UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ECONOMIA POLÍTICA INTERNACIONAL

MARCUS VINICIUS DA SILVA TAVARES

5G – CONEXÃO PARA UM NOVO MUNDO: UMA ANÁLISE TRANSVERSAL DO CASO EUA VS HUAWEI

Rio de Janeiro
2023

Marcus Vinicius da Silva Tavares

5G – CONEXÃO PARA UM NOVO MUNDO: UMA ANÁLISE TRANSVERSAL DO CASO EUA VS HUAWEI

Dissertação apresentada ao Programa de Pós-Graduação em Economia Política Internacional, do Instituto de Economia da Universidade Federal do Rio de Janeiro (PEPI-UFRJ), como parte dos requisitos necessários à obtenção do título de Mestre em Economia Política Internacional.

Orientador: Prof. Dr. José Luís da Costa Fiori

Rio de Janeiro

2023

FICHA CATALOGRÁFICA

M231c Tavares, Marcus Vinicius da Silva.
5G - conexão para um Novo Mundo: uma análise transversal do caso Estados Unidos vs Huawei / Marcus Vinicius da Silva Tavares. – 2023.
116 f.; 31 cm.

Orientador: José Luís da Costa Fiori.
Dissertação (mestrado) – Universidade Federal do Rio de Janeiro, Instituto de Economia, Programa de Pós-Graduação em Economia Política Internacional, 2023.
Bibliografia: f. 106-116.

1. Geopolítica. 2. Tecnologia da informação e comunicação. 3. Huawei. 4. Estados Unidos. I. Fiori, José Luís da Costa, orient. II. Universidade Federal do Rio de Janeiro. Instituto de Economia. III. Título.

CDD 327.101

Ficha catalográfica elaborada pela bibliotecária: Luiza Hiromi Arao CRB 7 – 6787
Biblioteca Eugênio Gudin/CCJE/UFRJ

Marcus Vinicius da Silva Tavares

5G – CONEXÃO PARA UM NOVO MUNDO: UMA ANÁLISE TRANSVERSAL DO CASO EUA VS HUAWEI

Dissertação apresentada ao Programa de Pós-Graduação em Economia Política Internacional, do Instituto de Economia da Universidade Federal do Rio de Janeiro (PEPI-UFRJ), como parte dos requisitos necessários à obtenção do título de Mestre em Economia Política Internacional.

Aprovada em 13 de fevereiro de 2023

_____

Prof. Dr. José Luís da Costa Fiori (IE/PEPI/UFRJ) – Orientador

_____

Profª. Dr. ª Monica Ellen Seabra Hirst (CPEI/UTDT)

_____

Prof. Dr. Alcides Eduardo dos Reis Peron (RI/FECAP)

Dedicatória

Dedico esse sucesso pessoal a todos os que nasceram sob o manto asfixiante da pobreza, que se alimentaram da fome, que beberam de suas próprias lágrimas e que, mesmo em meio às adversidades da vida, fazem e fizeram do mundo um lugar melhor com os seus sorrisos e esperança.

Agradecimentos

Não podendo ser diferente, agradeço primeiramente ao povo brasileiro, sem o qual a UFRJ não poderia existir. Agradeço a esse povo tão heroico e sofrido, que cotidianamente se levanta sob o sol das incertezas e se deita sob a lua da esperança. Que Deus abençoe ricamente esse povo e que o seu futuro grandioso ansiado em nosso hino chegue o quanto antes.

Agradeço aos meus pais, a quem tudo devo. Obrigado, pai! Obrigado por seu amor e sua compreensão, que se mostram mesmo no seu jeito duro e por vezes silencioso. Obrigado por me carregar tantas vezes no colo pelos caminhos escuros desse mundo, por me mostrar a dureza que seria viver essa vida e por me inspirar a ser o melhor ser humano possível mesmo nos momentos mais difíceis. Obrigado, mãe! Por me compreender mesmo quando não compreendia, por me amar incondicionalmente, por todo o seu cuidar e por me ensinar que a alegria da vida reside nas menores coisas. Obrigado, vó! Que agora na eternidade Deus esteja a te mostrar essas poucas linhas para você perceber como sempre, por toda a eternidade, carregarei o amor e a gratidão por você em meu coração. Sem você não teria chegado aqui, pois foi você quem me despertou o amor pelo saber. Obrigado Amanda, Gustavo e Julyana pelas brigas e risadas do dia a dia, sem as quais a loucura me tomaria.

Agradeço a todos os meus estimados amigos que estiveram comigo nessa jornada, alguns antigos e outros que conquistei. Sem vocês não teria chegado até aqui. Obrigado por cada risada e abraço neste que foi um tempo tão difícil.

Obrigado, Sérgião por dedicar tempo a me ajudar e por todas as suas palavras de incentivo, tu és referência em tudo para mim. Que a irmandade que nasceu na UFRJ perdure por todas as nossas vidas. Obrigado, Caíto, por todas as nossas prosas que permeiam esse trabalho e pelo carinho e a amizade que levarei para a vida. Obrigado aos irmãos que a vida me deu e que levarei pela vida, Diego e Eduardo, falar mais a vocês é desnecessário. Que venham muitos quilos de sal pela frente. Agradeço também às mães e ao pai que me deram esses irmãos e que me adotaram como filho. Obrigado, Zaninha, Tica e Expedito! Obrigado por cada conversa e risada.

Deixo meu especial agradecimento às professoras Monica e Tatiana, não só pelo conhecimento transferido e as amizade que surgiram, mas cujo o amor pela docência me

cativou. À professora Tatiana, deixo ainda um abraço repleto de carinho. Proporcional ao grau de importância que você teve para que eu chegasse ao fim dessa jornada.

Agradeço ao corpo docente do PEPI-UFRJ e levarei seus ensinamentos e humanidade por toda a vida.

E por último, gostaria de deixar um agradecimento sem medida ao meu orientador. Obrigado, Fiori! Agradeço a sua atenção dedicada, mas mais do que isso, agradeço por ser a fonte de inspiração intelectual que me conduziu a seguir a vida acadêmica e a ver o mundo por outras lentes através dos seus geniais escritos. Foi uma honra receber sua orientação e que nossas jornadas acadêmicas se cruzem novamente. Obrigado!!!

“As grandes concentrações econômicas pedem as concentrações de meios técnicos e o desenvolvimento da tecnologia [...] e de todas as vezes a ciência, por mais balbuciante que fosse, estava presente ao encontro.” (Braudel 1987, p. 13)

Resumo

Desde o ano de 2019, a tecnologia 5G vem ganhando cada vez mais espaço nos noticiários econômicos e políticos, bem como nos estudos acadêmicos. Tal fato não só é devido a sua importância no romper de uma nova era das tecnologias da informação e comunicação que é fundamental para um novo paradigma industrial. Mas se deve sobretudo às sanções impostas pelos EUA à Huawei, sob a alegação de espionagem em conjunto com o estado chinês. Tais acusações levam a indagações quanto aos interesses por trás das sanções estadunidenses. Ao mesmo tempo em que nossos olhos se voltam com facilidade e encanto às aplicabilidades que nos são anunciadas na automação das indústrias, veículos sem condutores e casas e cidades inteligentes; as aplicabilidades militares são igualmente vastas e capazes de influenciar de forma ainda imensurável o tabuleiro do poder global. Dentro desse cenário, o presente trabalho objetiva investigar as aplicabilidades econômicas e militares da tecnologia 5G e como as mesmas se correlacionam no campo do conflito geopolítico entre China e EUA num contexto de disputa hegemônica.

Palavras-chave: Huawei. China. EUA. Geopolítica do 5G. Cibersegurança. Hegemonia. Inteligência Artificial.

Abstract

Since 2019, 5G technology has been getting more attention in economic and political circles, as well as in academia. Part of the reason for this is that 5G technology is an essential element of the new age of information and communication technology (ICT), leading to the emergence of a new industrial paradigm. But the main reason for all the attention concerning 5G technology is the sanctions imposed by the US on the Chinese ICT firm Huawei, under the allegation of espionage in cooperation with the Chinese State. These accusations bring questions concerning the real interests behind the American sanctions. At the same time that our eyes easily focus on the interesting and appealing civilian applications of 5G technology, such as in the automation of industries, driverless vehicles, and intelligent houses and cities, the military applications of 5G are equally vast and capable of influencing in an immeasurable manner the global power board as it is now drawn. In this scenario, the present work investigates the economic and military applications of 5G technology and the way these technologies are correlated in the larger geopolitical conflict between China and the USA.

Keywords: Huawei. China. USA. 5G geopolitics. Cybersecurity. Hegemony. Artificial Intelligence.

SUMÁRIO

INTRODUÇÃO 12

1 – O CRESCIMENTO DA HUAWEI E O ESTADO CHINÊS 19

1.1 Nacionalismo econômico 20

1.2 O desenvolvimento tecnológico chinês 23

1.3 A atuação do Estado chinês e o crescimento da Huawei 25

2 – O 5G E UM NOVO MUNDO 33

2.1 A tecnologia 5G 43

2.2 Segurança nas redes 5G 45

3 – CIBERPODER 48

3.1 Ciberterritório 48

3.2 O ciberpoder 61

3.3 Dados – recursos estratégicos 77

4 – ESTADOS UNIDOS VS HUAWEI 85

4.1 As sanções à Huawei 89

4.2 Huawei e os impactos das sanções 95

5 CONSIDERAÇÕES FINAIS 102

6 REFERÊNCIAS 106

Introdução

Comumente, somos ensinados a pensar a história moderna como originária do impulso contra inercial da era das grandes potências europeias, relegando – quando a tanto – às sociedades orientais um papel secundário na história, quase mítico – no sentido mais cético que a palavra possa ter. Fato é, que ao olharmos regressivamente na história europeia, podemos concluir que parte do seu desenvolvimento cultural e científico está correlacionado com as suas interações com as sociedades muçulmanas, tendo a Europa bebido da fonte Islã tal qual essa bebeu durantes séculos do conhecimento chinês, através do comércio mútuo, da conquista e colonização (KENNEDY, 1996, p. 14). Tal troca deveu-se a centralidade oriental ao longo da história do mundo.

No passado, o efeito restritivo das civilizações orientais sobre quaisquer possíveis pretensões expansionistas territoriais "europeias" contra suas possessões, por vezes é extremamente naturalizado a ponto de se omitir a existência do que pode ser entendido como uma não intenção expansionista de grandes civilizações orientais. Uma vez que, as necessidades de suas populações eram atendidas pela fertilidade do seu território e pela coesão de sua estrutura administrativa (KENNEDY, 1996, p. 14).

Contudo, a incapacidade de alargar as fronteiras do que hoje é a Europa com terras orientais, tanto por conta dos desafios impostos pela coerção geográfica como pela incapacidade de enfrentar às civilizações que dominavam tais terras, cooperaram para o estado competitivo encontrado na Europa e as sucessivas guerras vivenciadas por tais povos no período pré-moderno.

Charles Tilly (1993, p. 127), um dos mais importantes pesquisadores sobre a origem do sistema estatal ao olhar para um mundo pré-moderno, traz que:

> os europeus seguiram uma lógica padronizada de provocação da guerra: todo aquele que controlava meios substanciais de coerção tentava garantir uma área segura dentro da qual poderia desfrutar dos lucros da coerção e mais uma zona-tampão fortificada, [...] para proteger a área segura. [...] Quando as potências adjacentes estavam perseguindo a mesma lógica, o resultado era a guerra.

Assim, as "zonas-tampão" configuram-se como mecanismos de defesa frente ao risco incessante das guerras decorrentes da expansão territorial dos seus vizinhos. Norbert Elias (1976) entende a expansão como uma necessidade das grandes potências, mesmo nos tempos de paz. Como Fiori (2004) bem sintetiza, as grandes potências continuaram a se expandir pois a guerra era uma possibilidade constante e inevitável das relações entre as grandes potências, sendo a conquista e o acúmulo de mais poder a única forma de se protelar a guerra. Como sentenciou Elias, "quem não sobe, cai". De modo que para Fiori

(2005, p. 68), “a guerra não está no fim do processo de expansão territorial: está na sua própria origem e acaba se transformando na sua primeira causa ou primeiro motor”.

Se o cenário de competição expansionista europeia compreendeu circunstâncias tanto interestatais, como intraestatais – exemplo dessas foi a dinâmica existente em Gênova entre a aristocracia rural que foi revigorada pela expansão comercial anterior ao século XIV e suas classes mercantis urbanas; a inovação também não se restringe a um único sentido, se fazendo presente no desenvolvimento tecnológico – bélico ou comercial – e também nas inovações das estruturas de acumulação de capital. (Arrighi 1996, p.113)

Ao olharmos para as cidades-Estados italianas, vemos que “o capitalismo milanês, veneziano e florentino se desenvolveram no sentido da gestão do Estado e de estratégias e estruturas cada vez mais “rígidas” de acumulação de capital” (Arrighi 1996, p.113). O capitalismo genovês, por outro lado, distintamente se deu por mercados, estratégias e estruturas de acumulação de capital com maior liquidez.

Fiori (2010, p. 140), traz como centro da sua teoria do Sistema Interestatal Capitalista que

> o verdadeiro ponto de partida do “sistema mundial moderno” são os “Estados-economias nacionais” que foram “inventados” pelos europeus e se transformaram em “máquinas de acumulação de poder e riqueza”, dotadas de uma “compulsão expansiva” maior do que a dos primeiros poderes e capitais que se formaram na Europa durante o “longo século XIII.

Indo além, Fiori (2010) define os próprios Estados como o “produto final” da acumulação de poder e riqueza que ocorreram nos séculos anteriores ao século XVI. Configurando-se a dinâmica expansionista como genótipo do neonato Sistema Interestatal Capitalista (composto na sua origem pelos Estados europeus). Embora tenha-se visto a diminuição das unidades soberanas e competitivas, bem como o aumento do equilíbrio de forças entre elas, a guerra seguiu sendo o modo mais importante de conservação e acumulação de poder, para Fiori (2010). A inovação do sistema repousava no fato que “as unidades envolvidas eram Estados e economias, articulados em um mesmo bloco nacional e com as mesmas ambições expansivas e imperialistas com relação aos demais “Estados-economias nacionais” do sistema” (FIORI, 2010, p. 140).

A destruição e a ocupação territorial não necessariamente precisavam ser o objetivo da conquista, podendo esse ser a submissão econômica de determinado território. Sendo, para Fiori (2010), a conquista e a monopolização de novas posições de poder político e econômico, ainda, a “mola propulsora” do novo sistema. O que se viu a partir dos séculos XVI e XVII foi uma centralização e monopolização, por parte dessas

unidades políticas vencedoras das guerras anteriores, do poder de tributação sobre territórios e populações extensas. Além disso, ocorreu o aperfeiçoamento da capacidade de emissão de moedas nacionais; criação de crédito e bancos sustentados nos títulos da dívida pública dos Estados (FIORI, 2010).

Como sintetiza Fiori (2008, p. 141), "no novo sistema, a produção e a riqueza interna de cada país passaram a ser uma condição indispensável de seu poder internacional." De forma que nesse novo sistema, o papel exercido pela competição expansionista acabou por impelir a "sociedade europeia" ao refinamento tecnológico – seja ele de impacto bélico ou comercial, gerando uma estrutura de acumulação de poder e capital sem precedentes, em especial após o que ficou conhecido como a Revolução Industrial.

Ao longo da história, podemos ver que "as grandes concentrações econômicas pedem as concentrações de meios técnicos e o desenvolvimento da tecnologia" (Braudel, 1987, p.13). O aprimoramento técnico naval permitiu à Europa vivenciar a era das grandes navegações e tornar-se centro do comércio do mundo. O desenvolvimento tecnológico "ocorreu com o Arsenal de Veneza no século XV, com a Holanda no século XVII, com a Inglaterra no século XVIII. E todas as vezes a ciência, por mais balbuciante que fosse, estava presente ao encontro." (BRAUDEL, 1987, p. 13) De igual forma esteve nas revoluções no modo de se viver, guerrear e acumular riquezas derivadas das descobertas química, elétrica, de petróleo e aço no século XIX e XX, bem como das inovações oriundas da microeletrônica, das novas fontes de energia e também da robótica, Internet e digitalização dos dados do cotidiano a partir da segunda metade do século XX.

