origem dos ataques e sua responsabilização legal são consideravelmente difíceis.

Pelas considerações expostas, os EUA são um importante caso definidor de tendência, sendo fonte legítima de informação para balizar a abordagem brasileira.

4.3.2.1 Estrutura militar de cibernética

Os EUA possuem uma robusta e bem organizada estrutura militar de cibernética. O seu principal órgão, USCYBERCOM, foi gestado na NSA, usufruindo da proximidade com a comunidade de inteligência. Os benefícios foram muito além da soma das partes, criando uma estrutura de cibernética, no nível estratégico, que amalgamou com sucesso as duas áreas. O USCYBERCOM é uma organização robusta, que conta com a participação de unidades de cibernética das Forças Singulares, construindo uma verdadeira sinergia de ações.

As Forças Singulares possuem suas próprias unidades, voltadas para ações nos níveis táctico e operacional (o USCYBERCOM também atua no operacional). O caso do U.S. Army é mais emblemático, pois o exército criou um ramo de cibernética, mantendo-o separado da arma de sinais. Isso permite a formação de pessoal altamente especializado e a formação de uma cultura própria de combate cibernético. Essa iniciativa permite, ainda, o emprego da cibernética no próprio teatro de operações, além de estender sua atuação pelas zonas de defesa e de interior.

A proteção de infraestruturas e da base industrial dos EUA é conduzida pelo USCYBERCOM, que nesse caso atua em cooperação com outras agências e com as indústrias e a sociedade civil. Ou seja, a estrutura militar possui uma bem

consolidada verticalização, alcançando todos os níveis de ação (a atuação política fica por conta do DoD). Ela também possui significativa penetração horizontal, sendo capaz de arregimentar a indústria e a sociedade civil.

Trata-se de uma estrutura militar bem consolidada, ampla, atuante e com bom nível de maturidade, encontram-se em condições de pleno emprego.

4.3.2.2 Pensamento em defesa cibernética

O pensamento de defesa cibernética dos EUA se apresenta bem estruturado e amadurecido. O país possui uma estratégica de cibernética, além de doutrina voltada para a área. Os documentos são revisados e o Congresso dos EUA acompanha as formulações de mais alto nível e os resultados, revelando boa integração com o nível político. Essa integração é importante, pois um dos pontos importantes da defesa cibernética dos EUA é a capacidade de impor custos ao adversário pelo meio jurídico. Assim as leis fazem parte da primeira linha de defesa. Em último, encontra-se o próprio poder militar convencional, deixando claro que ataques cinéticos podem ser conduzidos como retaliação à ataques cibernéticos.

A estratégia dos EUA faz uma acurada análise do cenário internacional, identificando ameaças e prevendo maior dificuldade da estratégia de dissuasão, ambiente altamente contestado no espaço cibernético e a necessidade de se atuar preventivamente. Esse último pensamento recebeu o nome de Defesa Avançada e materializa a visão de que, no espaço cibernético, defender já é uma derrota.

Além disso, a abordagem dos EUA é ampla, extrapolando os campos científico-tecnológico e militar. O entendimento do país é que a defesa começa pela imposição de custos através da judicialização dos ataques cibernéticos sofridos. Com isso, o USCYBERCOM possui um quadro jurídico destinado a suportar a legalidade das ações, e a atuar na retaliação. O campo político é envolvido de duas formas, na formulação de leis que fortalecem a capacidade legal de os EUA se protegerem de, e retaliarem, ataques cibernéticos. A outra forma, é através da atuação em organismos supranacionais seja para buscar a condenação aos ataques, seja para desencadear ações cinéticas de retaliação.

O pensamento em defesa cibernética mostra-se, assim, evoluído, com boa aderência às estruturas e à realidade dos EUA e bem refletido em sua estrutura militar.

4.3.2.3 Tendências relevantes para o cenário prospectivo

Pode-se extrair, do estudo do caso dos EUA, 5 tendências que possivelmente delinearão o futuro da guerra cibernética e aqui são generalizadas. Em primeiro, nota-se a tendência já consolidada de enxergar a guerra cibernética como uma atividade multidisciplinar multinível. As ações se desenrolam na esfera militar, técnica, jurídica e abarcam os níveis político, estratégico, operacional e táctico.

Em segundo, no campo cibernético a mera existência da capacidade ofensiva de cibernética será considera justificativa para ataques preventivos. Como demonstrado, a possibilidade de uma ação ofensiva por um outro estado ou grupo é uma ameaça intolerável, já que um ataque, se bem sucedido, só será detectado quando for tarde demais, e se for notado. A não anulação dessa capacidade no adversário ou competidor, antes do seu, portanto, oferece sério risco à soberania cibernética do país.

Em terceiro, a atuação defensiva é vista como uma fraqueza com grande possibilidade de derrota para o país que assim atuar. Essa tendência complementa a segunda, e diz respeito à dificuldade de se identificar certos tipos de ataques e ao fato de que um ataque cibernético bem sucedido já pode ser causador de dano significativo. O caso *stuxnet* é um bom exemplo.

Em quarto, as ações cibernéticas serão marcadas por um nível cada vez maior de emprego tecnológico, exigindo o emprego de pessoal cada vez mais especializado. O emprego no nível tático deve aumentar, com o aumento da densidade tecnológica no teatro operacional.

Outra tendência identificada é o aumento da disputa por projeção de poder no espaço cibernético. Os conflitos tendem a se acirrar na medida em que China e Rússia buscam contestar a hegemonia dos EUA. O espaço cibernético oferece as condições ideais para a atuação anônima, o que deve atrair também outros atores, engajados pelas mais diversas causas e interesses.

4.3.2.4 Possíveis impactos para o Brasil.

Ao abordar a guerra cibernética como uma atividade multidisciplinar multinível, os principais elementos que se destacam com possibilidade de

repercussão para o Brasil são o jurídico e o político. Ambos são historicamente usados como forma de impor a vontade das nações centrais sobre as periféricas através de mecanismos aceitos internacionalmente.

Politicamente, pode-se esperar o apelo pela celebração de acordos e tratados que visem a coibir ou limitar atividades cibernética, mas que na prática servirá apenas para tolher o desenvolvimento da capacidade cibernética de entrantes no jogo. Pode-se, ainda, esperar nesse ponto de atuação, a ocorrência de pressões a fim de que o País mantenha uma postura essencialmente defensiva. As ações políticas tendem a se dar em desfavor do Estado brasileiro e de sua segurança e devem contar com o apoio coeso das nações centrais, Rússia e China.

Juridicamente, pode-se esperar o emprego de medidas contra empresas, cidadãos brasileiros e interesses do país, a fim de enfraquecer o desenvolvimento da capacidade cibernética e evitar-se a coesão nacional em torno do tema. As pressões jurídicas podem incluir, sem se limitar, à medidas no campo da propriedade industrial e do comércio.

O caráter eminentemente ofensivo adotado no espaço cibernético tende a ter, em algum momento, o Brasil como alvo. As declarações de Joe Biden ilustram, sem esgotar, a questão. No futuro, é pouco provável que o Brasil consiga manter-se fora dos combates cibernéticos, especialmente os velados. Também se afigura como provável a ampliação do grupo de nações que devem conduzir ações cibernéticas contra o País, com base em pretextos como a Amazônia e o meio-ambiente ou outros interesses nacionais.

O ambiente cibernético que o Brasil vai encontrar no futuro, além de progressivamente mais contestado, deverá ser formado por atores cada vez mais técnicos e especializados, com ferramentas mais complexas e evoluídas. Tal situação tende a exigir bastante da estrutura militar de cibernética do Brasil e a estressar o sistema, com repercussões difíceis de se antever.