Os ventos que hoje sobram trazem as novas de uma tenra era de inovações tecnológicas e de geração de capital que tendem a ser concentrados, novamente, pelos Estados mais poderosos. Entretanto, o novo arranjo de forças existente no Sistema Interestatal Capitalista é a novidade. Desde o surgimento desse sistema interestatal, a primazia internacional sempre foi euro-americana, porém, na terceira década do século XXI, a China não só anuncia seu desejo de deter a liderança tecnológica do mundo, como também desenvolveu a melhor versão da tecnologia propulsionadora de todo esse novo ciclo inovativo – o 5G, a nova geração de rede móvel.

A tecnologia 5G com sua capacidade de fluxos de dados praticamente instantâneos é tida como peça-chave na "Indústria 4.0", também chamada de a Quarta Revolução Industrial. A "Indústria 4.0" possibilitará uma integração mais fluída e "natural" entre equipamentos, elevando o mundo a um novo nível de robótica, gerando

cidades inteligentes repletas de veículos autônomos e casa "inundadas" por equipamentos interagindo via Internet das Coisas (*IoT* – sigla em inglês). Atualmente a Huawei, gigante chinesa das telecomunicações, detêm a melhor e mais barata versão da tecnologia de rede 5G.

Como elemento determinante na disputa do Poder Global, o 5G tem sido constantemente citado pelos mais diversos e importantes documentos do governo norte-americano. Os documentos de Estratégia de Segurança Nacional (*National Security Strategy* – NSS) de 2017, 2021 (de caráter interino) e de 2022, bem como a Ciberestratégia Nacional (*National Cyber Strategy*) de 2018 e Estratégia Nacional para Garantir o Plano de Implementação do 5G (*National Strategy to Secure 5G Implementation Plan*) de 2021 que fazem explícita menção a importância estratégica dessa tecnologia. Além disso, uma série de documentos foram produzidos pelos Estados Unidos impondo sanções que visam atingir a difusão da versão chinesa da tecnologia 5G tanto no território norte-americano como no cenário mundial.

Desde 2019, a Huawei sofre impactantes sanções por parte do governo dos Estados Unidos, sob a alegação de espionagem. Segundo o governo norte-americano, a tecnologia da empresa chinesa oferece risco aos EUA, uma vez que carregaria em si uma porta de acesso aos dados de seus usuários para uso da inteligência do Estado chinês, de modo que a sua participação na infraestrutura 5G do país ofereceria risco tanto aos usuários como também ao Estado norte-americano e ao seu complexo militar. Mesmo com tal lacuna planejada na segurança nunca tendo sido comprovada, a Huawei foi adicionada à lista negra do governo dos Estados Unidos. Tal medida não só impacta os negócios da empresa chinesa com gigantes companhias norte-americanas do setor de tecnologia, mas também com qualquer companhia que se valha de componentes tecnológicos cuja propriedade intelectual tenha ligação com os Estados Unidos. As sanções ainda alcançam a aferição de ganhos da Huawei decorrentes da sua participação no mercado financeiro.

A capacidade de ingerência na comunicação global tem sido de suma importância desde os primórdios do Sistema Interestatal, mas, para muito além disso, a tecnologia 5G se relaciona a incrementos de produtividade agrícola e industrial, gerando aumento de rentabilidade. Além disso, dada aos seus aspectos técnicos inovadores demanda o desenvolvimento de novos recursos de segurança. Com isso impacta o nível de segurança do eficaz funcionamento da Infraestrutura Crítica, que se configuram como serviços e bens cuja destruição resultariam em graves impactos a um Estado – tais como

as infraestruturas de comunicações, de energia, de transportes, de finanças e de águas. Porquanto cada vez mais esses serviços fazem uso da Internet e do Ciberespaço.

Sendo outra preocupação dos Estados, a digitalização do cotidiano de suas populações, a captação dessa massa imensurável de dados e a existência de capacidade de sua utilização para ingerência sobre o comportamento da população de um país alvo através do uso conjunto de algoritmos e Inteligência Artificial. A tecnologia 5G também tente a impactar ao exercício da guerra através da difusão e uso para fim bélico de veículos não tripulados por Estados mais fracos ou mesmo atores não estatais – como terroristas. De modo que a dinâmica do jogo do Poder Global tende a ser alterada em decorrência da ampla gama de inovações tecnológicas a serem impulsionadas pela tecnologia 5G nos próximos anos

O poder norte-americano tem sido amplamente estudado, com diversas interpretações sobre o momento pelo qual passa, bem como a própria ordem liberal mundial. Desde que ascendeu ao posto de desafiante da hegemonia inglesa, os EUA sempre estiveram na vanguarda tecnológica no tocante aos meios de produção, e isso é especialmente o caso em relação à infraestrutura da informação. O atual momento se desenha decisivo. As razões pelas quais os EUA aplicam sanções comerciais à Huawei, sob a alegação de proteção à segurança nacional, soam como verdadeiras, porém, como se pode concluir, por motivos mais abrangentes do que os alegados.

Como visto, Estados têm atuado de modo a expandir seu poder político e econômico através da conquista e monopolização de novas posições por longos séculos, sendo a obtenção de novos territórios e o exercício soberano sobre eles com fins a ampliar a dinâmica de acumulação de poder e capital de suma importância na dinâmica de poder do tabuleiro global. Embora desde o fim da Segunda Guerra Mundial não se tenha guerras anexadoras entre as grandes potências mundiais, entende-se que o caso em tela configura-se como uma disputa territorial entre grandes potências, dentre as quais se destacam sobremaneira os Estados Unidos e a China.

Sendo assim, defende-se que a disputa que envolve a tecnologia 5G é regida pelos mesmos argumentos discursivos que balizam as disputas territoriais desde a pré-modernidade: as grandes potências necessitam se expandir pois a guerra é mais que uma possibilidade, ela é inevitável nas relações entre as grandes potências, sendo a guerra unicamente constrangida pelo acúmulo de um poder de tal ordem que desencoraje aos adversários. Os Estados, portanto, têm se empenhado em expandir, o que pode ser

chamado de seus ciberterritórios, se valendo do argumento que é preciso atuar contra os riscos que ameaçam a segurança nacional.

Entretanto, embora seja possível a territorialização do ciberespaço, bem como transportar até certa medida a lógica territorial que fundou o Sistema Interestatal Capitalista, as assimetrias de poder são marcadas por características que estão intrinsecamente ligadas ao capital transnacional, o que possibilitou aos Estados Unidos a construção de um ciberterritório global dotado de poder supranacional de maneira inconteste. Sendo o caso em tela extremamente simbólico, uma vez que o 5G desenvolvido pelos ascendentes rivais chineses pode ser compreendido como expoente do primeiro caso de ameaça ao ciberterritório global norte-americano.

O grau de abstração necessário para compreensão do objeto de estudo como ente geográfico é o grande desafio à consecução dos objetivos propostos. Sendo fundamental o entendimento da infraestrutura da Internet como ligação entre as dimensões física, cognitiva e virtual. A essa dificuldade se soma o entendimento de como o capital está associado ao projeto de poder das grandes potências sobre a Internet e o Ciberespaço, bem como os países visam influenciar os comportamentos dos usuários.

Ademais, é necessário destacar a limitação característica da análise que ocorre contemporaneamente ao objeto de estudo. Sem tempo histórico decorrido suficientemente, a pesquisa se atém às evidências e aos fatos citados no trabalho de modo a entender as consequências até o presente momento. A limitação também se revela na literatura sobre a tecnologia 5G. As obras que abordam a nova tecnologia trafegam, em sua grande maioria, entre o tecnicismo do olhar da engenharia e a abordagem dos impactos econômicos previstos com a inserção da tecnologia no nosso dia a dia. As sanções dos Estados Unidos sobre a Huawei e seu 5G mobilizam a literatura desde 2019, entretanto cabe ressaltar que, mesmo centrando suas análises no aspecto da Cibersegurança, da espionagem e vigilância, com grande frequência desconsideram tais aspectos como parte de uma lógica maior e mais sofisticada de poder que foge ao discurso de neutralidade tecnológica e da moeda.

Tendo em vista as acusações que levaram as sanções, o primeiro capítulo versa sobre a ligação entre a Huawei e o Partido Comunista Chinês (PCCh). O capítulo aborda as políticas econômicas do Estado chinês, imbuídas pelo nacionalismo econômico, e como elas possibilitaram a Huawei alcançar a posição de liderança global no tocante ao 5G. Tendo o governo da China se valido de variadas estratégias de estímulo à demanda,

desde a absorção de tecnologia estrangeira ao estabelecimento de padrões favoráveis às companhias chinesas, passando por direcionamento de capital à Huawei.

O segundo capítulo aborda a característica disruptiva da tecnologia 5G, sua natureza propulsionadora de novas tecnologias, os seus aspectos técnicos inovadores e desafios decorrentes. Detendo-se primeiramente em como se relaciona com os vetores da nascente Indústria 4.0, passando para sua relação com algumas tecnologias bélicas e de vigilância. Por último, descreve-se os aspectos técnicos da tecnologia 5G e como alguns deles se configuram como desafios à cibersegurança.

O terceiro capítulo é dedicado à compreensão da Internet, sua infraestrutura e também do ciberespaço enquanto entes territoriais. Tendo em vista tal fim, o capítulo parte da origem do termo ciberespaço para compreender como as interpretações dadas a ele impactam a interpretação do 5G como parte da geografia do poder global. Essa primeira seção visa ofertar bases para a compreensão da segunda seção do capítulo que é dedicada ao Ciber militarismo norte-americano e as dinâmicas do Ciberpoder Global.

O quarto capítulo expõe as sanções que atingiram a Huawei e a tecnologia 5G desenvolvida pelos chineses, buscando entender seus objetivos e quantificar a efetividade de tal recurso. Para isso debruça-se sobre os documentos oficiais norte-americanos, bem como sobre os fatos que os antecederam e sucederam. A análise aborda o poder norte-americano sobre o setor financeiro e também sobre a cadeia produtiva de semicondutores, aborda-se como tais condições de poder afetam a produção e difusão de equipamentos chineses necessários na construção da infraestrutura 5G.

1 – O crescimento da Huawei e o Estado chinês

O economista francês Jean Baptiste Say formulou, no século XIX, um axioma que ficou conhecido como Lei de Say. Segundo a qual, “um produto, tão logo seja criado, nesse mesmo instante gera um mercado para outros produtos em toda a grandeza de seu próprio valor” (SAY, 1803, p. 138), de forma que as funções de oferta e de demanda coincidem e tendem ao equilíbrio geral (inclusive de pleno emprego) nas economias de livre mercado. A visão que a oferta cria a sua própria demanda pressupõe a venda de todas as mercadorias produzidas, uma vez que a produção gera renda em proporção suficiente para tal. Entende-se, portanto, que o aumento das condições de oferta gera um impulso ao crescimento da economia

Porém, segundo Kalecki (1977), por meio do Princípio da Demanda Efetiva, as decisões de gastos determinam a renda. Sendo assim, os agentes econômicos não são capazes de determinar a sua própria renda, mas, por outro lado, conseguem estipular o quanto podem gastar. Em caso dos agentes como um todo reduzirem seus gastos, a economia acaba por ser conduzida para uma situação em que a demanda efetiva é insuficiente, o que resulta em depressão de emprego e renda. Dessa forma, a demanda detém um papel dinâmico na economia, a despeito da oferta e da Lei de Say.

Ao olhar para os problemas e desafios do crescimento em países subdesenvolvidos, Kalecki (1993b, p. 16) enxerga que

> O problema crucial enfrentado pelos países subdesenvolvidos é, portanto, ampliar consideravelmente os investimentos [...]. Há, no entanto, três importantes obstáculos ao aumento dos investimentos. Primeiro, é possível que o investimento privado não esteja disponível em ritmo adequado. Em segundo lugar, podem faltar recursos físicos para produzir mais bens de investimento. Em terceiro lugar, mesmo se essas duas dificuldades forem superadas, existe ainda o problema da oferta adequada de produtos de primeira necessidade para suprir a demanda resultante do aumento do emprego.

Kalecki (1993a, p. 29) ao criticar a visão segundo a qual é "a falta de mercados adequados [que é] o principal obstáculo ao desenvolvimento, mais do que a inflação” traz o pensamento que "[...] se o investimento for suficientemente alto, ele impulsionará a demanda por bens de consumo”. Assim, o alto nível de investimento é fator gerador de demanda por bens de consumo.

Como destaca Medeiros (2010, p.463), “as transformações estruturais da economia chinesa se deram a partir de uma dinâmica macroeconômica em que os investimentos foram o principal componente e indutor do ciclo econômico.” O Estado chinês exerceu papel de liderança e coordenação no tocante aos investimentos. Esta

liderança se deu de maneira direta quanto a alocação de investimentos e indiretamente no tocante a sistemas de incentivo via políticas macroeconômicas, políticas sobre crédito, políticas tecnológicas e políticas de preços.

Abordaremos o processo de mudança ocorrido no setor de Tecnologia da Informação e Comunicação (TIC) de modo a demonstrar como o êxito da política do Estado chinês em desenvolver o setor via estímulo da demanda através de investimento e políticas protetivas se correlaciona com o debate proposto por Helleiner (2002) sobre nacionalismo econômico.

1.1 Nacionalismo econômico

Helleiner (2002) ao voltar seu olhar para o tema do nacionalismo econômico, a abordagem acadêmica quanto ao tema e também o seu uso compartilha a percepção de uma utilização ambígua do termo. De modo que o termo tem sido usado por economistas e formuladores de políticas liberais para descrever e desacreditar políticas com as quais discordam. Quadro que se dá, segundo o autor, a despeito de poucos estudos acadêmicos sérios quanto ao tema ao longo do século XX.

No campo da Economia Política Internacional, especificamente desde a década de 1970, a expressão “nacionalismo econômico” começou a ser usada como uma variação econômica da ideologia realista tão em voga no contexto da Guerra Fria (HELLEINER, 2002). Robert Gilpin (1987, p. 31), descreve o nacionalismo econômico da seguinte maneira: “Sua ideia central é que as atividades econômicas são e devem ser subordinadas ao objetivo de construção do Estado e os interesses do Estado”.

Em **Global Political Economic** (2001, p. 14), Gilpin argumenta que o núcleo analítico do nacionalismo econômico é o mesmo do “realismo estadocêntrico”; ele “reconhece a natureza anárquica dos assuntos internacionais, a primazia do Estado e seus interesses nos assuntos internacionais e a importância do poder nas relações interestatais”. Sendo, nessa forma de pensar, o nacionalismo econômico uma tradição de pensamento estatista que tem suas raízes nas doutrinas mercantis dos séculos XVII e XVIII. Definição que recebe críticas como a feita por Crane (1998), Abdelal (2001) e Shulman (2000) que entendem poder haver diferença entre interesse da nação e os interesses dos Estados. Existe uma distinção entre nacionalismo econômico e mercantilismo, “uma vez que a ideologia estatista deste último era bem diferente das ideias nacionalistas mais modernas que surgiram no século XIX” (HELLEINER, 2002, p. 310).

Abdelal (2001, p.33) traz que o nacionalismo econômico deveria ser definido como “um conjunto de políticas que resulta de uma identidade nacional compartilhada, ou da predominância de um nacionalismo específico na política de um Estado”. Crane (1999, p. 215), por sua vez, sugere que o nacionalismo econômico é uma “faceta da identidade nacional”. Shulman (2000) mostra, inclusive, como objetivos nacionalistas como a promoção da unidade, identidade e autonomia de uma nação podem ser buscados através de políticas econômicas que podem incluir o livre comércio.

Como conclui Helleiner (2002, p. 311, tradução nossa):

> O argumento de que o “nacionalismo econômico” poderia ser usado para descrever o endosso de uma variedade tão ampla de políticas, incluindo as liberais, sem dúvida seria controverso para muitas pessoas. Mas segue logicamente do primeiro argumento que a definição de nacionalismo econômico deve ser derivada de identidades nacionais e nacionalismo. Uma vez que as identidades nacionais são tão variáveis e mudam ao longo do tempo e do lugar, devemos esperar o mesmo das políticas que os nacionalistas econômicos endossam.