4.3.3 **Análise do caso da República Popular da China**

Não sendo a RPC uma democracia e não possuindo o país uma transparência desejável, torna-se mais difícil extrair informações significativas. Entretanto, como o país é um dos principais competidores dos EUA e frequentemente desperta o interesse de pesquisadores e estudiosos, uma observação indireta da RPC se faz possível.

Analisando a postura chinesa diante do Brasil, não se identifica de pronto nenhuma ameaça. A RPC não oferece críticas ao País ou à sua gestão ambiental, mas obtém do Brasil as *commodities* que necessita. Paralelamente, a China enfrenta os EUA num jogo de poder, fazendo com que se possa esperar pouco ou nenhum apoio da RPC ao Brasil, salvo se seus interesses forem diretamente ameaçados. Não obstante, o Brasil deve reconhecer que, num conflito de interesses entre a China e o Brasil, é provável que a RPC não ceda, buscando impor sua vontade ao Brasil, entre outros meios, pela cibernética.

4.3.3.1 Estrutura militar de cibernética

A RPC, de maneira similar aos EUA, possui uma robusta e bem organizada estrutura militar de cibernética. Fruto da importância estratégica que o país deu ao ciberespaço e ao setor espacial, o Exército de Libertação Popular foi reestruturado de forma a ter capacidade de cibernética. Para isso, foram criadas unidades específicas, como a brigada “Blue Force”. Há, também, grande integração com o campo científico-tecnológico.

A estrutura chinesa goza da vantagem de estar inserida num sistema autoritário e altamente estável, o que lhe confere destreza e agilidade. A RPC não se limita a desenvolver uma estrutura, mas tem testado essa mesma estrutura contra diversos países, em especial os EUA. Dessa maneira, a estrutura militar de cibernética é reconhecidamente um meio de imposição da vontade nacional chinesa mesmo em tempo de paz e na ausência de conflitos.

Além do pessoal militar, a estrutura chinesa faz amplo uso de hackers, sem ligação oficial com o governo chinês. Isso confere a capacidade de cibernética chinesa os meios para operar clandestinamente, além de manter o sistema constantemente atualizado com mão-de-obra altamente especializada, recrutada conforme a necessidade.

Como é um sistema que não se prende às práticas legais internacionais, a china impõe à sua estrutura de cibernética o desenvolvimento de capacidades de operações psicológicas com as mais diversas matizes, visando a desestabilização de nações competidoras.

A estrutura militar de cibernética chinesa também possui, a similaridade dos EUA, ótima horizontalização, tendo grande capacidade de envolver as indústrias, os demais setores estatais e a sociedade.

Com base nessa discussão e assentado no exposto na subseção 3.3, percebe-se que a China possui uma estrutura coesa, robusta, com boa abrangência horizontal. A estrutura tem acesso a pessoal altamente especializado, recrutado diretamente da sociedade civil (*hackers*), capacidade de operar clandestinamente e grande capacidade de conduzir operações psicológicas de desestabilização.

4.3.3.2 Pensamento em defesa cibernética

O pensamento chinês sobre o assunto defesa cibernética é, de maneira idêntica ao dos EUA, bem estruturado e amadurecido. A RPC enxerga no espaço cibernético um espaço vital para o crescimento chinês e um meio de contestar e mudar a ordem mundial atual.

A mentalidade chinesa tem como visão de futuro a resolução com vitória de todas as guerras internacionais até meados do século XXI. Nesse sentido, a RPC vem efetivamente empregando seu poder militar cibernético, com aval do campo político, a fim de obter seus interesses.

Um ponto que merece destaque do pensamento chinês é o emprego da cibernética para operações psicológicas que buscam gerar conturbações sociais. Tal uso, que talvez não seja muito bem visto no ocidente, é perseguido pelo governo chinês.

4.3.3.3 Tendências relevantes para o cenário prospectivo

Do caso chinês exposto na subseção 3.3, pode-se tirar como uma tendência o emprego de *hackers* e atores não estatais. Tais atores conferem maior liberdade de ação, pois dificilmente podem ser ligados aos estados-nação. Adicionalmente, pode-se lançar mão de pessoal altamente especializado, o que se alinha com a tendência do caso anterior da maior especialização técnica do pessoal envolvido nas ações cibernéticas.

Esse viés traz como corolário a tendência do aumento de operações clandestinas e, por conseguinte, do emprego da cibernética com fins de desestabilização ou manipulação social de outras nações. Deve-se esperar que a imposição da vontade das nações centrais, pelo menos às com tradição de desrespeitar normas internacionais, se dê por meio da manipulação social.

Também ratificando uma tendência do caso dos EUA, deve-se esperar que o espaço cibernético se torne um campo de franca disputa, com ações cibernéticas sendo permanentemente conduzidas. Um verdadeiro campo de batalha, no qual se desenrolará uma guerra virtual.

Outro viés confirmado é o aumento da especialização técnica e do nível tecnológico envolvido nas ações cibernéticas. Ao empregar *hackers* “profissionais” a China recruta mão-de-obra que não é apenas executora, mas possui habilidades técnicas que permitem a adaptação aos desafios encontrados durante a ação. A previsibilidade na condução tende a cair, valorizando os atores que possuam conhecimento técnico.

4.3.3.4 Possíveis impactos para o Brasil.

O Brasil é um país particularmente vulnerável às operações cibernéticas clandestinas e à manipulação social. O país não apresenta leis robustas que permitam impor retaliações a esses tipos de ataque, utiliza urnas eletrônicas no seu sistema eleitoral e a guerra de narrativas dificilmente é debelada.

Por outro lado, o emprego de mão de-obra qualificada e o aumento da densidade tecnológica, podem ampliar a desvantagem brasileira, haja vista o *gap* tecnológico entre o País e as potências centrais.

Também ratificando o estudo do caso dos EUA, a tendência da conflagração de uma ampla guerra cibernética não deve poupar o Brasil, que se verá envolvido pelo conflito. A marca desse conflito, porém, serão ações clandestinas e a constante negação dos seus autores, tornando difícil, dados a mentalidade e o sistema legal brasileiro, a defesa e a dissuasão.

4.3.4 **Análise do caso da República Federativa do Brasil em contraste com o caso dos EUA e da RPC**

De maneira similar aos EUA e à RPC, o Brasil é um país com vasto território e muitas riquezas naturais. Entretanto, não possui economia e nem poder militar que se compare a qualquer um desses. O Brasil é uma democracia em amadurecimento e um país pacifista.

Entretanto, conforme estipulado em sua PND, o Brasil precisa estar preparado para defender os seus interesses. Isso pode ser confirmado na postura internacional com relação a questões sensíveis para a nação brasileira, como a soberania nacional.

É neste contexto que a capacidade cibernética brasileira se insere, buscando garantir a soberania nacional no espaço cibernético, proteger os interesses nacionais e contribuir para a dissuasão. O Brasil não nomina competidores e nem identifica aqueles que ameaçam os interesses do País, contudo, na PND pode-se entrever que o Brasil reconhece a existência desses, como fica patente nesse excerto: “Nesse contexto de múltiplas influências e de interdependência, os países buscam realizar seus interesses nacionais, podendo encorajar alianças ou **gerar conflitos de variadas intensidades.**” (grifo do autor) (BRASIL, 2012).

4.3.4.1 Estrutura militar de cibernética

A estrutura militar de cibernética brasileira é consideravelmente mais modesta do que a da RPC e EUA. Entretanto, mostra-se bem organizada e com papéis bem definidos. No caso brasileiro, a estrutura é liderada pelo Exército Brasileiro, mas este, ciente da necessidade de amplo envolvimento do setor de Defesa, conseguiu motivar o envolvimento de todas as Forças Singulares.

No Brasil, a condução das atividades de defesa cibernética são fortemente assentadas no ComDCIber, embora haja previsão de ações no nível táctico. Logo, a estrutura mostra alguma verticalização, não sendo claro que haja o mesmo grau de verticalização visto nos EUA e na RPC.

Os militares brasileiros estão cientes da necessidade de envolvimento da sociedade civil e demais áreas do governo. Para isso conduzem ações diversas com o intuito de ampliar a horizontalização da estrutura, mas tais iniciativas ainda não frutificaram. O Congresso Nacional tem se envolvido timidamente, realizando acompanhamento e buscando apoiar algumas iniciativas. Apesar de ainda não

terem trazido o retorno esperado, mostram uma postura acertada e coerente com a Guerra do Futuro.

No que toca ao pessoal, a estrutura militar de cibernética brasileira prescinde de importantes recursos humanos constituídos pelo QEM. Isso torna a estrutura menos apta a se adaptar e evoluir com o setor de cibernética e tende a prejudicar sua eficácia.

4.3.4.2 Pensamento em defesa cibernética

A inserção do setor cibernético como um dos três setores estratégicos de Defesa, ao lado do espacial e do nuclear, mostra a importância que o Brasil dá ao espaço cibernético no escopo da Defesa e Desenvolvimento Nacionais.

O pensamento em defesa cibernética no Brasil está bem estruturado e possui documentação que serve para realizar o preparo e o emprego. Essa documentação formaliza a estratégia, a doutrina e o emprego da cibernética. Assim, o Brasil mostra-se alinhado com os EUA e a China.

No que toca ao conteúdo dessa documentação, porém, o País destoa significativamente em vários pontos. Em primeiro, o caráter pacifista do país confere ao pensamento na área de cibernética uma visão primordialmente defensiva, com o país buscando identificar e conter os ataques. O emprego da ofensiva é colocado apenas no contexto de apoio às operações e quando autorizado pelo poder político. Assim, mesmo se o Brasil identificar um competidor com capacidade e motivação para conduzir um ataque, a tendência não é realizar um ataque preventivo.

Além desse fato, conforme os conceitos extraídos dos manuais mostraram, o Brasil enxerga a cibernética apenas como uma forma de afetar a estrutura de Comando e Controle adversária. Tal visão é significativamente mais restritiva que à dos EUA e da China.

4.3.4.3 Tendências relevantes para o cenário prospectivo

Há duas tendências que podem ser identificadas no caso brasileiro com desdobramentos no cenário prospectivo. A primeira é que o caráter pacifista deve continuar limitando tanto o pensamento sobre guerra cibernética quanto a estrutura

militar envolvida. Ambos devem ser continuamente afetados, mantendo ou ampliando a derivação destes com relação a abordagem das potências centrais.

O outro viés, ainda relacionado com o primeiro, é a busca por celebração de acordos internacionais que venham a restringir o emprego e o desenvolvimento da capacidade cibernética. Tal postura acentuará os limites impostos a capacidade cibernética nacional sem, contudo, afetar possíveis competidores como os listados na seção 4.2.

4.3.4.4 Possíveis impactos para o Brasil.

Os impactos para o Brasil vão, principalmente, no sentido de comprometer sua segurança cibernética. O afastamento do Quadro de Engenheiros Militares (QEM) da área de cibernética dá um perfil mais executor à estrutura militar de cibernética, com menor capacidade de adaptação às constantes mudanças vividas no espaço cibernético.

O aumento do perfil altamente especializado nos ataques visto nos casos dos EUA e China, também é observado no caso de atores não estatais. Isso é demonstrado no artigo chamado "*Hackers are getting more hands-on with their attacks. That's not a good sign*" (PALMER, 2020), que revela a popularização desse tipo de ataque.

No médio prazo, há risco de tanto a estrutura militar de cibernética, quanto o pensamento brasileiro na área se desatualizarem.

5 UMA PROPOSTA DE TRANSFORMAÇÃO PARA O EXÉRCITO BRASILEIRO NO CAMPO DA GUERRA CIBERNÉTICA

O Espaço Cibernético, pelas razões exaustivamente expostas nesse trabalho, pode se configurar em um vetor de ameaças à Segurança Nacional. Isso significa que o novo espaço tem potencial para afetar o cumprimento da missão constitucional do Exército Brasileiro. Ao mesmo tempo, a busca de diversos países pelo protagonismo cibernético, mostra que o Espaço Cibernético tem papel essencial no concerto das nações.

Como foi visto, o Espaço Cibernético oferece uma atraente oportunidade para imposição de vontades em um mundo no qual isso se tornou cada vez mais custoso de se fazer pelos meios tradicionais. O campo cibernético também favorece aqueles que detém grande capacidade tecnológica, fazendo com que, por um lado, o hiato tecnológico entre os países aumente de importância. A cibernética não é, em um primeiro momento, amplificadora desse hiato, mas certamente tende a estimulá-lo, à medida em que se percebe o valor do espaço cibernético.

Portanto, o domínio da arte da Guerra Cibernética pode dar ao Exército, e por conseguinte ao Brasil, importante elemento dissuasório. Além de se alinhar com a Doutrina de Defesa Nacional, o Processo de Transformação do Exército ora em curso torna o momento apropriado para que o EB reflita sobre sua abordagem relativa à Guerra Cibernética.

Para elaborar uma proposta de transformação que possa refletir e abordar as considerações levantadas nesse trabalho, utilizar-se-á da análise SWOT[22] (*Strengths*, *Weakness, Oportunities*, *Threats*).

[22] A análise SWOT é uma ferramenta utilizada para diagnóstico de cenário, que busca levantar as Forças (S), Fraquezas (W), Oportunidades (O) e Ameaças (T) a que uma organização está exposta. Dessa forma, a ferramenta possibilita melhorias internas e externas, ao comunicar aos decisores esses pontos levantados (CRUZ e colab., 2017). Externamente, busca identificar oportunidades que possam se converter em benefícios para a organização. Já as ameaças são tudo aquilo que está presente no exterior e tem capacidade de prejudicar a organização e seus objetivos. Internamente a SWOT identifica as forças e fraquezas de uma organização. As forças são tudo que a organização tem e que contribuem de forma positiva para a consecução de seus objetivos, devendo ser reforçadas e mantidas. Já as fraquezas são fragilidades internas que podem vir a prejudicar a organização e/ou seus objetivos.

No caso do Exército Brasileiro, as oportunidades representam identificações feitas no cenário prospectivo que podem contribuir para o cumprimento de sua missão constitucional. As ameaças, por sua vez, representam aquilo que tem capacidade de prejudicar esse cumprimento. Por isso, são elementos importantes no direcionamento e na reavaliação da transformação do EB.

Para o EB, essa ferramenta tem, assim, a capacidade de identificar seus elementos que contribuem positivamente para sua missão. Ao mesmo tempo, permite ao Exército Brasileiro olhar para o que precisa ser aprimorado ou modificado. É, portando, valiosa ferramenta para subsidiar a formulação dessa proposta, pois permite aos decisores formularem políticas e estratégias que melhorem a vantagem competitiva do EB e seu desempenho organizacional.