Ao revisar List, autor nacionalista mais importante do século XIX, Helleiner (2002) entende que List apresenta uma definição semelhante a visão dos autores citados anteriormente. Segundo o autor, o problema dos liberais econômicos residiria no fato que eles avaliam a política econômica principalmente do ponto de vista dos indivíduos e do bem-estar da humanidade como um todo. “Entre cada indivíduo e toda a humanidade, no entanto, está a nação” (LIST, 1904, p. 141). Estando isso no centro da disputa de List com os liberais: “Eu indicaria, como característica distintiva do meu sistema, a nacionalidade. Na natureza da nacionalidade, como interesse intermediário entre os do individualismo e da humanidade inteira, toda a minha estrutura se baseia” (LIST, 1904, p. 142).

Sendo assim, o pensamento de List entende que os indivíduos são cidadãos e membros de nações, não devendo o objetivo da política econômica se limitar à maximização da riqueza, mas devendo incluir também o desenvolvimento da cultura e do poder de uma nação (HELLEINER, 2002, p. 311). Entretanto, o pensamento ‘listiano’ de nacionalismo econômico não era a única forma existente no século XIX.

Segundo Helleiner (2002), para Thomas Attwood, um banqueiro e político de classe média de Birmingham, era preciso atacar as políticas monetárias liberais, pois ele entendia que o padrão-ouro corroeria a ‘lealdade nacional’ em tempos de guerra, minando a capacidade do Estado de atender às necessidades econômicas domésticas da nação. Já em nomes como Johann Fichte e Adam Muller temos a defesa da ideia de autarquia, uma vez que ela poderia servir melhor às necessidades econômicas domésticas (Fichte) ou reforçar identidades nacionais coletivas (Muller) (HELLEINER, 2002). Também era

possível encontrar nacionalistas econômicos que acreditavam nas políticas econômicas liberais servindo aos objetivos nacionalistas. Segundo Helleiner (2002, p. 322), “em alguns contextos, a adoção do livre comércio ou do padrão-ouro foi vista pelos nacionalistas como ferramentas para reforçar o desenvolvimento econômico nacional e o poder nacional de várias maneiras.”

Determinadas políticas acabaram por conquistar o apoio nacionalista devido a sua associação ao prestígio nacional ou seu vínculo com projetos políticos destinados a fortalecer identidades nacionais nascentes ou refletir as existentes. Não representando os nacionalistas econômicos um desafio político para os liberais econômicos, mas sim grandes aliados políticos no projeto de introdução de políticas de livre comércio e/ou padrão-ouro. Apesar de o endosso dos nacionalistas econômicos ocorrerem por razões “erradas” do ponto de vista econômico liberal (HELLEINER, 2002).

Segundo Helleiner (2002, p. 324), “a lição a ser tirada dessa história é que haverá muitos projetos de política econômica nacionalista na era contemporânea, alguns dos quais desafiarão o liberalismo econômico e outros não.”

Reich (1991), argumenta que o contexto de uma economia globalizada tende a afastar os nacionalistas econômicos das políticas protecionistas do passado para o Estado que se concentra em grandes investimentos públicos em educação e infraestrutura. Helleiner (2002) ao olhar para a argumentação feita por Reich (1991) antevê que “aqueles que empregam uma definição convencional de nacionalismo econômico podem ver seu livro como uma rejeição do ‘nacionalismo econômico’”. Entretanto, ao compartilhar sua interpretação do texto, Helleiner identifica que seu argumento se mantém na tradição de pensamento nacionalista econômico ‘listiano’, uma vez que Reich argumenta que as mudanças nas condições do mundo exigem novas ferramentas políticas para alcançar o mesmo nacionalismo.

Parece-nos possível concluir, ao olharmos para o caso econômico chinês, que as políticas que possibilitaram o desenvolvimento econômico e tecnológico da China nas últimas décadas reificam a visão de um nacionalismo econômico que assuma diversas formas na contemporaneidade. Tendo sido possível à China transformar em ferramenta de barganha a sua posição de grande importância na cadeia global de valor. Usando sua inserção na estrutura da economia liberal mundial aos seus interesses nacionalistas econômicos. Melhorando as condições de vida da sua população e aumentando o seu poder no tabuleiro global.

Ganhos de poder que ficam claros nas pretensões expostas por Xi Jinping, líder máximo da China, em 18 de outubro de 2017. Quando em seu discurso anunciou uma "nova era", apresentou cronogramas para o rejuvenescimento da China em 2049, prometeu maior ativismo chinês na governança global, pediu militares de "classe mundial", comprometeu a China a se tornar um "líder global em inovação" e declarou que a China "se tornaria um país líder em força nacional abrangente e influência internacional". Uma "nova era" onde "vê a China se aproximando do centro do palco do mundo".

1.2 O desenvolvimento tecnológico chinês

Nas últimas três décadas, nenhum país se desenvolveu mais que a China. Nesse período, a China transformou-se em: segunda maior economia, maior exportadora, segunda maior importadora e detentora das maiores reservas internacionais (US$3,8 trilhões, aproximadamente) (LEÃO, 2015, p.10). Tal mudança se deve às políticas de industrialização, de inserção nas cadeias produtivas regionais e globais, de suprimento de energia, de gestão da moeda e do crédito, de distribuição de renda e de redução das desigualdades regionais, de ciência, tecnologia e inovação, de modernização do aparato militar e dos sistemas de defesa, de apoio à internacionalização das empresas e de financiamento da infraestrutura no entorno asiático, e de atuação nas instituições multilaterais. Tais políticas estão articuladas em uma ampla estratégia de desenvolvimento de curto, médio e longo prazo.

Como detalha Nogueira e Qi (2022, p.230), o desenvolvimento chinês é fruto das reformas iniciadas em 1978, esse processo pode ser dividido analiticamente em três períodos de características próprias: de 1978 a 1991, a etapa inicial que se concentrou nas zonas rurais e introduziu lentamente mecanismos de mercado na economia; de 1992 a 2008, etapa responsável por pelas grandes transformações estruturais do modo de produção; e de 2009 (após a grande crise financeira de 2007/08) até a eclosão da pandemia do Covid-19.

As reformas durante o primeiro período (1978-1991) foram responsáveis por uma grande oferta de incentivos e também pela formação de uma economia de mercado que coexistisse com o sistema de planejamento. Nesse período a grande maioria da riqueza produtiva do país ainda se concentrava fora da zona urbana, sendo as empresas de vila e município (TVEs) de grande importância na geração dessa riqueza. Entretanto, é também

nesse período que uma parcela menor, mas crescente, dos camponeses inicia o processo de migração do campo para a cidade a fim de trabalhar em empresas de capital externo nas zonas econômicas especiais (ZEEs).

A segunda fase (1992-2008), é marcada pelo emergir de uma classe capitalista privada doméstica, por um processo de privatização maciça de bens estatais e coletivos e a expropriação de terras. Tendo ocorrido um aumento nas participações do capital privado e do Estado na renda nacional (NOGUEIRA; QI, 2022).

O terceiro estágio (2009 até a presente data) corresponde ao que os autores chamam de 'aliança tensa'. O termo 'aliança tensa' refere-se às "contradições internas que passaram a impor pressão sobre a relação entre o capital privado e o Estado, reduzindo seus interesses comuns e intensificando os conflitos" (NOGUEIRA; QI, 2022, p.231). Ante o cenário de abalo e instabilidades após a grande crise financeira de 2007/08, as disputas estratégicas com os Estados Unidos, que abarcavam os âmbitos comercial, tecnológico e militar, levaram a um fortalecimento da aliança entre o Estado e as diferentes frações da burguesia e levou a uma nova onda de centralização do poder político.

Em um olhar retrospectivo é possível perceber que desde a reabertura, a política industrial chinesa tem visado integrar-se competitivamente e também ascender nas cadeias de produção global. Se valendo para tal da combinação de estratégias de integração nas cadeias de valor globais com a formação de "campeões nacionais" em setores julgados estratégicos por seus líderes. Existindo no momento esforços para construir uma base de inovação nacional a fim de que a propriedade intelectual dos produtos e serviços comercializados nas cadeias globais sejam pertencentes às empresas chinesas (NOGUEIRA, 2015, p.58).

A política industrial inclui um estrito controle do sistema financeiro pelo Estado, o que se deu através de um amplo conjunto de políticas macroeconômicas voltadas ao desenvolvimento industrial: uma taxa de câmbio favorável às exportações, controle sobre a conta de capitais, crédito subsidiado, incentivos fiscais, taxa de juros baixa. Tais políticas caminham alinhadas com um apoio ao desenvolvimento de "campeões nacionais" em setores estratégicos, tais como petróleo, siderurgia, construção civil, ramos militares e tecnologia da informação (MEDEIROS, 2010).

Em sua busca por uma maior e melhor inserção competitiva nas cadeias de valor globais, o projeto de desenvolvimento chinês buscou atrair tecnologia e capital estrangeiros. Para isso desenvolveu as zonas econômicas especiais e enfatizou grandes

investimentos em infraestrutura, gerando uma demanda efetiva, fortes acréscimos de competitividade industrial e redução dos custos com links de serviços. A regulamentação que regeu a abertura chinesa aos investimentos externos diretos (IEDs) visava a constante tentativa de absorver tecnologia e modos de produção estrangeiro a fim de obter uma modernização industrial e militar (NOGUEIRA, 2015).

Entendamos absorção tecnológica como a capacidade de difundir uma tecnologia internamente, de modo que a mesma seja base do processo criativo de novas tecnologias e processos. Comumente, as firmas estrangeiras conseguem impor suas vontades e o compartilhamento técnico não ocorre; porém a China obteve sucesso e os IEDs vieram acompanhados de conhecimento codificado (licenciamento, compartilhamento de Design, aplicação de patentes, fórmulas) e de know-how (estilo gerencial, processos e treinamentos de empregados). Tal excepcionalidade deveu-se à capacidade chinesa de atender o anseio das firmas por redução de custos de produção, bem como a seu enorme mercado doméstico (NOGUEIRA, 2015).

A partir da década de 1990, a estratégia chinesa para induzir absorção tecnológica adotou medidas restritivas das importações de bens finais por meio de barreiras tarifárias e não tarifárias, o que se deu de forma concomitante à criação de políticas favoráveis à entrada de capital estrangeiro. As regulações muito restritas em tal período visavam o catch-up de firmas domésticas, isto é, o desenvolvimento tecnológico nacional a partir, dentre outras coisas, das barreiras comerciais, do financiamento público a empresas nacionais, e da absorção da tecnologia das empresas estrangeiras. Sendo as compras públicas, ainda nos últimos anos, um importante instrumento impulsionador das marcas chinesas. As compras públicas equivaleram a 3,5% do PIB em 2016.

Uma das exigências para a existência de IED era a formação de joint-ventures, onde ao menos metade do capital deveria ser chinês e diferentes esferas governamentais deveriam ser consultadas para aprovar sua formação. Além de constar no contrato da formação da sociedade das joint-ventures a previsão de transferência tecnológica. Tal estratégia se justifica pela existência de um canal mais estreito de interação técnica-administrativa (NOGUEIRA, 2015).

1.3 A atuação do Estado chinês e o crescimento da Huawei

Nos primeiros anos da década de 1980, os engenheiros chineses não apresentavam conhecimento e experiência significativa no tocante à produção, design ou

desenvolvimento de centrais digitais de telecomunicações. Em 1983, após 33 meses de negociações que envolveram os governos chinês e belga, o antigo Ministério de Correio e Telecomunicações da China, a estatal Corporação Industrial de Correios e Telecomunicações, vinculada ao Ministério de Correio e Telecomunicações, e a belga *Bell Telephone Manufacturing Company* (BTM), uma antiga subsidiária da estadunidense *International Telephone and Telegram Corporation* (ITT), formou-se a primeira joint-venture no ramo de telecomunicações na China – a *Shanghai Bell Telephone Equipment Manufacturing Corporation* (NOGUEIRA, 2015, p.64-65).

O longo tempo de negociações entre as partes deveu-se à costura do primeiro grande acordo de transferência de tecnologia de ponta da China moderna. O acordo continha "exigências de transferência de tecnologias para a produção local dos principais componentes do Sistema-12 utilizado na época, incluindo um chip LSI (circuito integrado de larga escala) customizado, unidades computadorizadas de teste e tecnologia de produção de circuitos impressos." (NOGUEIRA, 2015, p. 65).

A formação da Shanghai Bell possibilitou tanto a manufatura e operação de equipamentos contendo tecnologia de ponta na época, como também que se recebesse os devidos treinamentos. Além disso, a Shanghai Bell investiu diretamente na formação de profissionais e na cooperação com universidades locais e institutos de pesquisa para suprir as demandas da adaptação do Sistema-12.

A instalação do Sistema-12 levou a que fossem requeridos funcionários do corpo técnico do Ministério de Correios e Telecomunicações, que após um período junto à Shanghai Bell retornavam aos seus postos de trabalho junto ao ministério – o mesmo se deu com técnicos e pesquisadores de órgãos estatais. As próprias estatais chinesas requereram auxílio direto à Shanghai Bell para questões operacionais e administrativas, bem como se beneficiaram do envio de missões que exploraram os métodos de gestão das multinacionais (NOGUEIRA, 2015).

Segundo Mu e Lee (2005), o conhecimento absorvido na Shanghai Bell acabou por ser de suma importância para a consecução do desenvolvimento de uma central digital de tecnologia e padrão chineses. Em 1992, a *Great Dragon*, estatal chinesa, lançou o HJD-04, o primeiro sistema para centrais digitais desenvolvido na China. A absorção de conhecimento por meio de institutos de pesquisas chineses e por empresas competidoras da Shanghai Bell – que captavam anualmente entre 3% e 4% dos engenheiros da joint-venture – foi de suma importância para o estabelecimento de empresas como a ZTE e a Huawei (MU; LEE, 2005; NOGUEIRA, 2015).

O HJD-04 foi desenvolvido inicialmente para atender exclusivamente ao interior e às zonas rurais, regiões nas quais o padrão tecnológico do Sistema-12 encontrava limitações. Porém, apoiado pela geração de receita no interior rural e por políticas estatais protetivas – tal como padrões técnicos e compras públicas – o sistema HJD-04 obteve um rápido crescimento pelo país; de forma que em 1998 a Huawei – uma das empresas líderes chinesas que empregava o HJD-04 – ultrapassou a Shanghai Bell na venda de centrais digitais no território chinês (MU; LEE, 2005; NOGUEIRA, 2015).

Como Nogueira (2015, p. 67) detalha, o desenvolvimento da indústria eletrônica foi uma das prioridades explícitas do corpo principal de políticas de ciência, tecnologia e inovação do governo chinês. No período compreendido entre as décadas de 1980 e 1990, os três principais programas nacionais visando o desenvolvimento e a promoção de setores de alta tecnologia, inovação e ciência pura – Programa de Desenvolvimento e Pesquisa de Tecnologias-Chave (lançado em 1982), o Programa Nacional para Pesquisas Avançadas (Programa 863, lançado em 1986) e o Programa para o Desenvolvimento de Pesquisa Básica Nacional (Programa 973, lançado em 1998) – deram ênfase à indústria eletrônica. Sendo a criação do Ministério da Indústria Eletrônica, em 1982, que em 1998 passou a ser chamado de Ministério da Indústria de Informação, em 1998, outra importante evidência da importância conferida pelo governo chinês ao setor eletrônico.

De modo que o Programa Nacional de Política Industrial para os anos 1990 declarava a indústria eletrônica como um dos “pilares”. Em 1994, o Programa Nacional de Política Industrial declarou a indústria eletrônica como uma das indústrias pilares e condicionou por uma década o acesso de investidores estrangeiros ao mercado chinês à transferência de tecnologia. O objetivo do plano era fazer da indústria eletrônica, juntamente com os setores de máquinas, petroquímico, automóveis e materiais para construção, os motores principais do crescimento contínuo industrial chinês (NOGUEIRA, 2015).

A fim de alcançar o desenvolvimento almejado, o Estado chinês usou amplamente, desde a década de 1990, a estratégia de direcionar seu enorme investimento em infraestrutura aos cofres das empresas nacionais. Para tal, optava por padrões técnicos que as empresas chinesas pudessem atender e que por vezes empresas estrangeiras não utilizassem. Um exemplo foi o conjunto de projetos de fomento a criação de uma ampla infraestrutura de tecnologia de informação – apelidado de Projetos de Ouro (*Golden Projects*). Os projetos visavam o estabelecimento de redes de comunicação de fibra óptica para uso do setor bancário, alfândega e coletores de impostos, informação médica e de

saúde e redes universitárias e científicas; para tal enfatizaram a utilização de padrões tecnológicos, serviços e produtos de firmas chinesas (NOGUEIRA, 2015, p.72).

Os padrões adotados não se correlacionavam apenas com as compras públicas, mas alcançavam todo o mercado interno; o caso do padrão V5 é um exemplo dessa readequação direcionada a ganhos das firmas nacionais.

O padrão V5 era utilizado em sistemas de comutação de grandes capacidades para centrais telefônicas, tendo sido desenvolvido por um conjunto de firmas chinesas, dentre as quais estavam a ZTE e a Huawei. Estando este padrão restrito ao interior rural da China, onde as empresas chinesas atuavam sem competição estrangeira, até o governo chinês alterar os padrões e estipular que os novos sistemas de comutação vendidos em todo o mercado chinês deveriam ser compatíveis com a interface V5.1. Tal mudança resultou em uma rápida expansão das empresas chinesas do segmento, visto que as empresas estrangeiras, geralmente não produziam sistemas compatíveis com tal interface. Além dos regulamentos técnicos, em 1995, o governo proibiu a importação de grandes sistemas de comutação financiados por empréstimos de governos estrangeiros.

Os empréstimos de governos estrangeiros foram muito úteis no apoio às empresas no exterior para ocuparem o mercado chinês na década de 1980 e início de 1990, como se deu no estabelecimento no mercado de dispositivos de comutação na China das empresas que formaram o que passou a ser descrito como "sete países com oito sistemas", referindo-se aos sistemas pertencentes à NEC, FUJTTSU, AT&T, Nortel, Ericsson, Siemens, BTM e Alcatel, empresas originárias do Japão, EUA, Canadá, Suécia, Alemanha, Bélgica e França (Zhao et al. 2007). No final da década de 1990, o sistema de comutação controlado por programa de marcas domésticas detinha 80% do mercado chinês. Marcas estrangeiras foram forçadas a se retirar do mercado chinês, onde antes dominavam e desfrutavam de lucros substanciais. O preço do equipamento caiu de US$300 a US$500 por linha no início de 1990 a US$30 por linha (ZHAO et al., 2007, p. 42; NOGUEIRA, 2015).

Outro exemplo emblemático é a mudança de diretrizes no Ministério de Correio e Telecomunicações. Inicialmente, como vimos, fora especialmente ativo na disseminação de tecnologia estrangeira para o setor de telecomunicações; porém na década de 1990, passou a estimular as firmas emergentes chinesas via compras públicas. O montante investido na segunda compra pública nacional coordenada para o setor de telecomunicações da China, entre 1997 e 1998, acabou sendo absorvido em grande parte pela Huawei, responsável pela instalação de 6.506 milhões de linhas, ou 40% do total de

solicitações do período. Além disso, para garantir o atendimento dos pedidos, a Huawei foi contemplada com uma linha de crédito de RMB 3,85 bilhões concedidos pelo Banco da Construção da China (*China Construction Bank*), o que representou 45% do total de créditos concedidos pelo banco em 1998 (MU; LEE 2005, p. 778; NOGUEIRA, 2015).

É importante salientar que, ao se falar de políticas públicas do governo chinês voltadas ao desenvolvimento da indústria eletrônica, estas geralmente se concentram em computadores e periféricos, eletrônicos de consumo, componentes eletrônicos e equipamentos de telecomunicação. Tendo o segmento de equipamentos de telecomunicações se beneficiado amplamente das políticas de desenvolvimento do governo chinês – principalmente a partir do lançamento do Programa Nacional de Médio e Longo Prazo para Desenvolvimento de Ciência e Tecnologia.

Lançado em janeiro de 2006, o Programa Nacional de Médio e Longo Prazo para Desenvolvimento de Ciência e Tecnologia (MLP, na sigla em inglês) visava articular pesquisa básica e aplicada em áreas-chave e em fronteiras tecnológicas com megaprojetos nacionais, reforma institucional do sistema nacional de Ciência e Tecnologia (C&T) e políticas públicas de promoção da inovação nacional. A China mudava seu foco estratégico de crescimento, priorizando atividades voltadas à inovação tecnológica ao invés da indústria e agricultura tradicional (FREITAS, 2011).

Um dos objetivos do MLP era promover a ascensão das empresas chinesas nas cadeias globais de valor através da propriedade intelectual própria. Embora se tenha alcançado grandes avanços na área de C&T desde a década de 1980, o MLP intentava enfrentar problemas do desenvolvimento científico e tecnológico chinês, como por exemplo a elevada dependência de tecnologia estrangeira e o fraco desempenho em inovações de tecnologias comercializáveis. Além do mais, a capacitação tecnológica chinesa não possibilitava o suficiente atendimento às necessidades do país em áreas como energia, água e utilização de recursos, proteção ambiental e saúde pública.

Outro ponto considerado insuficiente era no tocante aos armamentos nucleares e as conquistas aeroespaciais, bem como a capacidade inovadora chinesa em tecnologias relacionadas à defesa nacional, existindo uma grande dependência de tecnologias importadas. Outro ponto problemático, como detalha Freitas (2011), era a própria ciência chinesa, cujos ganhos e progressos quantitativos em termos de *funding* e de pessoal alocado em pesquisa científica nem sempre se apresentavam os resultados esperados, "gerando grande insatisfação na classe política, em razão da baixa tolerância da cultura

chinesa com o fracasso, e suscitando, em um círculo vicioso, condutas científicas inapropriadas" (FREITAS, 2011, p. 6).

O foco se voltou para segmentos estratégicos da fronteira tecnológica, nichos considerados estratégicos para o desenvolvimento nacional continuado e nos quais o desenvolvimento tecnológico global é apenas de nível intermediário e ainda não consolidados – existindo a possibilidade de deter a propriedade intelectual dos produtos, como no caso de biotecnologia, proteção ambiental, novas gerações de produtos de informática (como novas gerações de rede e *cloud computing*), novas energias, novos materiais, veículos movidos a novas energias e equipamentos de alto nível (desde aviões e trens de alta velocidade até satélites).

Uma busca cada vez mais frequente de políticas alternativas para a promoção de tecnologia nacional pôde ser vista nos anos posteriores ao lançamento do MLP, como no apoio chinês à adoção da tecnologia 3G TD-SCDMA. A tecnologia TD-SCDMA é um dos três padrões internacionais de terceira geração existentes para telefonia móvel. Após um cenário de intensa disputa entre operadoras domésticas, fabricantes estrangeiros e fabricantes nacionais – entre as quais novamente estavam a ZTE e a Huawei – o governo chinês optou pelo padrão TD-SCDMA que fora desenvolvido por um instituto de pesquisa estatal (Datang) e que sofreu resistência das fabricantes estrangeiras e também das operadoras nacionais. O padrão não apenas foi adotado, como também o governo apoiou as fabricantes chinesas via linha de crédito e por meio de subsídios (NOGUEIRA, 2015).

Fato é que a China, em pouco mais de três décadas, saiu de uma condição de extrema pobreza para se tornar não só a segunda maior economia do mundo, mas também se tornar um Estado com uma enorme capacidade de investimentos. Hoje, o país acumula mais de US$5 trilhões em reservas internacionais no *People´s Bank of China* – o Banco Central chinês – e seus demais bancos estatais possuem uma enorme capacidade de aporte financeiro aos projetos de expansão chineses. Como exemplo temos os patrimônios líquidos do *China Development Bank* (CDB) superior a US$2,3 trilhões, do Industrial & *Commercial Bank of China*, cerca de US$4,3 trilhões, do Bank of China, superior a US$3,2 trilhões, e o *do China Investment Corporation*, acima de US$1 trilhão.

Toda essa capacidade tem servido às políticas de internacionalização da China em suas diversas dimensões, sendo uma delas os empréstimos concedidos a países, em especial da África e da Ásia, para investimento em infraestrutura. Empréstimos esses, em grande parte, condicionados às compras de bens e serviços chineses, que acabam por gerar ganhos com os juros da operação e promover o crescimento e a globalização das

principais empresas chinesas. Um dos segmentos que tem se beneficiado da estratégia é o da telecomunicação. Exemplo disso foi a construção pelas empresas ZTE e Huawei, na Etiópia, de uma rede nacional de telefonia e internet, em acordo com o provedor estatal local e com apoio dos chineses na prestação de serviços (BURLAMAQUI, 2015).

Como definido em Burlamaqui (2015, p.317): "O financiamento público e, em última instância, o Estado empreendedor (schumpeteriano) chinês foram os principais atores responsáveis pelo sucesso dessas empresas, respaldando seu processo de modernização tecnológica e de internacionalização." Em 27 de dezembro de 2004, em Pequim, a Huawei e o CDB (*China Development Bank*) assinaram um acordo de US$10 bilhões visando a internacionalização da companhia. Posteriormente muitas outras linhas de crédito do CDB foram concedidas aos clientes da empresa no mundo em desenvolvimento, o que lhe permitiu conquistar uma parcela significativa destes mercados. Tendo a relação entre Huawei e CDB se estreitado, em 205, via assinatura de um contrato de partilha de riscos e passaram a compartilhar informações sobre clientes e projetos. Tais movimentos se reverteram em frutos já em 2005, quando o grupo Vodafone, a maior empresa de telefonia móvel do mundo, aprovou a Huawei como o primeiro fornecedor chinês de equipamentos para sua rede (SANDERSON; FORSYTHE, 2013, p. 160).

Após o apoio do CDB à sua penetração em mercados externos, a Huawei apresentou um salto nas suas vendas no exterior, saindo da ordem de US$20 bilhões no ano de 2004 para cerca de US$60 bilhões já no ano de 2006 (Gráfico 1). Em 2012, a Huawei já era a maior fabricante de equipamentos de telecomunicações; estava envolvida na Europa com mais da metade das redes de telecomunicações super-rápidas 4G, sendo também uma forte concorrente em telefones celulares; na África, o baixo custo de seus equipamentos havia ajudado a um grande salto no tocante a telecomunicação móvel (BURLAMAQUI, 2015, p.317).

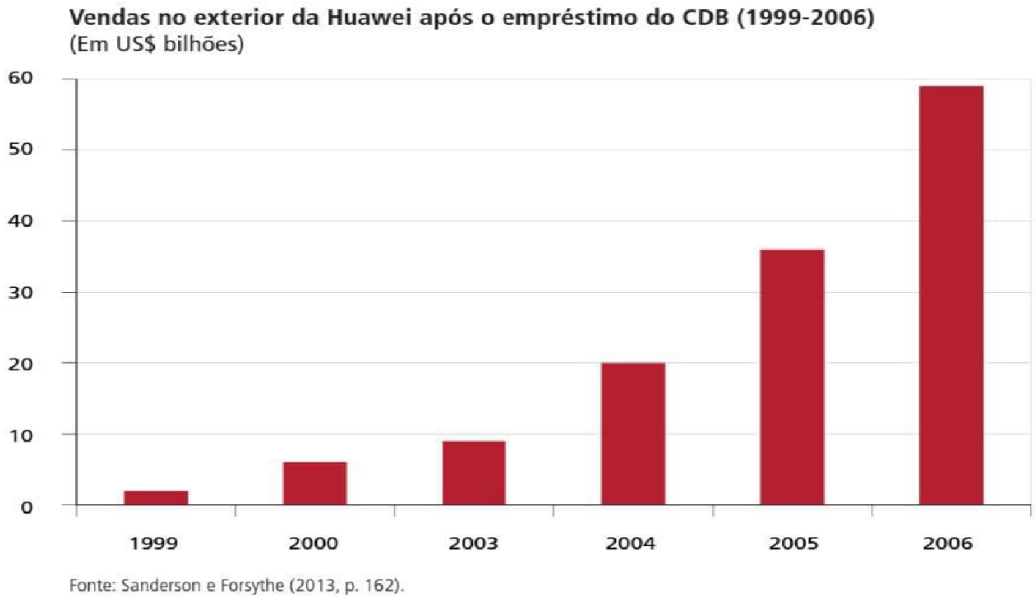


Gráfico 01

Com o forte apoio das políticas de desenvolvimento do Estado chinês, a Huawei passou de uma empresa com dificuldades para ganhar clientes, mesmo na China, a maior empresa de fabricação de equipamentos de telecomunicações do mundo – ultrapassando a Ericsson no ano de 2012. Segundo o seu relatório anual de 2019, a Huawei teve uma receita de cerca de US$123 bilhões e investiu cerca de US$18,6 bilhões em P&D, fechando o ano com mais de 85 mil patentes registradas. O crescimento vertiginoso da Huawei no cenário internacional, pode ser visto como um exemplo de sucesso de todo apoio e estratégia chinesa. Levando uma empresa chinesa à liderança tecnológica num dos setores identificados como possíveis no momento de formulação de MLB. Com um alto nível de investimento em Pesquisa e Desenvolvimento, o que tem gerado a propriedade sobre um grande número de novas patentes.

Um dos frutos do investimento da Huawei em novas tecnologias é a vanguarda da empresa chinesa quanto a tecnologia 5G - a nova geração de rede móvel, capaz de prover significativas melhorias na cobertura, disponibilidade e velocidade de conexão, permitindo também uma maior densidade de dispositivos conectados. A tecnologia 5G com sua capacidade de fluxos de dados praticamente instantâneos é peça chave para o surgimento e difusão de uma enorme gama de novos recursos tecnológicos. Tendo em vista a melhor compreensão da importância da tecnologia 5G, o próximo capítulo irá se debruçar sobre seus aspectos técnicos e como os mesmos abrem caminho para o desenvolvimento tecnológico.

2 – O 5G e um novo mundo

Carros e outros diversos veículos sem motorista se deslocam autonomamente por cidades inteligentes repletas de dispositivos altamente sofisticados que são capazes de monitorar e gerir o agir de milhões de pessoas. Médicos realizam cirurgias complexas a centenas de quilômetros de seus pacientes através de sofisticados aparatos tecnológicos. Robôs capazes de realizar diversas funções que até o presente momento são executadas por seres humanos dão vida a fábricas dotadas de linhas de montagem autonomamente ajustáveis a novas demandas ou imprevistos e são capazes de corrigir os possíveis problemas que venham a surgir.

Diversos equipamentos que outrora eram impensáveis de estarem conectados à Internet são abundantes em nossas casas. Geladeiras, fogões, condicionadores de ar, sistema de iluminação ofertam uma gama imensurável de dados às Inteligências Artificiais que se valem dessa hiperconectividade e digitalização de nossas vidas para influir no nosso dia a dia no "mundo real". Nossas vidas, mais do que somos capazes de perceber ou imaginar, são impactadas por algoritmos poderosos que direcionam nossas escolhas de forma imperceptível à nossa razão. Assim, o futuro previsto pelas mais consagradas obras de ficção científica será uma realidade concretizada. Realidade que passa pela tecnologia 5G, o que a confere grande importância.

Estima-se que a era da conexão 5G configurar-se-á por sua maior largura de banda de até 20 Gigabits por segundo (Gbps), baixa latência de 1 milissegundo (ms), alta densidade de dispositivos de um milhão de dispositivos por quilômetro quadrado e tecnologias de virtualização. Medições de desempenho feitas em uma rede 5G real mostrando um download máximo largura de banda de 458 Megabits por segundo (Mbps) e tempo mínimo de ida e volta (RTT – sigla em inglês) de 6 ms. Embora esses números ainda estejam longe das projeções para o pleno funcionamento da tecnologia 5G, eles representam um desempenho cinco vezes melhor que o desempenho, em termos de largura de banda e latência, das redes 4G.