A aplicação da análise SWOT produziu a Tabela 7, que sumariza as Forças, Fraquezas, Oportunidades e Ameaças, quando considerada a missão do Exército Brasileiro à luz do cenário prospectivo da Guerra do Futuro levantado. Não se pode deixar de registrar que o cenário prospectivo pode não ocorrer ou ocorrer com algumas diferenças do que aqui foi elaborado. Por isso faz-se mister o constante acompanhamento dos fatos portadores de futuro a fim de se manter esse cenário e a matriz SWOT atualizados.

Tabela 7: Análise SWOT do cenário prospectivo e do referencial teórico.

		FATORES POSITIVOS		FATORES NEGATIVOS
FATORES INTERNOS	FORÇAS (S)	1. Existência de uma estrutura militar de cibernética bem organizada e estabelecida 2. Existência de normas e documentos que formalizam o pensamento militar sobre Guerra Cibernética 3. Realização de iniciativas que visam ao envolvimento da sociedade civil e outros setores governamentais 4. Existência da Escola Nacional de defesa Cibernética (ENaDCiber) 5. Existência de quadro altamente especializado (QEM) 6. Existência de um sistema de TI bem organizado e estruturado (SisTEx) 7. Capacidade de *lobby* junto ao Congresso Nacional 8. Liderança nos assuntos relativos à Cibernética	FRAQUEZAS (W)	1. Inexistência de um grupo profissional na área de cibernética 2. Aproveitamento marginal de pessoal altamente especializado (QEM) 3. Hiato tecnológico 4. Escassez de recursos humanos e financeiros 5. Cultura pacifista 6. Visão eminentemente defensiva 7. Adoção de conceitos restritos quanto ao emprego da Guerra Cibernética 8. Identificação imprecisa e/ou vaga das ameaças e riscos à Segurança Nacional a partir do espaço cibernético
FATORES EXTERNOS	OPORTUNIDADES (O)	1. Apoio do Congresso Nacional 2. Possibilidade de intercâmbio com nações do arco do conhecimento 3. Conflito de interesses entre as nações centrais, Rússia e China 4. Existência de boa interligação com o resto do planeta (infovias) 5. Ausência de regulações internacionais específicas sobre Guerra Cibernética	AMEAÇAS (T)	1. Espaço cibernético cada vez mais contestado 2. Nível de sofisticação dos ataques cibernéticos crescente 3. Aumento de atores com capacidade cibernética 4. Espaço cibernético favorável a ações coercitivas 5. Especialização cada vez maior dos atores cibernéticos 6. Hiato tecnológico 7. Presença de ameaças no entorno estratégico real e virtual, representadas por nações e grupos não estatais 8. Uso de *hackers* sem ligação estatal 9. Postura eminentemente ofensiva dos atores 10. Desacoplamento entre a capacidade cibernética nacional e a evolução indicada pela Guerra do Futuro

Fonte: o autor.

Feita a análise SWOT, as propostas a seguir buscam mitigar as fraquezas identificadas, fortalecer as forças, aproveitar as oportunidades e reduzir a exposição às ameaças. Para tanto, as propostas serão formuladas segundo o conceito de DOAMEPI, empregado pelo Exército Brasileiro para obter as suas capacidades (BRASIL. EXÉRCITO. ESTADO-MAIOR., 2019). DOAMEPI é um acrônimo para os fatores Doutrina, Organização, Adestramento, Material, Educação, Pessoal e Infraestrutura.

PROPOSTA 1: Revisão doutrinária e normativa
JUSTIFICATIVA: A revisão visa à eliminação ou redução dos limites conceituais hoje existentes e ao alinhamento com a conduta visualizada na Guerra do Futuro. Assim busca-se manter o pensamento militar brasileiro atualizado e alinhado com as tendências.
ENQUADRAMENTO DOAMEPI: Doutrina
FATORES SWOT ABORDADOS:

S: 2, 8	**W:** 5, 6, 7, 8
O: 5	**T:** 7, 8, 9, 10

PROPOSTA 2: Envolvimento do QEM na área de cibernética
JUSTIFICATIVA: O envolvimento do QEM na área de cibernética tende a infundir a área com pessoal e conhecimentos diversificados e altamente especializado, ampliando a capacidade de cibernética. Tende, também, a mitigar o hiato tecnológico e a favorecer o desenvolvimento de ferramentas especializadas. Por fim, espera-se aumento no nível de especialização técnica e sofisticação nas ações cibernéticas.
ENQUADRAMENTO DOAMEPI: Organização, Pessoal
FATORES SWOT ABORDADOS:

S: 1, 4, 5	**W:** 2, 3, 4
O: 2	**T:** 2, 3, 5, 6

PROPOSTA 3: Criação da Arma de Cibernética
JUSTIFICATIVA: A criação da Arma de Cibernética contribui para a profissionalização e aumento do nível técnico. Também tende a fortalecer a Doutrina e o pensamento militar de cibernética. A Arma de Cibernética contribui,

ainda, para o aumento da verticalização da estrutura militar e mitiga a escassez de pessoal. Busca-se, assim, um perfil técnico altamente especializado e experiente. É uma medida com forte apelo dissuasório por ser uma construtora e demonstradora de capacidade.

ENQUADRAMENTO DOAMEPI: Doutrina, Organização, Educação, Pessoal

FATORES SWOT ABORDADOS:

S: 1, 2, 4, 5, 7	**W:** 1, 4
O: 1, 2, 3, 4, 5	**T:** 1, 2, 3, 4, 5, 7

As propostas ora apresentadas abordam todas as fraquezas e ameaças identificadas e apresentam-se em ordem crescente de horizonte temporal quanto aos resultados esperados. A proposta 1 tem horizonte de curto prazo. A proposta 2 deve apresentar resultados no médio prazo, enquanto a proposta 3 deve ter resultados em longo prazo.

Como as propostas delineadas são baseadas num retrato do momento presente e em prognósticos de futuro construídos a partir desse retrato, é imprescindível o acompanhamento de conjuntura, de forma a mantê-las sempre atuais e oportunas.

6 CONCLUSÃO

A evolução tecnológica agregou novos elementos à guerra. Sem dúvida, dentre esses novos elementos, o Espaço Cibernético se tornou um elemento de destaque quando se pensa a guerra do futuro. Sua importância já não é mais discutida, mas está ratificada pela visão das principais potências.

O Brasil não se manteve alheio às novas tendências. A despeito das dificuldades que o País possui, envidou esforços no sentido de se preparar para essa nova arena de disputa. Os esforços, conduzidos com racionalidade e visão, deram ao Brasil uma sólida na base sobre a qual se preparar para o futuro.

Esse trabalho iniciou por uma revisão documental, buscando insumos que permitissem contextualizar o cenário futuro na área de cibernética. Foi sem surpresa alguma que se identificou o Espaço Cibernético como um ambiente altamente contestado. Na verdade, ficou claro que são conduzidas guerras cibernéticas sem nenhum constrangimento. Esse novo espaço, ao aproximar as nações, ressaltou suas diferenças e, livres do escrutínio da opinião pública, os estados-nação puderam dar vazão ao neorrealismo que verdadeiramente impera entre os países, relegando o idealismo dos organismos supranacionais a um papel figurativo.

Nada disso surpreendeu. Nações buscam satisfazer seus interesses. Mas a caracterização dessa realidade é imprescindível para corretamente traçar o cenário futuro para o qual o Brasil deve se preparar. Não um cenário pacífico de cooperação, mas um cenário hostil, de imposição da vontade pelos novos meios trazidos com a Cibernética. Mais sutis e difíceis de combater.