A alta velocidade e estabilidade de conexão proporcionada pela tecnologia 5G se entrelaça com a constatação apresentada em Schwab (2016) quanto ao aproveitamento pelas inovações da Quarta Revolução Industrial da capacidade de disseminação da digitalização e da tecnologia da informação. De forma que o 5G será fundamental para o

pleno desenvolvimento dos três principais vetores tecnológicos que, segundo o autor, baseiam a Quarta Revolução Industrial – as tecnologias físicas, as tecnologias digitais e as biotecnologias.

As tecnologias físicas compreendem áreas como a robótica avançada, veículos autônomos, manufatura aditiva ou impressão em 3D e o desenvolvimento de novos materiais (SCHWAB, 2016; PIRES, 2018).

Embora a inserção de robôs em linhas produtivas seja algo consolidado e que já não gere nenhuma estranheza, o uso esperado na Indústria 4.0 vai muito além do que fora no passado. Se em seu uso inicial os robôs eram utilizados em espaços apartados do convívio com os trabalhadores, o que se espera para os próximos anos é que tarefas que exigem mobilidade e jogo de articulações – e que outrora requeriam trabalhadores para serem desempenhadas – sejam executadas por robôs. Passando assim, a ter-se linhas de montagem operadas com robôs que possuem leitura espacial por escaneamento e que podem ser programados sem auxílio de um especialista (PIRES, 2018, p.19). Outros aspectos da robótica avançada são a capacidade de controle de cada robô ou equipamento automatizado via Internet e a capacidade dessas máquinas interagirem entre si dentro de um plano estabelecido pelos engenheiros; existindo a capacidade que cada equipamento corrija suas atuações em caso de mudanças inesperadas no processo (SCHWAB, 2016; PIRES, 2018).

A Quarta Revolução Industrial também possibilitará o desenvolvimento e aprimoramento de veículos autônomos, indo além de "vants" (Veículos aéreos não-tripulados, conhecidos como *drones* em inglês), levando ao desenvolvimento de carros, ônibus e caminhões capazes de deslocarem-se de modo autônomo pelas ruas e rodovias, "graças a equipamentos e softwares de escaneamentos de ambiente, de posicionamento e de dirigibilidade capazes de 'aprender' com experiências que o veículo enfrenta no trânsito, armazenando eventuais erros e corrigindo em suas versões atualizadas" (PIRES, 2018, p. 20).

A manufatura aditiva (ou impressão 3D) consiste em "um processo de produção de objetos a partir da deposição de variados materiais em camadas, como plásticos, metais, cerâmicas e até mesmo argamassa para a construção de edificações" (PIRES, 2018, p. 21). Esta tecnologia é utilizada em setores como o automotivo e aeroespacial, odontológico, e na engenharia para construção de maquetes e protótipos.

Outra área pertencente à chamada 4ª Revolução Industrial é a de desenvolvimento de novos materiais. O intuito é o desenvolvimento de novos materiais mais eficientes que

os utilizados até o momento, reduzindo custos produtivos e possibilitando acréscimo de segurança. Sendo esse desenvolvimento o fruto de pesquisas de centros universitários, possibilitadas pelo barateamento dos custos de armazenamento de informação, pela capacidade de processamento de dados por sistemas de Inteligência Artificial (IA) e também pela existência de ambientes virtuais de simulação que derivam de fatores anteriores. O que nos leva ao vetor das tecnologias digitais.

As tecnologias digitais se referem à Inteligência Artificial, à Internet das Coisas, à análise de Big Data, às moedas virtuais e à economia sob demanda. A alta velocidade de conexão proporcionada pela Internet 5G possibilitará a integração de uma série de dispositivos como máquinas e equipamentos industriais, equipamentos urbanos (como os de iluminação pública e semáforos), computadores pessoais, telefones celulares, tablets, automóveis e uma variedade de eletrodomésticos que podem ser conectados em rede e controlados à distância por meio da Internet (SCHWAB, 2016; PIRES, 2018).

Estima-se, segundo pesquisa realizada pelo *World Economic Forum* (WEF, 2015), que em 2025 o mundo chegue próximo de 1 trilhão de dispositivos conectados à Internet; resultando, como detalha Pires (2018), em uma maior eficiência, aumento de produtividade, melhoria da qualidade de vida, controle dos impactos da atividades produtivas sobre o meio ambiente, menor custo de prestação de serviços, maior segurança frente a possibilidade de monitoramento virtual, maior eficiência logística dentro e fora das empresas, facilidade para a concepção de produtos ajustados às necessidades de cada cliente, etc.

A existência dessa grande conexão de dispositivos leva a um novo e mais alto patamar de dados circulantes na Internet, o que leva ao desafio de tornar todos esses dados circulantes em informações úteis. Para tal, a "análise de Big Data" configura-se como importante instrumento da Quarta Revolução Industrial. Como Pires (2018, p.22) bem explica:

> A análise de Big Data se vale da grande capacidade de processamento dos supercomputadores e ainda de sistemas de Inteligência Artificial para procurar padrões na massa de dados e construir informações significativas para diversos campos de atividade, como reconhecer padrões de consumo de indivíduos e grupos sociais, formação de perfis de pessoas supostamente implicadas em crimes ou militância política virtual, impacto de políticas públicas sobre a opinião pública, estratégias de marketing e de mobilização social por meio de redes sociais, etc. De acordo com o estudo do WEF (2015), se considera o fato de que em 2025 os Estados Nacionais deixarão de realizar censos decenais por conta das informações sociais e demográficas coletadas por sistemas de análise de Big Data.

Outra ferramenta são os sistemas de Inteligência Artificial (IA), capazes de armazenar e manipular dados, adquirir, representar e manipular conhecimentos (Pires 2018). Segundo Pires (2018), os sistemas de IA passam a ser cada vez mais capazes de deduzir e inferir novos padrões a partir do conhecimento preexistentes e utilizar métodos de representação e manipulação capazes de resolver problemas complexos de caráter qualitativo, ou seja, que não são passíveis de regras ou leis previamente ensinadas ao computador (PIRES, 2018, p.23). Como utilidade a esse processamento de dados em tamanha grandeza temos, por exemplo, a potencialização de pesquisas científicas, o aprimoramento de sistemas de gestão, a precificação de ativos (como ações e moedas), acréscimo de eficiência na gestão de tráfego e tráfico das cidades, a definição mais exata de padrões de consumo de grupos e indivíduos.

Outro aspecto importante das tecnologias digitais diz respeito à formação de uma *on demand-economy*, ou, uma economia sob demanda (ou sob medida). Cada vez mais, sítios eletrônicos e aplicativos de Internet tenderão a moldar novas formas de interação humana voltadas a troca de bens e serviços. Para os próximos anos, é esperado um aumento do chamado consumo colaborativo, onde determinados bens e ideias passam a ser compartilhados mediantes custos menores do que os correlatos no mercado (SCHWAB, 2016; PIRES, 2018). Tal formato é disponibilizado por plataformas como o Facebook, o WhatsApp, o Uber, a AirBnB, etc. Nos dias atuais, temos o Facebook como maior empresa de mídia – mesmo sem gerar conteúdo –, o Uber como a maior empresa de táxi – sem ter frota –, a AirBnB como a maior empresa de hotelaria – sem possuir uma rede hoteleira – e a Amazon como a maior empresa de vendas – sem possuir lojas físicas. O alto tráfego de dados, juntamente com a análise de Big Data e a Inteligência Artificial, aliados à capacidade da Indústria 4.0 de rápida adaptação nas linhas de produção a novas demandas, tende a levar a economia sob demanda a um novo patamar e de várias formas ainda não imaginadas.

As biotecnologias são o terceiro vetor da Quarta Revolução Industrial, que compreendem o uso de tecnologias de sequenciamento genético, da Biologia sintética por meio de manipulação do DNA, da combinação de edição de genes e impressoras 3D, das Ciências do Cérebro e do Biomimetismo no processo de desenvolvimentos de novos materiais. Tal realidade abre perspectivas inovadoras no cuidar da saúde, na produção de alimentos, na criação de próteses, na interação entre ondas cerebrais e objetos externos ao corpo humano e no desenvolvimento de materiais poupadores de energia ou de estruturas inspiradas nos seres vivos – o que tende a impulsionar novas formas de

produção, construção civil e de projetar. Sendo os avanços da informática de suma importância para os avanços dos experimentos em laboratórios, no desenvolvimento de instrumentos de medição cada vez mais sofisticados e no desenvolvimento de nanoestruturas (SCHWAB, 2016; PIRES, 2018).

Tais avanços são possíveis devido à capacidade de armazenamento e processamento de dados alcançados nas últimas décadas; sendo a tendência que tais dados aumentem com o ganho de velocidade de conexão ofertado pela tecnologia 5G, levando a um progressivo e exponencial avanço das biotecnologias.

A ampla possibilidade de desenvolvimento de novas tecnologias abre espaço para o surgimento de novas aplicabilidades e novos modelos de negócios, resultando em expressivo impacto na economia mundial. No primeiro momento, pelo qual passamos, os países direcionarão seus esforços de modo a implementar a infraestrutura 5G. Essas primeiras implantações atendem majoritariamente a aplicativos que se valerão de tecnologia eMBB (voltados ao uso de mídias de Realidade Aumentada, 4K, streaming de vídeo em 360 graus, etc), entretanto os passos seguintes conduzirão a implementação massiva dos aplicativos com tecnologia MIoT (Internet das Coisas Massiva), responsável pela disseminação de objetos pessoais e industriais conectados à Internet, e MCS (Serviços de Missão Crítica - que são redes à prova de falhas e oscilação) voltados ao setor industrial e também governamental, que ganharão força no médio a longo prazo, conforme o 5G passar a atender mais profundamente as aplicações esperadas para indústrias e cidades.

Embora devido às diferentes indústrias terem suas próprias estruturas econômicas e regulatórias, que acabam por afetar o processo e o momento de adoção dos novos modelos de negócios decorrente da tecnologia 5G, as implantações de 5G afetarão praticamente todos os setores industriais. De forma que o IHS Markit – empresa de análise de dados – estimou que “a potencial atividade de vendas globais em vários setores da indústria habilitados pelo 5G pode chegar a US$12,3 trilhões em 2035. Isso representa cerca de 4,6% de toda a produção real global em 2035” (CAMPBELL et al, 2017, p. 16, tradução nossa).

A implementação do 5G na economia global atingirá diversos setores econômicos. Estima-se que a manufatura terá a maior parcela da atividade econômica prevista para 5G em 2035 – quase US$3,4 trilhões ou 28% dos US$12,3 estimados (CAMPBELL et al, 2017, p. 16, tradução nossa). Cabendo ressaltar como o crescimento da importância da manufatura ligada ao 5G se relaciona com o transbordamento oriundo de outras

atividades. A implementação de qualquer um dos casos de uso do 5G estimulará a realização de gastos complementares com equipamentos a serem produzidos pelo setor manufatureiro.

Por exemplo, drones viabilizarão as vendas no setor de transportes. No entanto, isso exigirá que o setor de transporte adquira drones do setor manufatureiro. Casos de uso médico exigirão gastos complementares em equipamentos prontos para 5G do setor manufatureiro. A mesma linha de raciocínio se aplica ao setor de informação e comunicação, que verá a segunda maior parcela da atividade econômica habilitada para 5G, com mais de US$1,4 trilhão (CAMPBELL et al, 2017). Implementando qualquer um dos casos de uso do 5G, exigir-se-á gastos com serviços de comunicação.

Embora o 5G possa permitir cerca de 4,6% da produção real global em 2035, a porcentagem de ativação por setor varia de uma alta de 11,5% no setor de informação e comunicação para uma baixa de 2,3% no setor de hospitalidade. O tamanho do setor manufatureiro, que será responsável por quase 30% da produção real global em 2035, juntamente com o fato de que grande parte das vendas de fabricação habilitadas para 5G serão secundárias (ou seja, vendas de equipamentos em suporte ao caso de uso) levarão para um percentual (4,2%) ligeiramente abaixo da média geral. Mais notável é o fato de que o 5G pode permitir 6,5% dos serviços públicos (governo) e 6,4% da produção agrícola em 2035, apoiado por implantações de cidade inteligente e agricultura inteligente, respectivamente (CAMPBELL et al, 2017)

Para colocar essas descobertas em um contexto mais amplo, é preciso também considerar quantas indústrias serão realmente afetadas por cada caso. Por exemplo, a disponibilidade de veículos autônomos e drones fará mais do que estimular as vendas de carros sem motorista e veículos aéreos não tripulados (Vant’s) para os consumidores. Eles também serão implantados em aplicações agrícolas e de mineração variando da vigilância de recursos naturais remotos ao transporte autônomo de minérios a tratores autônomos. Eles serão amplamente utilizados no setor de transporte para transporte sem motorista e entrega de produtos comerciais e de consumo bens. Os municípios integrarão veículos autônomos em seus sistemas de trânsito enquanto usam drones para funções de monitoramento. Na fabricação, os veículos autônomos também serão usados em sistemas de estocagem e recuperação dentro da fábrica. Finalmente, os veículos autônomos também afetarão o setor de seguros à medida que as taxas de acidentes com veículos diminuírem (CAMPBELL et al, 2017).

Atingir o potencial de habilitação de produção do 5G exigirá investimentos contínuos das empresas na cadeia de valor 5G para melhorar e fortalecer continuamente a base tecnológica fundamental. A cadeia de valor 5G abrangerá um amplo espectro de empresas de tecnologia, incluindo, entre outros: operadoras de rede, provedoras de tecnologias e componentes essenciais, fabricantes de dispositivos, fabricantes de equipamentos de infraestrutura, e desenvolvedores de conteúdo e aplicativos.

A IHS Markit (2017) modelou a atividade econômica da cadeia de valor 5G para sete países que devem estar na vanguarda do desenvolvimento 5G: Estados Unidos, China, Japão, Alemanha, Coreia do Sul, Reino Unido e França.

De 2020 a 2035, a IHS Markit estimou o investimento médio anual coletivo em Pesquisa e Desenvolvimento (P&D) e Investimento em Bens de Capital das empresas que fazem parte da cadeia de valor 5G nesses países em mais de US$200 bilhões. No primeiro momento, a P&D e implantações de infraestrutura de rede dominarão as atividades de investimento em 5G. Posteriormente, o foco dos investimentos mudará para o desenvolvimento de aplicativos e serviços que exploram os recursos exclusivos de 5G.

> O ciclo de investimento sustentado é outro indicador de que o 5G é um ‘jogo longo’ que verá as prioridades de investimento mudarem à medida que a infraestrutura é implantada, novos modelos de negócios ficam online, a base de tecnologia subjacente é continuamente fortalecida e os ciclos de substituição para muitos dos casos de uso são prolongados.

Espera-se que os Estados Unidos e a China dominem os investimentos tanto em P&D (US$1,2 trilhão) quanto em Bens de Capital (US$1,1 trilhão) ligados ao 5G, ao longo do horizonte temporal de 16 anos do estudo. A estimativa é que os Estados Unidos responderão por cerca de 28% do investimento global em 5G, seguido pela China com 24%. Gastos além dos sete países citados devem representar cerca de 23% dos investimentos globais em 5G.

O estudo feito pela IHS Markit estima que, até 2035, apenas a cadeia de valor do 5G gerará US$3,5 trilhões em produção econômica e apoiará 22 milhões de empregos. Ocorrendo na China a maior parte desses novos empregos ligados ao 5G. Além disso, estimou-se que de 2020 a 2035, as contribuições anuais do 5G para o Produto Interno Bruto (PIB) Global totalize US$3,0 trilhões.

O Estado que irrompe a nova era tecnológica na qualidade de pioneiro passa a ter vantagem produtiva e maior capacidade de internalizar capitais, dado a alta rentabilidade que oferece; o que se reflete num acréscimo de capacidade de acúmulo de poder. De forma que se pode entender que o pioneirismo das novas tecnologias se associa com o

capital político e ganhos de capacidade de incremento de poder militar, abrindo a possibilidade de paulatinamente se estabelecer em uma posição de liderança global – tal qual ocorreu com a Inglaterra no século XIX e os EUA no século XX. Sendo assim, estabelecendo-se a versão chinesa do 5G como base da Indústria 4.0, a China tenderia a ter ganhos crescentes de poder no sistema internacional – o que é abissalmente ofensivo a perspectiva de jogo de soma zero – onde os ganhos de um representam as perdas de outro – do realismo adotado na política externa dos EUA desde o governo Trump quanto a China.

Embora os ganhos econômicos relacionados à tecnologia 5G se mostrem suficientes para uma intervenção norte-americana por meio de sanções, a perspectiva militar direta existente por trás da tecnologia 5G não pode ser ignorada. Num mundo onde o confronto direto entre duas potências nucleares poderia trazer um nível de destruição incalculável, um novo modelo de guerra que conjugue tecnologias disruptivas e outros meios são uma realidade.

Majerowicz (2020) salienta que as Tecnologias da Informação e Computação (TICs) são um elemento central para o poder estrutural contemporâneo, pois elas sustentam a Revolução dos Assuntos Militares, a Indústria 4.0 e o aprimoramento tecnológico dos aparatos repressivos domésticos do estado. A autora salienta seu caráter fundamental tanto nas armas de precisão, como para a transformação de táticas e de estratégias militares em novas formas de guerra – tais como a guerra eletrônica e a *cyberguerra*. Ademais, por meio das TICs, existiria a possibilidade de se afetar a opinião pública – tal qual visto nos últimos anos ao redor do mundo, como por exemplo defendem os teóricos adeptos do conceito de Guerra Híbrida.

Embora sejam anteriores, o uso de *Vants*, principalmente pelos EUA, tem se acentuado rapidamente desde o atentado de 11 de setembro de 2001; o que se deve ao amplo desenvolvimento das TICs. Entre os anos de 2004 e 2014, mais de 370 ataques foram realizados com o uso de *Vants*, provocando mais de 3000 vítimas. Esses ataques atingiram o seu ápice durante a administração Obama, em 2009. Nesse período, mais de 330 ataques foram realizados, alcançando o pico de 122 no ano de 2010 (NEW AMERICA FOUNDATION, 2014).

Ao olhar para o futuro que surge no horizonte próximo, Barreiros (2019) detalha que, devido ao incremento tecnológico, o conceito de drones deve ir além dos *Vants*, abarcando todo tipo de plataforma terrestre, aérea ou naval operada à distância, com graus variados de autopilotagem e capacidade decisória tática. Incremento esse que tende a

levar a que se trate as munições guiadas e/ou inteligentes (G-RAMMs, *guided rockets, artillery, mortars and missiles*) a partir de um ponto de vista comum. Barreiros (2019, p16) relata que:

> A proliferação da produção e do uso de munições inteligentes (bem como os VANTs) já representa um sério desafio ao equilíbrio estratégico convencional e, a tirar pelas forças armadas chinesas, poderão constituir nessa primeira metade do século XXI uma "quarta força" em adição às já tradicionais: aviação, marinha e exército.

Durante a década de 2020, regiões como o Pacífico ocidental e o Golfo Pérsico (em função dos avanços chineses e iranianos nesse campo, respectivamente) poderão se configurar como "áreas de não acesso", devido aos elevados riscos operacionais, o que não deve se limitar a tal região, mas ocorrendo também em outros cenários geopolíticos até 2050 (BARREIROS, 2019).

Embora os EUA ocupem a fronteira da tecnologia dos *Vants* com os *stealth drones* (Lockheed Martin RQ-170 *Sentinel, Northrop Grumman* RQ-180), são seguidos por programas de desenvolvimento em países como Rússia (*Mikoyan Skat* e *Sukhoi* S-70 *Okhotnik*), Israel, China (CH-7), Índia (DRDO Aura), Inglaterra (BAE *Taranis*), e pelo consórcio liderado pela Dassault francesa, reunindo Itália, Suécia, Espanha, Grécia e Suíça (*Dassault nEUROn*) (BARREIROS, 2019).

A massificação do uso de *Vants* tende a resultar no enxameamento (*swarming*), onde se terá uma atuação conjunta de um alto números de unidades autônomas – fruto do incremento de novas capacidades e da diminuição de custos para a produção de tais equipamentos.

Barreiros (2019) descreve que:

> Em aspecto doutrinário, o swarming na guerra futura consistirá em mais um desdobramento da corrente noção de "guerra centrada em redes" (GCR ou NCW): neste cenário, um volume restrito de plataformas multipropósito tripuladas e centenas (ou mesmo milhares) de plataformas não tripuladas propósito-específicas de baixo custo trocam informações em tempo real, identificando e designando alvos a serem destruídos com munições inteligentes, alertando para ameaças e condições situacionais, e traçando estratégias de ataque e defesa coletivas de acordo com as circunstâncias.

Os enxames permitirão uma ação cooperativa entre um grande número de equipamentos militares autônomos, semiautônomos e automáticos, atuando de forma inteligente demonstrando uma "inteligência emergente" derivada de dispositivos sensoriais e decisórios integrados no que pode ser compreendido como "internet das coisas militares" (BARREIROS, 2019). De forma que os componentes de um enxame

estarão conectados entre si, a outros enxames, bem como veículos, sensores, robôs e dispositivos pessoais empregados por soldados humanos, e também conectados com redes de logística (munições, provisões, medicamentos, etc.) constituindo uma evolutiva consciência interoceptiva num organismo que une componentes biológicos e eletrônicos (BARREIROS, 2019).

Uma estratégia baseada no "enxameamento" irá requerer um amplo desenvolvimento no campo da inteligência artificial, uma vez que a demanda para o ideal funcionamento ultrapassa as capacidades cognitivas humanas. Sendo assim, "prioritário que as plataformas militares reunidas em um enxame venham a contar com um grau suficiente de autonomia a ponto de realizarem tarefas básicas e de decidirem acerca de cursos de ação orientados por protocolos táticos gerais" (BARREIROS, 2019, p.26), restando ao controlador humano a função de comando na retaguarda.

Outro ponto de extrema importância – principalmente devido às acusações que basearam as sanções – é no tocante à proteção das redes de computação e informação de espionagem e roubos (conhecida como "cyber segurança"). Após os ataques terroristas do 11 de setembro em Nova York, diante do contexto da Guerra ao Terror do governo Bush, o desenvolvimento de tecnologias biométricas, de comunicação e de monitoramento se deu de maneira muito rápida, movidas por um senso de perigo iminente e de emergência. O emprego de tais tecnologias buscava levar a cabo a filtragem daqueles percebidos como perigosos, embora havendo reconhecida imprecisão na definição do conceito de inimigos, podendo abarcar a qualquer um cujo a subjetividade dos parâmetros dos agentes responsáveis pelo monitoramento assim nominasse.

A fim de monitorar esses perigos invisíveis e iminentes, agências de segurança dos Estados passaram a apoiar medidas provisórias e decretos executivos por parte de governos que flexibilizavam leis e direitos, tornando possível ações preventivas, antes que novos ataques ocorressem, configurando aquilo que Agamben (2003) considera como sendo práticas de exceção. O que possibilitou que as agências de inteligência norte-americanas tivessem acesso a um número praticamente ilimitado de dados que circulavam pela infraestrutura de Internet estadunidense.

2.1 A tecnologia 5G

O 5G é a quinta geração de tecnologias de rede celular especificadas pelo Projeto de Parceria de 3ª Geração (*3rd Generation Partnership Project* - 3GPP). A tecnologia da nova conexão prossegue com 2G, 3G e 4G e suas tecnologias associadas, ao mesmo tempo em que apresenta melhorias significativas de desempenho (LOGHIN *et al*., 2020).

A primeira diferença a ser citada é quanto ao Espectro de Onda Milimétrica (*Millimeter Wave Spectrum* – em inglês). A maioria das redes sem fio de tecnologias de comunicação das conexões anteriores funcionam em espectros abaixo de 6 GHz, além de utilizar essa frequência, o 5G operará em um espectro de alta frequência – de 28 GHz até 95 GHz, faixa que caracteriza o Espectro de Onda Milimétrica (mmWave – sigla em inglês). O que evita a ocorrência de congestionamentos de dados (LOGHIN *et al*., 2020).

A segunda diferença é referente ao uso massivo de tecnologia de múltiplas entradas e múltiplas saídas (multiple-input and multiple-output – MIMO, em inglês). Essa tecnologia compreende grandes formações de antenas tanto na estação base quanto na ponta onde estão os dispositivos para criar vários caminhos para transmissão de dados. O que permite a conexão 5G alcançar alta eficiência espectral e melhor eficiência energética. A isso se soma o Beamforming, um subconjunto do MIMO massivo que diz respeito à formação de feixe de onda, controlando sua direção e resultando na identificação o caminho mais eficiente para entregar os dados a um receptor e reduzindo a interferência dos terminais próximos. Além disso, a tecnologia Full-duplex utilizada na conexão 5G dobra a capacidade dos enlaces sem fio na camada física, o que permite que um dispositivo seja capaz de transmitir e receber dados ao mesmo tempo, usando uma mesma frequência. Essas conjunto de novas tecnologias, permite que se entenda o 5G como detentor de potencial de melhorar os serviços na ponta de uso, suportando um grande número de aplicabilidades – que se reflete na aceleração do desenvolvimento de Cidades Inteligentes e também que se aprimore a experiência do usuário (LOGHIN *et al*., 2020).

O terceiro aspecto inovador é referente a redes densamente distribuídas por estações bases que utilizam infraestrutura de células pequenas (*Small Cells*), o que permite uma banda larga aprimorada (eMBB – sigla em inglês) e baixa latência. As Small Cells são fundamentais para compensar o fato que as ondas de alta frequência (acima de 25GHz), com as quais o 5G trabalha, viajam distâncias menores que as ondas características até a conexão 4G (LOGHIN *et al*., 2020).

O quarto ponto que se difere é referente a comunicação de dispositivo para dispositivo. O 5G permite uma comunicação direta entre os dispositivos, demandando o mínimo de ajuda da infraestrutura nesse processo. Essa comunicação dispositivo a dispositivo (D2D) tende a potencializar a aceleração do desenvolvimento de aplicativos centrados na borda. O que permitirá que veículos autônomos possam se comunicar diretamente entre si, reduzindo assim a latência e evitando a falha na conexão com a estação base. Similarmente, dispositivos de borda podem compartilhar dados entre si através do uso da comunicação D2D 5G.

Na virtualização, quinto aspecto a ser abordado quanto às diferenças, as tecnologias de redes definidas por *software (software-defined networking* - SDN), de virtualização de funções de rede (*network function virtualization* - NFV) e de fatiamento de rede se destacam. SDN é uma abordagem que separa o plano de dados de rede (ou seja, processo de encaminhamento de dados) do plano de controle (ou seja, o processo de roteamento). Essa separação leva a uma configuração e gerenciamento mais fáceis e como maior flexibilidade e elasticidade (KREUTZ *et al*., 2015; LOGHIN *et al*., 2020). Complementar ao SDN, o NFV usa sistemas de Commodity Hardware para executar serviços de rede que são tradicionalmente implementados em hardwares como roteadores e firewalls, o que resulta em uma diminuição de custos. Com NFV, a flexibilidade da rede é melhorada e o tempo de colocação no mercado é reduzido (HAN *et al*., 2015; LOGHIN *et al*., 2020).

O desmembramento e a virtualização das funções de rede utilizam tecnologias digitais, em especial a computação em nuvem e a Inteligência Artificial, para processar o grande volume de dados que são transmitidos em grande velocidade de transmissão, necessários para garantir a customização da rede (LOGOTA et al., 2015, p. 30; MAJEROWICZ, 2021, p. 11). Como explica Triolo, Allison e Brown (2018, p. 7, tradução nossa), “uma consequência prática disso é que os fabricantes de equipamentos de infraestrutura projetarão e implantarão sistemas operacionais e de gerenciamento que usam Inteligência Artificial, tanto separadamente quanto em colaboração com as operadoras”.

Como sexta característica inovadora, citamos o fato que as redes 5G se valerão do SDN e NFV de modo a usar o fatiamento de rede (*network slicing*) para a transmitir simultaneamente de ponta a ponta redes virtualizadas sobre uma única infraestrutura física. A separação proporcionada pelo 5G entre operadoras de infraestrutura e provedores de serviços maximizará os recursos de hardware, o que fornece uma gama

diversificada de serviços para empresas e usuários finais (FOUKAS *et al*., 2017; LOGHIN *et al*., 2020)

Por último, cita-se a característica de melhoria de desempenho. O 5G tem uma latência baixa, aproximadamente 1ms, maior eficiência energética e uma taxa de transferência máxima de 10-20 Gbps (AL-FALAHY; ALANI, 2017; LOGHIN *et al*., 2020). A largura de banda que a conexão 5G trabalhará além de oferecer suporte a melhores experiências de uso também permitirá que mais dispositivos se mantenham conectados. A título de comparação, enquanto uma estação base 4G suporta cerca de cem mil dispositivos, ao se passar para a tecnologia 5G, uma base poderá suportar até um milhão de dispositivos por quilômetro quadrado (MOHYELDIN, 2016). Como Loghin et al. (2017, p.1186, tradução nossa) sintetiza, "o projeto de uma rede 5G visa a sua flexibilidade e adequação para implantação de borda, o que melhora a latência de ponta a ponta, bem como a experiência geral dos usuários."

2.2 Segurança nas redes 5G

As inovações citadas anteriormente não só ofertam grandes ganhos de velocidade e de baixa latência, mas também mudam a dinâmica e se constituem como grande desafio no tocante à segurança e privacidade. Como Borelli (2022, p.144-145) explica,

> a infraestrutura de rede 5G tende a nublar a separação entre o centro e a periferia da rede – o que também tende a tornar a arquitetura bastante sensível, uma vez que, por ser pautada por software, isso tende a facilitar e ampliar atividades maliciosas, assim como a dificuldade de detectá-las devido ao grande volume de dados sendo transferido.

Triolo, Allison e Brown (2018) aborda os riscos estruturais da nova infraestrutura de rede. A tendência de transferência integral de dados e atividades para o meio digital (seja por indivíduos, corporações, cidades ou governos) se concretizando, as novas infraestruturas podem se tornar vulneráveis e suscetíveis a ataques cibernéticos.

Como citado, o 5G funciona com a virtualização e o fatiamento da rede, o que permite que aplicativos com requisitos distintos compartilhem a mesma rede. Entretanto, uma fatia de rede 5G compreende vários recursos virtualizados que são gerenciados por vários provedores, o que dificulta a garantia do isolamento dos dados circulantes. Para se alcançar um modelo de virtualização e fatiamento estritamente seguro seria necessário

que as camadas nas quais os espectros de rádio se dividem se coordenassem e concordassem entre si através de um protocolo que as cruzasse.

Outro ponto desafiador é que o 5G é um facilitador essencial para a comunicação máquina a máquina. Aplicativos baseados na localização do dispositivo, por exemplo, podem ver novos dispositivos entrando e saindo do alcance em alta velocidade. Este tipo de comunicação, destinada a essa finalidade, onde existe uma alta taxa de rotatividade representa um novo desafio para a autenticação de dispositivos. Os dispositivos deveriam se identificar entre si antes de ocorrer a comunicação, mas dado o grande número de dispositivos e também as suas aplicações, seria necessária a capacidade de suportar um grande número de usuários e evitar que se concentrem em um único ponto de confiabilidade. De modo que as práticas atuais de segurança não comportam as necessidades requeridas para suprir essa demanda de segurança.

As redes anteriores concentravam os dados em menos pontos finais de comunicação (endpoints), o que levou a práticas de segurança que conseguiam coletar dados nos terminais e dentro das redes para posteriormente analisar. A tecnologia 5G funciona com mais endpoints e com redes que são muito mais rápidas, o que resulta em maior "superfície de ataque" e aumenta a probabilidade da rede ser atacada. Dado o impacta da nova velocidade das redes, o protocolo atual de armazenamento e posterior analise não mais atende como prática de segurança. Sendo assim, o 5G exige uma nova plataforma de análise de segurança.

Como definem Loghin *et al.* (2017, p. 1190, tradução nossa),

> o 5G também apresenta novos desafios e oportunidades em termos de privacidade, pois a largura de banda aprimorada e a latência reduzida do 5G abrem a possibilidade de transformar dispositivos móveis em bancos de dados privados que podem ser consultados em tempo real.