A caracterização desse cenário, conforme dito, iniciou-se com uma revisão de literatura. Após a contextualização do cenário atual interno e externo, deu-se a análise extensiva do pensamento e das estruturas militares de cibernética dos EUA. Foi graças a abundante documentação, que se identificou que os EUA possuem uma mentalidade essencialmente ofensiva. Não é para menos. Os norte-americanos perceberam que a melhor defesa cibernética e não permitir que seus adversários empreguem contra eles ataques cibernéticos. Isso porque um ataque cibernético bem sucedido é, por definição, não percebido até que seja tarde demais.

Os EUA amadureceram sua estrutura de cibernética junto da NSA. Por isso, sua visão contempla um emprego abrangente da Cibernética. Seu nível de refinamento de pensamento e sua capacidade de identificar com precisão aquilo que lhes ameaça permitiu-lhes traçar com propriedade os desafios que precisam vencer.

Em seguida, esse estudo se deteve na análise documental referente ao caso chinês. O fato de o governo da RPC não ser transparente fez com que a documentação sobre as estratégias militares e o pensamento chinês sobre cibernética não pudesse ser obtida. Essa limitação foi contornada analisando-se a china através da observação indireta. Isto é, buscou-se analisar documentos produzidos sobre terceiros que avaliavam os aspectos de interesse para o presente trabalho.

A China terminou por ratificar alguns pontos levantados por ocasião da análise dos EUA. Isso também não foi surpresa, pois como ambos os países estão engajados numa competição por poder tanto no âmbito regional, quanto mundial, é natural que haja forte acoplamento entre as estratégias e pensamentos militares de ambos os países.

Todavia, a China trouxe como elemento novo, o amplo e rotineiro emprego de atores sem ligação direta com o estado. O poder chinês vale-se, assim, de *hackers* recrutados no mundo civil, o que dá à China uma negação plausível para a autoria de suas ações. Essa abordagem confere ainda mais liberdade de ação à China. Mais do que os EUA ou as demais potências centrais, a China faz livre uso do seu poderio cibernético a fim de obter os ganhos que almeja e prejudicar o interesse de seus competidores.

A análise chinesa foi seguida pela análise do Brasil, ponto central do interesse desse estudo. O Brasil apresentou boa documentação, facilmente acessível ao escrutínio. Todavia, diferentemente da China e dos EUA, pouco se pode identificar a respeito das ações cibernéticas brasileiras. Novamente, não há surpresa. O forte viés pacifista do Brasil, historicamente imposto pelas nações dominantes de maneira a facilitar seu controle, dá um tom extremamente comedido à mentalidade de cibernética brasileira.

No desenvolvimento da estratégia e doutrina de cibernética, o Brasil mostra-se vago na identificação das ameaças e titubeante no emprego ofensivo dessa capacidade. Essa hesitação é, sem dúvida, um óbice à própria estratégia de

dissuasão buscada pelo Brasil, já que a crença no emprego de uma capacidade é essencial para que se desestimule ações contrárias ao interesse nacional. Essa postura ofensiva é, por exemplo, a visão adotada pelos EUA e que a história mostra ser mais vantajosa, ao desestimular as agressões.

O Brasil também exibe uma segregação de pessoal dentro do Exército Brasileiro que afasta o QEM, um quadro altamente especializado, da área de cibernética. Essa postura também se revela desalinhada com as tendências encontradas nos EUA e China e tende a reduzir a capacidade de defesa cibernética do País.

Percebe-se, contudo, que tanto o Exército Brasileiro quanto o Ministério da Defesa possuem capacidade cibernética bem estruturada, em que pese os desafios existentes, como o *Gap* tecnológico, escassez de recursos humanos e financeiros e deficiente integração da sociedade civil na área de Defesa. Isso mostra que o pensamento sobre Defesa Cibernética no Brasil revela o empenho e a vontade de se construir um sistema capaz de proteger o País.

Uma vez procedida a análise documental, foram conduzidos estudos de caso, onde foram analisados EUA, China e Brasil, a fim de se construir um cenário prospectivo da Guerra do Futuro. Diversas tendências foram levantadas, mas merecem ressalvas àquelas que ratificaram achados da análise documental.

Uma das tendências que apareceram tanto na análise documental quanto na construção do cenário prospectivo é a que revela o Espaço Cibernético como um ambiente de guerra. O espaço oferece condições para que nações e grupos não estatais empreguem meios não convencionais para obter seus objetivos, tornando o ambiente extremamente contestado. A situação de confronto é constante, envolve os mais diversos atores e tende a se acentuar no futuro.

Esse cenário de guerra virtual tenderá a envolver o Brasil, seja pelo confronto de seus objetivos nacionais, seja pelo interesse que potências externas têm no país. Assim, a tradição pacifista do Brasil tende a ser contestada no espaço cibernético, o que deve suscitar ações de atores no sentido de fortalecê-la, a fim de limitar a capacidade nacional de o País se defender no campo cibernético.

Com base na análise documental e no cenário prospectivo, empregou-se a ferramenta SWOT com o fito de se subsidiar a formulação de propostas capazes de manter a Defesa Cibernética brasileira alinhada e atualizada com a evolução prevista na Guerra do Futuro.

Tendo-se levantado as Forças, Fraquezas, Oportunidades e Ameaças, foram elaboradas três propostas à luz do conceito DOAMEPI. Cada proposta possui um horizonte temporal diferente, mas buscam mitigar todas as fraquezas, evitar as ameaças, explorar as oportunidades e fortalecer os pontos de força.

Com isso, esse trabalho busca contribuir para a capacidade do Exército Brasileiro cumprir sua missão constitucional. Em que pese o excelente trabalho de formulação do pensamento militar brasileiro de cibernética e a organização de uma estrutura militar muito bem modelada, o caráter constantemente inovador da área de cibernética torna oportuna a análise feita. As propostas buscam adequar a capacidade de cibernética ao futuro prospectado, garantindo atualidade, aumentando a qualidade, a eficiência e a eficácia, sem perder de vista a necessária adequação à realidade do Brasil.

7 REFERÊNCIAS

ALBERTS, David S. e GARSTKA, John J. e STEIN, Frederick P. **Network Centric Warfare**. 2. ed. [S.l.]: CCRP publication series, 2000. Disponível em: <http://dodccrp.org/files/Alberts_NCW.pdf>. Acesso em: 3 ago 2020.

Army's Cyber branch marks its fifth anniversary | Article | The United States Army. Disponível em: <https://www.army.mil/article/226345/armys_cyber_branch_marks_its_fifth_anniversary>. Acesso em: 13 jun 2020.

BANKAI. **History of UX Evolution - Timeline for Computer Age**. Disponível em: <https://bankai.eu/files/ux-timeline/ux-timeline-1d.pdf>. Acesso em: 4 out 2020.

BBC. **Facebook scandal "hit 87 million users" - BBC News**. Disponível em: <https://www.bbc.com/news/technology-43649018>. Acesso em: 5 ago 2020.

BBC. **Nato: Cyber-attack on one nation is attack on all**. BBC, 2019. Disponível em: <https://www.bbc.com/news/technology-49488614>. Acesso em: 8 ago 2020.

BELYAEV, Dmitry. **US and Taiwan Seriously Concerned over China's Cyberspace Activity**. Disponível em: <http://bda-expert.com/2013/05/ssha-i-tajvan-serezno-obespokoeny-dejstviyami-kitaya-v-kiberprostranstve/>. Acesso em: 25 ago 2020.

BRASIL. ESTADO-MAIOR DO EXÉRCITO. **Portaria nº 075-EME, de 10 de junho de 2010**. Boletim do Exército. [S.l: s.n.]. , 2010

BRASIL. EXÉRCITO. COMANDO DE OPERAÇÕES TERRESTRES. **Manual de Campanha - GUERRA CIBERNÉTICA**. Portaria nº 42 - COTER, de 8 de junho de 2017., 2017.

BRASIL. EXÉRCITO. ESTADO-MAIOR. **Portaria nº 326-EME, de 31 de outubro de 2019. Aprova o Manual de Fundamentos Doutrina Militar Terrestre (EB20-MF-10.102), 2a Edição, 2019.** , 2019. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/4760/1/EB20-MF-10.102.pdf>.

BRASIL. MINISTÉRIO DA DEFESA. **Estratégia Setorial de Defesa**. Portaria Normativa Nº 26/GM-MD, de 16 de abril de 2019. Brasil: [s.n.]. , 2016

BRASIL. **Constituição da República Federativa do Brasil - Promulgada em 5 de outubro de 1988**. , 2016, p. 4. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf?sequence=1>. Acesso em: 22 out 2020.

BRASIL e colab. **Estratégia de Segurança da Informação e Comunicações e de**

Segurança Cibernética da Administração Pública Federal. Decreto nº 10.222, de 5 de fevereiro de 2020. [S.l: s.n.]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm>. Acesso em: 1 set 2020. , 2020

BRASIL. **Política Nacional de Defesa. Estratégia Nacional de Defesa**. Diário Oficial da União - Seção 1 - 26/9/2013, Página 1, p. 155, 2012. Disponível em: <http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>.

BRASIL e EXÉRCITO BRASILEIRO e ESTADO-MAIOR DO EXÉRCITO. **Portaria nº 118-EME, de 3 de abril de 2017.** Boletim do Exército, n. 15, 2017. Disponível em: <https://www.dcem.eb.mil.br/images/arquivos/secoes/cursos/dct/cige/Port_Nr_118-EME_3_ABR_17.pdf>. Acesso em: 3 out 2020.

BRASIL e MINISTÉRIO DA DEFESA. **Atribui ao Centro de Defesa Cibernética a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética no âmbito do Ministério da Defesa**. Portaria nº 3.405-MD, de 21 de dezembro de 2012. [S.l: s.n.]. , 2012

BRASIL e MINISTÉRIO DA DEFESA. **Diretriz de Implantação de Medidas Visando à Potencialização da Defesa Cibernética**. Portaria Normativa nº 2.777-MD, de 27 de outubro de 2014. [S.l: s.n.]. , 2014

BRASIL e MINISTÉRIO DA DEFESA. **Política Setorial de Defesa 2020-2031 e Mapa Estratégico do Setor de Defesa.** Portaria Normativa Nº 25/GM-MD, de 16 de abril de 2019. Brasil: [s.n.]. , 2019

BRASIL e MINISTÉRIO DA DEFESA e ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS. **Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014**. . [S.l: s.n.]. , 2014

BRASIL e MINISTÉRIO DA DEFESA e EXÉRCITO BRASILEIRO. **Centro de Defesa Cibernética do Exército**. Portaria nº 666, do Gab Cmt EB, de 4 de agosto de 2010. [S.l: s.n.]. , 2010

BRASIL e MINISTÉRIO DA DEFESA e EXÉRCITO BRASILEIRO. **Regulamento da Escola Nacional de Defesa Cibernética - EB10-R-07.014**. Portaria nº 396, do Gab Cmt EB, de 21 de março de 2019. [S.l: s.n.]. , 2019

BRASIL e MINISTÉRIO DA DEFESA e MINISTÉRIO DA CIÊNCIA, Tecnologia e Inovação. **Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética**. Portaria Interministerial MD/MCTI nº 1.424, de 31 de dezembro de 2014, 2014. Disponível em:

<http://www.editoramagister.com/legis_26349623_PORTARIA_INTERMINISTERIAL_N_1424_DE_31_DE_DEZEMBRO_DE_2014.aspx>.

BURKE, Crispin. **The Pentagon Should Adjust Standards for Cyber Soldiers — As It Has Always Done**. War on the Rocks, 2018. Disponível em: <https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done/>. Acesso em: 25 ago 2020.

BURTON, Rachael e STOKES, Mark. **The People ' s Liberation Army Strategic Support Force Leadership and Structure**. 2018.

Category:People's Liberation Army branches - Wikipedia. Disponível em: <https://en.wikipedia.org/wiki/Category:People%27s_Liberation_Army_branches>. Acesso em: 26 ago 2020.

CCDCCOE. **CCDCOE (About Us)**. Disponível em: <https://ccdcoe.org/about-us/>. Acesso em: 1 abr 2020.

CHENG, Joey. **Cyber conflict escalates: Second Chinese PLA hacking group accused -- Defense Systems**. Disponível em: <https://defensesystems.com/articles/2014/06/10/chinese-military-hacker-unit-crowdstrike.aspx>. Acesso em: 26 ago 2020.

CHINA e DEFENSE, Ministry of National. **Full Text: China's Military Strategy**. Disponível em: <https://news.usni.org/2015/05/26/document-chinas-military-strategy>. Acesso em: 1 abr 2020.

Chinese cyber-attacks: Hello, Unit 61398 | The Economist. Disponível em: <https://www.economist.com/analects/2013/02/19/hello-unit-61398?spc=scode&spv=xm&ah=9d7f7ab945510a56fa6d37c30b6f1709>. Acesso em: 26 ago 2020.

CIRIBELLI, Marilda Corrêa. **Como elaborar uma dissertação de Mestrado através da pesquisa científica**. Rio de Janeiro, RJ: [s.n.], 2003.

COMMONWEALTH SECRETARIAT. **Member countries - The Commonwealth**. Disponível em: <https://thecommonwealth.org/member-countries>. Acesso em: 30 set 2020.

COSTELLO, John e MCREYNOLDS, Joe. **China's Strategic Support Force: A Force for a New Era**. Washington, D.C.: National Defense University Press, 2018.

COUNCIL ON FOREIGN RELATIONS. **PLA Unit 61398 | CFR Interactives**. Disponível em: <https://www.cfr.org/cyber-operations/pla-unit-61398>. Acesso em: 26 ago 2020.

CRUZ, Diogenes Marco de Brito e colab. **Aplicação do Planejamento Estratégico a partir da análise SWOT: um estudo de caso numa empresa de tecnologia da informação.** IX Simpósio de Engenharia de Produção de Sergipe (IX SIMPROD), n. 2017, p. 140–154, 2017. Disponível em: <www.simprod.ufs.br>.

DIGITAL ATTACK MAP. **Digital Attack Map**. Disponível em: <https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18489&view=map>. Acesso em: 7 set 2020.

DOMINGO, Francis C. **Conquering a new domain: Explaining great power competition in cyberspace**. Comparative Strategy, v. 35, n. 2, p. 154–168, 2016.

DUARTE, Marco Túlio Souto Maior. **Uma Análise dos Documentos Relativos à Transformação Militar do Exército Brasileiro**. Revista de Iniciação Científica em Relações Internacionais, v. 5, n. 10, p. 95–111, 2018.

DUNLAP, Charles J. **Perspectives for Cyber Strategists on Law for Cyberwar**. Strategic Studies Quarterly, n. June 2010, p. 81–99, 2011. Disponível em: <http://scholarship.law.duke.edu/faculty_scholarship/2368/>.

ELLMAN, Jesse e SAMP, Lisa e COLL, Gabriel. **Assessing the Third Offset Strategy**. . [S.l: s.n.], 2017. Disponível em: <www.csis.org>. Acesso em: 7 ago 2020.