Dada as especificações da tecnologia 5G, é possível que os dados do usuário sejam armazenados no seu próprio dispositivo ao invés de serem guardados no provedor de serviço (*service provider*). De modo que o provedor de serviço só teria acesso aos dados do usuário em momentos específicos. Entretanto, essa possibilidade abre espaço a uma série de questões ainda sem respostas claras, conforme Loghin et al. (2017, p. 1190, tradução nossa):

> como gerenciar os dados privados de cada usuário em seu dispositivo local, para que diferentes provedores de serviços possam acessar os dados por meio de uma interface unificada e eficiente? Como permitir que os usuários tomassem decisões informadas sobre qual provedor de serviços deve ter permissão para acessar qual item de dados? Além disso, dado que cada usuário pode ter uma quantidade considerável de dados privados heterogêneos armazenados em seu dispositivo local, como poderíamos aliviar a sobrecarga

> dos usuários na configuração de controles de acesso para um número considerável de provedores de serviços? Quando um provedor de serviços e um usuário calculam conjuntamente o resultado de uma determinada tarefa, o provedor de serviços pode inferir informações confidenciais do resultado do cálculo, mesmo que não tenha acesso direto aos dados privados de um usuário. Por exemplo, com base no resultado da recomendação calculado a partir do histórico de compras de um usuário, o provedor de serviços pode inferir informações parciais sobre os itens que o usuário comprou no passado. Como devemos prevenir tais ataques de inferência sem degradar a precisão de o resultado calculado em conjunto pelo usuário e pelo prestador de serviço?

As mudanças impostas à cibersegurança pelas características existentes na tecnologia 5G constituem-se como importante e desafiante questionamento em um cenário onde a sua iminente implementação impacta positivamente as economias dos países. Por outro lado, a excessiva demora em construir uma infraestrutura nacional 5G tende a gerar enormes desvantagens em caso de adesão global em massa. De forma que os Estados se veem obrigados a ponderar entre os prós e contras da adesão imediata da tecnologia.

Em um cenário onde os Estados de fato se considerem seguros com a utilização de uma infraestrutura de Internet anterior ao 5G, o peso da insegurança gerado pela adesão à nova tecnologia tenderia a levar a mais profundas ponderações. Entretanto, a corrida envolvendo os mais distintos Estados para se construir redes 5G nacionais possibilitam o seguinte questionamento: o quão segura e neutra é a infraestrutura da Internet hoje? Ante uma possível conclusão de suscetibilidade compartilhada entre os Estados, a decisão quanto à origem dos equipamentos que integrarão a infraestrutura do 5G se dá não sobre ***se*** alguém terá acesso, mas sim sobre ***a quem*** conceder-se-á acesso ao exercício de poder sobre as suas infraestruturas da Internet.

3 – Ciberpoder

3.1 Ciberterritório

Segundo Kellner (2001), o termo ciberespaço foi utilizado pela primeira vez no conto “Burning Chrome”, escrito pelo norte-americano Willian Gibson em 1982. Entretanto, a primeira aparição do termo frequentemente é atribuída a outra obra de Gibson, Neuromancer, publicada no ano de 1984. No prefácio da edição brasileira dessa obra publicada em 2003, Alex Antunes, o tradutor, expressa que “o conceito criado por Gibson neste livro, o ciberespaço, é uma representação física e multidimensional do universo abstrato da 'informação'. Um lugar para onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica para trás” (Gibson, 2003, p. 5-6).

A definição dada por Gibson (2003) entende o ciberespaço como

> uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações [...] Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade. (2003, p. 67).

Gibson (2003, p. 14) descreve que Case, o protagonista da obra, “operava com uma taxa de adrenalina quase sempre alta, uma mistura de juventude e competência, com sua consciência fora do corpo projetada na alucinação consensual da matrix por meio de um deck ciberespacial customizado". Kellner (2001) ao refletir sobre essa descrição dada por Gibson, entende que eles guardam grande semelhanças para com os fenômenos atuais e reais. Essa percepção se choca com os aspectos alucinatórios e subjetivos desenvolvidos por Gibson ao falar da conexão entre o humano e o ciberespaço.

A reflexão desenvolvida por Kellner foi publicada pela primeira vez em 1995, embora o autor estivesse inserido em uma realidade muito diversa da existente agora – na terceira década do século XXI, Kellner, naquele momento, vivenciava impactos já muito mais evidentes da globalização dos recursos cibernéticos que resultaram na difusão do termo ciberespaço da literatura para a ciência e demais campos. O que permitia uma

leitura muito mais precisa da, ainda inicial, fusão entre os mundos da materialidade do "real" e da imaterialidade do "virtual".

Transcorridos cerca de 40 anos desde que Gibson cunhou o termo ciberespaço, inúmeros escritos depois – da fantasia a estudos científicos e filosóficos – a compreensão quanto a o que é o ciberespaço e sua ligação com o mundo tangível ainda é um grande desafio. Desafio que só se assevera com o aprimoramento tecnológico e o surgimento de inúmeras formas de interação humana com e no ciberespaço, bem como os desdobramentos do cibernético no mundo material.

O presente trabalho não intenta alcançar uma proposição que ponha fim ao debate conceitual quanto ao ciberespaço, entretanto entendemos que a compreensão de algumas das suas leituras são fundamentais para que se alcance os objetivos dessa pesquisa.

Koepsell (2004, p. 125) afirma o ciberespaço como sendo físico, tal qual o são os seus componentes. Para ele, o ciberespaço é

> um meio composto de chips de silício, fios de cobre, fitas e discos magnéticos, cabos de fibra ótica e de todos os outros componentes de computadores, meios de armazenamento e redes que armazenam, transmitem e manipulam bits. [...]. O software existe no ciberespaço como o texto existe no papel ou como uma estátua existe em pedra.

Na definição de Rabaça e Barbosa (2001) o ciberespaço é um espaço cibernético, um universo virtual que existe graças às informações circulantes e/ou armazenadas nos computadores ligados a Internet; constitui-se como uma dimensão virtual da dita realidade, um algo não palpável, imaterializado, sendo um lugar longe da nossa realidade. Mesmo as relações sociais, culturais e econômicas se estabelecem no imaginário (MONTEIRO, 2007).

Para Silva e Silva (2004), o ciberespaço configura-se não só como uma região invisível e abstrata por onde as informações circulam, mas também como um espaço social de trocas simbólicas entre pessoas situadas em diferentes lugares do mundo material.

Lévy (2000, p.92), define o ciberespaço como sendo um "[…] espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores." Para o autor, o termo abarca a infraestrutura material das tecnologias da informação e comunicação e também toda a gama de informações por ela armazenada, além disso, os próprios seres humanos que navegam e provêm esse fluxo informacional constituem o ciberespaço. Em sua definição de ciberespaço, o autor:

> inclui o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de rede hertzianas e telefônicas clássicas), na medida em que

> transmitem informações provenientes de fontes digitais ou destinadas à digitalização. Insisto na codificação digital, pois ela condiciona o caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo e, resumindo, virtual da informação que é, parece-me, a marca distintiva do ciberespaço. Esse novo meio tem a vocação de colocar em sinergia e interfacear todos os dispositivos de criação de informação, de gravação, de comunicação e de simulação. A perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e suporte de memória da humanidade a partir do próximo século. (Lévy, 2000, p. 92-93).

Monteiro (2007) para além do entendimento do ciberespaço "como um universo virtual proporcionado pelas redes de telecomunicações", concebe o ciberespaço "como um novo mundo, um novo espaço de significações, um novo meio de interação, comunicação e de vida em sociedade". Esse universo não é irreal ou imaginário, existe de fato, e o faz em um plano essencialmente diferente dos espaços conhecidos."

De forma que é possível separar as visões entre as que consideram o ciberespaço como um espaço de fato, as que o desconsideram como tal e ainda as que veem o ciberespaço como parte do mundo não virtual. Havendo ainda subdivisões entre os referidos grupos de interpretação.

Quanto ao primeiro tipo de interpretação do ciberespaço, é possível dividi-la entre excepcionalistas e não excepcionalistas. Para as teorias excepcionalistas, o ciberespaço se configura como um espaço separado do mundo real e "a suposição de separação permite e ratifica concepções altamente ritualizadas e simplificadas de ordenamento social, que ganham força em parte porque são concebidas como uma etapa distante do 'espaço real'" (COHEN, 2007, p. 212, tradução nossa).

O segundo grupo existente em tal vertente é o dos não excepcionalistas. Para eles também o ciberespaço se constitui enquanto um espaço de fato e separado, a diferença reside no entendimento que a suposição de separação com o mundo real permite e ratifica a negação da diferença entre os espaços; para que o ciberespaço seja exatamente igual ao espaço real é necessário ignorar que o ciberespaço é "povoado" por usuários reais que vivenciam o ciberespaço e o espaço real como diferentes, mas conectados, com atos praticados em um tendo consequências no outro (COHEN, 2007).

Cohen (2007, p. 212, tradução nossa) afirma que "o debate interno entre os teóricos do ciberespaço como espaço de fato – o debate quanto ao tipo de espaço o ciberespaço "é" – tem sido insuficientemente sensível às maneiras pelas quais as próprias teorias funcionam como atos de construção social." Segundo o autor, ambos os casos

ignoram tanto a experiência incorporada e situada dos usuários do ciberespaço quanto a complexa interação entre as geografias real e digital.

O segundo grupo de interpretações diz respeito ao debate sobre se o "ciberespaço" é "um espaço". Segundo Cohen (2007), a visão desse grupo, sob influência dos estudos culturais pós-modernistas, corretamente enfatiza a importância do espaço e das metáforas espaciais como veículos cultural e ideologicamente carregados para a extensão do poder. De forma que

> dizer que os humanos raciocinam espacialmente não é dizer que estamos presos a um lugar ou a uma propriedade, mas simplesmente dizer que somos seres corporificados e situados, que compreendem até mesmo as comunicações desencarnadas através do filtro da experiência corporificada e situada.

A terceira visão quanto ao entendimento da espacialidade do ciberespaço e seus desafios arquitetônicos e regulatórios não diz respeito quanta a questão de que tipo de espaço o ciberespaço é, "mas que tipo de espaço um mundo que inclui o ciberespaço é e será" (COHEN, 2007, p.213, tradução nossa). Para Cohen (2007), o ciberespaço faz parte do espaço vivido (espaço real), suas conexões com o espaço vivido ofertam o meio de compreensão do ciberespaço e também das eventuais necessidades regulatórias. Assim, uma teoria do ciberespaço e do espaço deve considerar a ascensão das espaço em que ocorrem as interações virtuais, a relação emergente e contestada entre o ciberespaço e o espaço corporificado, bem como as maneiras pelas quais o ciberespaço altera, instancia e interrompe geografias de poder.

A existência de distintas interpretações quanto ao tema do que é o ciberespaço e do alto nível de abstração necessário à sua compreensão, existente em todas as conceitualizações, favoreceu a construção da ideia do ciberespaço como um "lugar" (ou não lugar) onde diversos mundos podem coexistir apartados de um território, de leis e soberania. Esse processo de desterritorialização está intrinsecamente correlacionado com o rompimento de conceitos da modernidade que influenciaram a construção da ideia de territórios como é assumida hoje. Como Monteiro (2007) afirma, "com a emergência das novas tecnologias de informação e comunicação, o tempo da História já não é o mesmo. Na era *"virtual"* as definições de tempo e espaço se fundem (ou confundem)."

Walker (1993), em sua análise historiográfica sobre conceitos caros às teorias de Relações Internacionais, explana como a busca pela delimitação precisa territorial é um fenômeno da modernidade, atrelado justamente a uma visão cartesiana, geométrica e linear tanto do tempo como do espaço – frutos da revolução newtoniana.

A literatura recente sobre ciberespaço é cada vez mais mobilizada por estudos que consideram o ciberespaço como inseparável do mundo "real" e apontam a tendência de uma fragmentação da Internet e do ciberespaço. Como Lambach (2020, p.2, tradução nossa) sintetiza, "há um indiscutível senso de *fin de siecle* sobre a Internet, como se ela estivesse prestes a se desintegrar em sub-redes frouxamente acopladas, acabando com a era da "*web* aberta'".

O que se tem visto de uma forma mais clara é um processo no qual Estados tentam afirmar sua autoridade soberana sobre o ciberespaço baseando-se em lógicas territoriais conhecidas para estender sua governabilidade sobre o ciber. Estudiosos do tema têm entendido esse processo de fragmentação como uma tentativa de territorialização mais clara, tanto no tocante à Estado quanto a múltiplos territórios que advém das práticas privadas.

Lambach (2020, p.3, tradução nossa) se baseia na geografia crítica para analisar esse processo de territorialização. Para ele, "o território e as fronteiras devem ser vistos como práticas fluidas e adaptáveis, e não como estruturas estáticas e imutáveis delimitando e inscrevendo o espaço." De modo que "o ciberespaço é um excelente exemplo de novas territorialidades surgindo, mudando e sendo contestadas" justamente pela existência de distintas fronteiras internas no ciberespaço (de ordem privada, corporativa e estatal), mas também pelas fronteiras porosas para com o mundo "real" e que se estendem no mundo "real" (COHEN, 2007; OLSON, 2005; NISSENBAUM, 2004).

Para além e anteriormente à existência do ciberespaço, o conceito de território já era algo difícil de ser trabalhado. Gottmann (1975, p. 524) traz que o território é algo entendido como um "atributo por si só evidente das instituições governamentais estabelecidas" (GOTTMANN, 1975, p. 524), o que, para o autor, explica a dificuldade em se trabalhar com o conceito. A isso se soma o fato que embora desde seu primórdio a humanidade realize suas interações sobre o espaço terrestre, a busca pela delimitação territorial precisa é um fenômeno da modernidade (WALKER, 1993).

Teóricos de gerações anteriores à Internet já rejeitavam a ideia de território como um espaço físico delimitado e imutável, compreendendo-o como um lugar de interações humanas e dotado de dinâmicas de manifestações de poder. De modo que é possível elencar-se novos espaços além do terrestre, marítimo, aéreo e espacial como integrantes de um território, entretanto fazê-lo com o cibernético ainda é problemático não só devido a uma dificuldade de percepção e interpretação das dinâmicas de interações, mas também,

e principalmente, devido a incapacidade de nos atentarmos a existência de uma dinâmica de poder que se invisibiliza à sombra da ideia da neutralidade tecnológica e do ciberespaço como um não lugar ou lugar apartado da realidade.

Conforme a técnica avança e permite a geração de novas capacidades, novas formas de interações são criadas e ocorrem em espaços outrora impensáveis. Conforme Metri (2018), p. 514),

> não fazia sentido falar, por exemplo, de espaço aéreo nacional antes da Primeira Guerra Mundial. Porém, com o advento dos aviões e seu desenvolvimento para uso militar, este espaço se incorporou ao conceito de território dos estados nacionais característicos do século XX.

O que ocorreu com rios e mares, céu e espaço, hoje alcança a esfera do cibernético.

A incapacidade de interação e necessidade de superação se relaciona com o termo *coerção geográfica*, cunhado pelo historiador Fernand Braudel em seu artigo "História e Ciências Sociais: a Longa Duração" publicado na *Revista dos Annales* em 1958.

> Certas estruturas, por viverem muito tempo, tornam-se elementos estáveis de uma infinidade de gerações: atravancam a história, incomodam-na, portanto, comandam-lhe o escoamento. Outras estão mais prontas a se esfacelar. Mas todas são ao mesmo tempo sustentáculos e obstáculos. Obstáculos, assinalam-se como limites dos quais o homem e suas experiências não podem libertar-se. [...] O exemplo mais acessível parece ainda o da coerção geográfica. Durante séculos, o homem é prisioneiro de climas, de vegetações, de populações animais, de culturas, de um equilíbrio lentamente construído, do qual não se pode desviar sem o risco de pôr tudo novamente em jogo (BRAUDEL, 1969, pp. 49-50).