EXERCITO BRASILEIRO. **Política Militar Terrestre, integrante do Sistema de Planejamento Estratégico do Exército**. Separata ao Boletim do Exército, p. 23, 2019.

Falkland Islands (British Overseas Territory) travel advice - GOV.UK. Disponível em: <https://www.gov.uk/foreign-travel-advice/falkland-islands>. Acesso em: 30 set 2020.

FIGUEIRA, Flávio Zylberberg Balbino. **A Presença Militar Atual dos EUA na América do Sul e no Atlântico Sul e seus Reflexos para o Brasil**. 2018. Escola de Comando e Estado-Maior do Exército, 2018.

GIL, A C. **Métodos E Técnicas De Pesquisa Social**. [S.l.]: ATLAS EDITORA, 2019. Disponível em: <https://books.google.pt/books?id=rhB4wwEACAAJ>.

Global cyber attacks on the increase during COVID-19 crisis | SecurityWorldMarket.com. Disponível em: <https://www.securityworldmarket.com/int/News/Business-News/during-covid-19-no-one-is-immune-to-cyber-attacks>. Acesso em: 1 abr 2020.

GLOBAL FIRE POWER. **2020 Military Strength Ranking**. Disponível em: <https://www.globalfirepower.com/countries-listing.asp>. Acesso em: 10 ago 2020.

GUANGHUI, Ni. **Demystifying the first strategic support force of our army (defense line of sight, deepening national defense and military reforms)**. Disponível em: <http://military.people.com.cn/n1/2016/0124/c1011-28079245.html>. Acesso em: 26 ago 2020.

HILLNER, Eric P. **The Third Offset Strategy and the Army modernization priorities**. . [S.l: s.n.], 2019. Disponível em: <https://usacac.army.mil/sites/default/files/publications/17855.pdf>. Acesso em: 7 ago 2020.

HJORTDAL, Magnus. **China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence**. Journal of Strategic Security, v. 4, n. 2, p. 1–24, 2011. Disponível em: <www.jstor.org/stable/26463924>.

HUNKER, Jeffrey. **Cyber war and cyber power**. Research Paper, n. 62, 2010. Disponível em: <https://www.jstor.org/stable/resrep10354>.

Infrapedia | Global Internet Infrastructure Map. Disponível em: <https://www.infrapedia.com/app>. Acesso em: 4 out 2020.

INMARSAT. **I-4 and Alphasat coverage**. Disponível em: <https://www.inmarsat.com/wp-content/uploads/2019/04/Inmarsat_Alphasat_and_I-4_Coverage_April_2019_EN_LowRes.pdf>. Acesso em: 4 out 2020.

INTERNATIONAL COMMITEE OF THE RED CORSS. **Protocols additional to the Geneva Conventions of 12 August 1949**. n. August, p. 30, 35, 37–38, 53–54, 84, [S.d.]. Disponível em: <https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf>.

JÚNIOR, AUGUSTO W. M. TEIXEIRA. **A guerra do futuro e suas implicações estratégicas : uma perspectiva Clausewitziana**. Análise Estratégica, v. 11, n. 1, p. 17–24, 2018.

KANIA, Elsa B e COSTELLO, John K. **The Strategic Support Force and the Future of Chinese Information Operations**. The Cyber Defense Review, v. 3, n. 1, p. 105–122, 2018.

KASPERSKY. **Kaspersky Cyberthreat real-time map**. Disponível em: <https://cybermap.kaspersky.com/>. Acesso em: 7 set 2020.

KLIMBURG, Alexander (Org.). **National Cyber Security Framework Manual**. Tallinn: NATO CCD COE Publication, 2012. Disponível em: <https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf>.

KOVACS, Eduard. **Cyber Spies Targeting U.S. Defense, Tech Firms Linked to**

China's PLA: Report | SecurityWeek.Com. Disponível em: <https://www.securityweek.com/cyber-spies-targeting-us-defense-tech-firms-linked-chinas-pla-report>. Acesso em: 26 ago 2020.

LEAL PUJOL, Edson. **Diretriz do Comandante do Exército Brasileiro**. 2019.

Les territoires ultramarins | Ministère des Outre-mer. Disponível em: <https://outre-mer.gouv.fr/les-territoires-ultramarins>. Acesso em: 30 set 2020.

LOPEZ, C. Todd. **Persistent Engagement, Partnerships, Top Cybercom's Priorities**. Disponível em: <https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/>. Acesso em: 11 jun 2020.

LUTTWAK, Edward Nicolae. **Estratégia: A Lógica da Guerra e da Paz**. Rio de Janeiro: Biblioteca do Exército Editora, 2009.

MATTOS, Carlos de Meira. **ONGs internacionais na Amazônia**. Disponível em: <https://www1.folha.uol.com.br/fsp/opiniao/fz2906200509.htm>. Acesso em: 8 set 2020.

MORETTI, Enrico e STEINWENDER, Claudia e REENEN, John Van. **The Intellectual Spoils of War? Defense R&D, Productivity and International Spillovers**. . [S.l: s.n.], 2019. Disponível em: <http://www.nber.org/papers/w26483>. Acesso em: 10 ago 2020.

MORI, Leticia. **A proposta de Biden para a Amazônia e por que ela irritou Bolsonaro - BBC News Brasil**. Disponível em: <https://www.bbc.com/portuguese/brasil-54364961>. Acesso em: 2 out 2020.

MYRE, Greg. **"Persistent Engagement": The Phrase Driving A More Assertive U.S. Spy Agency**. Disponível em: <https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency>. Acesso em: 11 jun 2020.

NATO. **NATO - Topic: Collective defence - Article 5**. Disponível em: <https://www.nato.int/cps/en/natohq/topics_110496.htm?>. Acesso em: 8 ago 2020.

NEVES, Lucas e COLETTA, Ricardo Della e FERNANDES, Talita. **Macron diz que discutir status internacional da Amazônia é "questão que se impõe".** Disponível em: <https://www1.folha.uol.com.br/ambiente/2019/08/macron-diz-que-discutir-estatuto-internacional-da-amazonia-e-questao-que-se-impoe.shtml>. Acesso em: 8 set 2020.

NG, Jr. **China Broadens Cyber Options - Asian Military Review**. Disponível em:

<https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/>. Acesso em: 26 ago 2020.

NI, Adam e GILL, Bates. **The People's Liberation Army Strategic Support Force: Update 2019 - Jamestown**. Disponível em: <https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/>. Acesso em: 26 ago 2020.

NYE, Joseph S. **O Futuro do Poder**. 1. ed. [S.l.]: Benvirá, 2012.

Os ciberataques mais famosos dos últimos tempos. Disponível em: <https://www.kaspersky.com.br/blog/five-most-notorious-cyberattacks/11042/>. Acesso em: 5 ago 2020.

PALMER, Danny. **Hackers are getting more hands-on with their attacks. That's not a good sign**. Disponível em: <https://www.zdnet.com/article/hackers-are-getting-more-hands-on-with-their-attacks-thats-not-a-good-sign/>.

Pentagon creates new medal for cyber, drone wars - U.S. - Stripes. Disponível em: <https://www.stripes.com/news/us/pentagon-creates-new-medal-for-cyber-drone-wars-1.207820>. Acesso em: 8 ago 2020.

PERLO-FREEMAN, Sam e colab. **Trends in World Military Expenditure, 2012**. Stockholm International Peace Research Institute, n. April, p. 1–8, 2016.

PETUKHOV, Alexander Yur'evich e colab. **Transition of rivalry between USA and China to new internet-space**. Advances in Environmental Biology, v. 8, n. 13, p. 290–293, 2014.

PLA Unit 61398. Disponível em: <https://en.wikipedia.org/wiki/PLA_Unit_61398>. Acesso em: 26 ago 2020.

PLA Unit 61486. Disponível em: <https://en.wikipedia.org/wiki/PLA_Unit_61486>. Acesso em: 26 ago 2020.

POMERLEAU, Mark. **What the future holds for Cyber Command**. Disponível em: <https://www.fifthdomain.com/dod/cybercom/2019/07/25/what-the-future-holds-for-cyber-command/>. Acesso em: 11 jun 2020.

POMERLEAU, Mike. **CYBERCOM wants adversary to know it's hacked.** C4ISRNET, 2016. Disponível em: <https://www.c4isrnet.com/2016/08/31/cybercom-wants-adversary-to-know-it-s-hacked/>. Acesso em: 13 jun 2020.

Quem apoia Maduro ou Guaidó: entenda o xadrez político da crise na Venezuela - Jornal O Globo. Disponível em: <https://oglobo.globo.com/mundo/quem-apoia-maduro-ou-guaido-entenda-xadrez-politico-da-crise-na-venezuela-23398552>.

Acesso em: 30 set 2020.

REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE WITH ADDITIONAL VIEWS. . [S.l: s.n.], [S.d.]. Disponível em: <https://www.dhs.gov/news/2017/10/06/statement->. Acesso em: 5 ago 2020.

RODRIGUES, William Costa. **Metodologia Científica**. Faetec/IST. Paracambi, p. 01–20, 2007.

Rússia anuncia ampliação de cooperação militar com Venezuela | Notícias internacionais e análises | DW | 08.02.2020. Disponível em: <https://www.dw.com/pt-br/rússia-anuncia-ampliação-de-cooperação-militar-com-venezuela/a-52300614>. Acesso em: 30 set 2020.

SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. [S.l.]: Cambridge University Press, 2013.

SCIMAGO JOURNAL AND COUNTRY RANK. **SJR - International Science Ranking**. Disponível em: <https://www.scimagojr.com/countryrank.php?year=2019>. Acesso em: 2 ago 2020.

SEVIŞ, Kamile Nur e SEKER, Ensar. **Cyber warfare: Terms, issues, laws and controversies**. 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, 2016.

SHANKER, Thom. **Cyberwar Nominee Sees Gaps in Law - The New York Times**. Disponível em: <https://www.nytimes.com/2010/04/15/world/15military.html>. Acesso em: 8 ago 2020.

SMITH, Noah. **Military Spending on R&D Is a Boon for the Private Sector - Bloomberg**. Disponível em: <https://www.bloomberg.com/opinion/articles/2019-12-04/military-spending-on-r-d-is-a-boon-for-the-private-sector>. Acesso em: 10 ago 2020.

SPRINGER NATURE LIMITED. **Nature Index. 2019 tables: Countries/territories**. Disponível em: <https://www.natureindex.com/annual-tables/2019/country/all>. Acesso em: 2 ago 2020.

STAFF, Office of the Chairman of the Joint Chiefs of. **DOD Dictionary of Military and Associated Terms**. Joint Education and Doctrine Division, J-7, n. January, p. 382, 2020. Disponível em:

<https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.

STOLTENBERG, Jens. **NATO - News: NATO will defend itself**. Disponível em: <https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en>. Acesso em: 8 ago 2020.

Stuxnet: As origens. Disponível em: <https://www.kaspersky.com.br/blog/stuxnet-as-origens/4391/>. Acesso em: 5 ago 2020.

THE OPTE PROJECT. **File:Internet map 1024.jpg - Wikimedia Commons**. Disponível em: <https://commons.wikimedia.org/wiki/File:Internet_map_1024.jpg>. Acesso em: 23 ago 2020.

TRADOC. **The U.S. Army in Multi-Domain Operations 2028**. 2018.

U.S. ARMY. **Army Cyber Training | goarmy.com**. Disponível em: <https://www.goarmy.com/army-cyber/army-cyber-training.html>. Acesso em: 24 ago 2020a.

U.S. ARMY. **Cyber Direct Commissioning Program | goarmy.com**. Disponível em: <https://www.goarmy.com/army-cyber/cyber-direct-commissioning-program.html>. Acesso em: 24 ago 2020b.

U.S. ARMY. **Timeline of Army Cyber | goarmy.com**. Disponível em: <https://www.goarmy.com/army-cyber/timeline-of-army-cyber.html>. Acesso em: 23 ago 2020c.

U.S. ARMY CYBER COMMAND. **About Army Cyber Command**. Disponível em: <https://www.goarmy.com/army-cyber/about-army-cyber-command.html>. Acesso em: 23 ago 2020a.

U.S. ARMY CYBER COMMAND. **Army Cyber Command**. Disponível em: <https://www.arcyber.army.mil/>. Acesso em: 23 ago 2020a.

U.S. ARMY CYBER COMMAND. **Army Cyber Command About**. Disponível em: <https://www.arcyber.army.mil/Organization/About-Army-Cyber/>. Acesso em: 23 ago 2020b.

U.S. ARMY CYBER COMMAND. **Army Cyber Command History**. Disponível em: <https://www.arcyber.army.mil/Organization/History/>. Acesso em: 23 ago 2020c.

U.S. ARMY CYBER COMMAND. **ARMY CYBER FACT SHEET: Army Cyber Direct Commissioning Program > U.S. Army Cyber Command > Fact Sheets**. Disponível em: <https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1440683/army-cyber-fact-sheet-army-cyber-direct-commissioning-program/>. Acesso em: 23 jun 2020.

U.S. ARMY CYBER COMMAND. **FACT SHEET: U.S. Army Cyber Command**. . [S.l: s.n.]. Disponível em: <https://www.arcyber.army.mil/Portals/34/Fact Sheets/ARCYBER fact sheet - Cyber Mission Force (7Feb2020).pdf?ver=2020-02-10-121111-443>. Acesso em: 14 jun 2020b. , [S.d.]

U.S. CYBER COMMAND. **Command History**. Disponível em: <https://www.cybercom.mil/About/History/>. Acesso em: 14 jun 2020a.

U.S. CYBER COMMAND. **Mission and Vision**. Disponível em: <https://www.cybercom.mil/About/Mission-and-Vision/>. Acesso em: 9 ago 2020b.

U.S. DEPARTMENT OF DEFENSE. **Summary: Department of Defense Cyber Strategy**. . [S.l: s.n.], 2018.

U.S. DEPARTMENT OF DEFENSE e DEFENSE DEPARTMENT NEWS. **Cyber Mission Force Achieves Full Operational Capability**. Disponível em: <https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/>. Acesso em: 13 jun 2020.

US CYBERSPACE SOLARIUM COMMISSION. **U.S. Cyberspace Solarium Commision Report**. . [S.l: s.n.], 2020. Disponível em: <https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view>. Acesso em: 12 jun 2020.

WELCH, Larry D. **Cyberspace – The fifth operational domain**. IDA Research Notes, p. 1–7, 2011.

WIKIPEDIA. **Opte Project - Wikipedia**. Disponível em: <https://en.wikipedia.org/wiki/Opte_Project>. Acesso em: 23 ago 2020.

ZHEN, Liu. **Chinese army now makes up less than half of PLA's strength as military aims to transform itself into modern fighting force**. Disponível em: <https://www.scmp.com/news/china/military/article/2183050/chinese-army-now-makes-less-half-plas-strength-military-aims>. Acesso em: 26 ago 2020.