De grande importância à ideia de território em desenvolvimento neste capítulo, é a interpretação dada por Metri (2018) a proposição braudeliana. Para Metri, a ideia de coerção geográfica está associada ao conceito de longa duração desenvolvido por Braudel, dilatando as dimensões espaço e tempo presentes nesse conceito braudeliano. Dimensões que o ciberespaço fundiu, segundo a denúncia feita por Monteiro (2007). Assim, ambas as dimensões "dilatadas a fim de se tentar depreender perenidades e ponderosidades associadas aos objetos em investigação, o que permitiria ressignificá-los e, mesmo, identificar novos problemas" (METRI, 2018, p. 512). Assim, o autor assume

> O princípio de que o espaço físico se constitui numa dimensão da vida, presente em todo fenômeno social, uma vez que as experiências humanas, suas vivências, ocorrem necessariamente a partir de algum espaço concreto. Não há agrupamento social em qualquer momento da história que tenha se desenvolvido fora de um espaço acessível, e cujos movimentos não tenham sofrido influência do meio físico de onde se encontravam.

A geografia braudeliana se configura como "uma geografia da ação, do movimento, uma geografia das relações de força e daquilo que se arrisca nas lutas territoriais [...]." (LACOSTE, 1988, p. 176). De modo que Metri (2018) define tal

geografia como “uma concepção ampla, [...] complexa (porque contraditória) do exercício de reflexão geográfica”. A dimensão física das configurações espaciais vai além de uma moldura rígida ou de um elemento coercitivo da história humana, mas é também uma estrutura dotada de significados que sofrem modificações quando a dimensão física é analisada a partir dos movimentos humanos.

Como Metri (2018, p. 513) sintetiza,

> as configurações espaciais podem ser pensadas a partir de seus elementos físicos e também humanos. Nesse caso, a geografia torna-se impregnada por fenômenos sociais com capacidade de alterar os entendimentos sobre seus recortes físicos, sem deixar de ser “impregnadora” de elementos coercitivos.

Com base no até aqui exposto, entende-se haver a necessidade de se repensar a infraestrutura da Internet a partir da mesma enquanto parte do ciberespaço e elemento físico constituinte da geografia mundial. Como Bauman et al. (2014) traz, comumente, os assuntos cibernéticos são tratados a partir do seu aspecto intangível, focando nas interações via *softwares* e relegando, quando tal, a segundo plano a importância detida pelos *hardwares.*

Entretanto, as interações que se dão na esfera intangível demandam que os componentes tangíveis existam, e mais do que isso, diversos tipos de interações humanas ocorrem devido a existência dos componentes físicos. Desde a extração de insumos destinados as produções dos supracitados componentes até a manutenção, somando-se a isso os impactos no cotidiano que deles decorrem – tais como demandas energéticas, impactos ambientais, desdobramentos econômicos ou mesmo as consequências psicossomáticas das próprias interações sociais em ambientes cibernéticos.

Conforme dito, entende-se que a análise da espacialidade e da territorialidade demandam a investigação da dimensão do poder. Conforme o alemão Friedrich Ratzel (2011), o território é o espaço sobre o qual um Estado exerce a sua soberania. Para o autor,

> o homem não é concebível sem o solo terrestre, ainda mais sem a maior obra do homem sobre terra: o Estado. Assim como os termos cidade e estrada expressam, respectivamente, uma fração de humanidade e uma obra humana; quando se fala de Estado, designa-se uma fração de superfície terrestre. O Estado é obrigado a viver do solo. Ele possui invariavelmente apenas as vantagens oferecidas por um solo que lhe é assegurado. É o que exprime a ciência política quando diz que o território pertence à essência do Estado. Ela designa a soberania como *jus territoriale* e estabelece a regra de que as mudanças territoriais podem fazer-se apenas por leis (RATZEL, 2011, p. 51).

A visão de Ratzel converge com a leitura quanto ao tema em Haesbaert (2004), onde o conceito de território correlaciona-se com a ideia de poder, seja por dominação

dentro de um território como por apropriação de um espaço (ideia de propriedade). Segundo Haesbaert (2004, p. 95-96), pode-se "afirmar que o território, imerso em relações de dominação e/ou de apropriação sociedade-espaço, desdobra-se ao longo de um *continuum* que vai da dominação político-econômica mais 'concreta' e 'funcional' à apropriação mais subjetiva e/ou 'cultural-simbólica'".

Sack (1986, p. 219) afirma que "a territorialidade, como um componente do poder, não é apenas um meio para criar e manter a ordem, mas é uma estratégia para criar e manter grande parte do contexto geográfico através do qual nós experimentamos o mundo e o dotamos de significado." De forma que o conceito de território incorpora em si a dimensão política, as relações econômicas e culturais, visto que está ligada à como as pessoas se organizam e interagem.

Para Gottmann (1975, p. 526):

> Território é um conceito político e geográfico, porque o espaço geográfico é tanto compartimento quanto organizado através de processos políticos. Uma teoria política que ignora as características e a diferenciação do espaço geográfico opera no vácuo.

Ao pressuposto de território, soma-se o de soberania, sendo eles de suma importância tanto para a constituição da ideia de Sistema Interestatal quanto da conceitualização de Estado, sendo esse central no campo dos estudos das Relações Internacionais desde a assinatura dos Tratados de Vestfália que deram desfecho a Guerra dos 30 anos (1618-1648). A Paz de Vestfália e seus tratados, entre outras coisas, se constituem como marco pelo reconhecimento de que os Estados detêm autoridade sobre território determinado como seu, não cabendo intervenção sobre territórios reconhecidos como pertencentes aos Estados signatários dos tratados, representando isso flagrante violação à soberania. De modo que o conceito de soberania é dotado de um aspecto nacional e internacional.

Segundo Krasner (1999), o termo soberania tem sido usado de quatro maneiras diferentes ao voltarmos nossos olhares para as relações internacionais – soberania legal internacional, soberania vestfaliana, soberania doméstica e soberania da interdependência. A soberania jurídica internacional compreende-se como as práticas associadas ao reconhecimento mútuo entre territórios dotados de independência jurídica formal. A soberania vestfaliana, por sua vez, diz respeito à organização política baseada na exclusão de atores externos das estruturas de autoridade dentro de um determinado território. A soberania doméstica refere-se à organização formal da autoridade política

dentro do Estado e a capacidade dessas autoridades públicas de exercerem controle efetivo dentro das fronteiras de sua própria política. Por último, a soberania da interdependência faz referência à capacidade das autoridades estatais de regulamentarem e controlarem o fluxo de informações, ideias, bens, pessoas, poluentes ou capital além das fronteiras de seu estado.

Ainda segundo Krasner (1999, p.4, tradução nossa), "a soberania legal internacional e a soberania vestfaliana envolvem questões de autoridade e legitimidade, mas não de controle. Ambos têm regras ou lógicas distintas de adequação." Sendo a regra para a soberania jurídica internacional o reconhecimento que é estendido às entidades territoriais que possuem independência jurídica formal. A regra para a soberania vestfaliana constitui-se enquanto exclusão de atores externos, de fato ou de direito, do território de um Estado.

A soberania doméstica por sua vez envolve a autoridade e o controle, assim como a especificação da autoridade política legítima e a extensão em que essa autoridade pode ser efetivamente exercida. Por último, a soberania da interdependência preocupa-se exclusivamente com o controle e não com a autoridade, focando na capacidade de um Estado regular os movimentos através de suas fronteiras.

De modo que, ao falarmos de Estados, independente da forma que o termo soberania seja utilizado, a ideia de território está fortemente atrelada e é de suma importância. Entretanto, cabe novamente ressaltar que ambos os conceitos são assumidos pela sociedade e pelas teorias *mainstream* do campo da ciência política e das relações internacionais como dados e ahistóricos.

A breve exposição quanto aos conceitos de soberania e território, não só permite a compreensão quanto a importância deles para a legitimidade do Sistema Internacional, mas também reafirma a possibilidade de expansão da ideia de território para além do material tangível, permitindo através das concatenações de autores alheios e anteriores aos estudos do ciberespaço a compreensão das tecnologias cibernéticas enquanto território e dotadas de importância igual aos territórios terrestre, marítimo, aéreo e espacial.

Segundo Lambach (2020, p.11), "os territórios no ciberespaço são construções não exclusivas, que se sobrepõem e se cruzam, cujas formas e características estão sendo constantemente renegociadas." Assim o ciberespaço na verdade diz respeito a "uma multidão de territórios flutuantes, entrecruzados e às vezes conflitantes." Podendo existir territórios de origem privada, corporativa ou estatal.

Territórios privados fazem referência a capacidade de pessoas se organizarem na Internet em espaços com fins tipicamente sociais, como comunidades online ou salas de bate-papo (LAMBACH, 2020). Devido à finalidade buscada e aos recursos limitados dos usuários, esses territórios geralmente são relativamente pequenos em escala. De grande importância ao trabalho são os processos de territorialização corporativos e estatais.

A territorialização estatais, como Lambach (2020, p. 18, tradução nossa) chama atenção, “são ciber analogias para o território físico do Estado, buscando solidificar o alcance regulatório dos estados e sustentar reivindicações jurisdicionais. Assim, Estados reivindicam para si a judicialização das atividades em que o componente físico – o elo com a realidade, esteja em seu território. Com isso, o território virtual coincide com o território real. Alcançando usuários, servidores ou dados.

Discursos sobre 'cibersoberania', 'soberania de dados' ou 'soberania digital' deixam mais claro a analogia e revestem o tema dos mesmos caráteres internos e externos presentes na questão da soberania. De forma que os efeitos se dão sobre a busca do controle interno do compreendido como ciberterritório – o que se vê na produção de leis que buscam controlar os comportamentos dos usuários em ambiente cibernético, mas também impacta a dinâmica interestatal contra a agência de outros Estados sobre seu território.

Os *firewalls* nacionais são uma das formas mais conhecidas e eficazes para os governos reivindicarem a cibersoberania e exercerem poder sobre determinada porção territorial. Outro exemplo de poder dentro de um ciber-território é a possibilidade de utilização de kill switches, ‘bloqueadores de rede’ da internet, com os quais se pode desligar partes ou completamente a rede nacional de Internet por longos períodos de tempo. Outro exercício de poder estatal é a capacidade de acesso a dados dos usuários via leis que impõe às empresas o envio dos mesmos às agências governamentais (LAMBACH, 2020).

O processo de territorialização corporativo pode se mostrar mais evidente ao voltarmos nossos olhares a grandes corporações como Google, Apple, Facebook, Amazon e Microsoft e como esse processo é realizado através da gama de serviços ofertados aos seus clientes, bem como de recursos técnicos. Lambach (2020) chama a atenção para o fato que se no passado as ciber-fronteiras entre os territórios corporativos eram mais rígidas, agora vivenciamos a era da expansão de verdadeiros ecossistemas cibernéticos – embora cada vez mais inseridos em nossas vidas são também menos visíveis.

Os ecossistemas são baseados na integração de múltiplos serviços, de modo que é criada uma rede mais densa em seu núcleo, enquanto suas bordas permanecem relativamente porosas. Com esse arranjo tecnológico, estas empresas buscam criar produtos que "definam um 'território' na virtualidade através do qual todos os outros usuários irão querer ou terão que passar" (PRATT, 2000, p. 433). Para tal fim, as corporações usam uma série de recursos como gerenciamento de direitos digitais (DRM – sigla em inglês), licenças limitadas, cookies e requisitos de inscrição para criar limites que permitem o recolhimento de dados, a vigilância de utilizadores e a monetização do acesso a conteúdos digitais. Essas práticas não só traçam limites como também criam efeitos de aprisionamento, o que endurece as fronteiras entre os ecossistemas (LAMBACH, 2020).

Como destaca Lambach (2020), certos territórios corporativos também se estendem à infraestrutura do ciberespaço. Um exemplo corriqueiro, citado pelo autor, é o leitor de e-book desenvolvido pela Amazon – Amazon Kindle. Essa realidade tende a se estender nos próximos anos com a difusão da tecnologia 5G e a disso decorrente profusão de equipamentos da Internet das Coisas.

Um elemento de suma importância é a compreensão que os ecossistemas desenvolvidos por essas grandes corporações não são hermeticamente isolados do resto do ciberespaço. Os ecossistemas corporativos interagem entre si, entre outros recursos, através de conjuntos de definições e protocolos que facilitam a comunicação e troca entre uma empresa e outros aplicativos que utilizam seus ativos. De forma que através da gestão das fronteiras dos seus territórios as companhias definem o nível de acesso que outras corporações têm aos dados e usuários que circulam dentro do seu ciber-território. Mas não são somente outras corporações que têm acesso a tais informações.

Embora geralmente as grandes companhias de tecnologia (as *Big Techs*) se mostrem contrárias à regulamentação estatal – que consideram ilegítimas, ineficazes e para os puristas tecnológicos sufocam os efeitos libertadores e fortalecedores da tecnologia (KOHL; FOX, 2017, p. 10), elas cumprem a maioria dos regulamentos legais determinados pelos estados. Mesmo que a contragosto e nos seus próprios termos (LAMBACH, 2020).

Como constata Lambach (2020, p. 24, tradução nossa), os "ciber-territórios corporativos e estatais se cruzam, permitindo que o estado delegue a aplicação das leis estatais aos dirigentes corporativos, responsabilizando as corporações pelas infrações legais que ocorrem em 'seus' territórios". Como explica Berman (2018, p. 12), tal

capacidade é estimada pelos Estados devido ao alcance global que elas detêm e por isso se refletir positivamente sobre a eficácia legal pretendida pelos Estados. Isso se explicaria pelo argumento desenvolvido por Lambach (2020), segundo o qual, os Estados têm grande controle sobre a infraestrutura localizada em seu país, mas pouco controle sobre os aspectos globais do ciberespaço.

É bem verdade que os Estados detêm pouco poder e controle sobre os aspectos globais que extrapolam a sua territorialidade física, mas quanto ao poder de ingerência sobre a infraestrutura localizada em seu país cabe a ressalva das sérias consequências decorrentes de possíveis intervenções estatais. Com exceções dos equipamentos pertencentes ao Estado, os demais são salvaguardados pelo direito de propriedade. Embora haja condições de sobrepor o interesse público ao privado, é necessário que se entenda as consequências econômicas de se opor arbitrariamente sobre grandes conglomerados tecnológicos.

A multiplicidade de territórios regulatórios e a falta de regras claras para resolução de controvérsias provocou debates sobre a necessidade de regulação do ciberespaço (SVANTENSSON, 2016), em especial nas áreas de ciberdefesa e cibersegurança (FINNEMORE; HOLLIS, 2016, SCHMITT, 2017). O debate em questão se dá entre os que defendem um modelo multissetorial e os defensores de um modelo multilateral de governança da internet, tendo grande importância nas argumentações a permissibilidade das regulações de caráter extraterritoriais.

A abordagem multilateral tem como centro ideias fortemente ligadas a visão de soberania e soberania cibernética, seus defensores entendem ser preciso uma forma de governança mais centrada no Estado, mediada por organizações intergovernamentais como as Nações Unidas (ONU) ou a União Internacional de Telecomunicações (ITU). Por outro lado, a abordagem multissetorial – modelo predominante de governança da internet desde a década de 1990 – enfatiza a necessidade de inclusão de atores privados na formulação de políticas, bem como a influência limitada dos governos e uma arquitetura descentralizada da internet.

Países como China e Rússia argumentam que esse modelo “é uma fachada para manter o domínio centrado no Ocidente sobre esse novo 'recurso global’" que é a Internet (LANTIS; BLOOMBERG, 2018, p. 156) e não respeita a soberania nacional (ARONCZYK; BUDNITSKY, 2017; WEI 2017). Tais acusações alcançam justamente os Estados Unidos e seus aliados ocidentais, maiores defensores de um modelo de governança da Internet multisetorial.

Como Lambach (2020) traz, esse debate, que já dura mais de duas décadas, resultou em instituições de governança da Internet. Esse já longo debate tem ocorrido em locais como o Primeiro Comitê da Assembleia Geral das Nações Unidas – desde 1998, as Cúpulas Mundiais sobre a Sociedade da Informação de 2003 e 2005 e o Fórum Anual de Governança da Internet endossado pela ONU, e inaugurado em 2006.

Em 2011, Rússia, China, Tadjiquistão e Uzbequistão propuseram um código de conduta internacional para segurança da informação à Assembleia Geral da ONU, o código de conduta foi posteriormente elaborado em uma proposta para a Conferência Mundial sobre Telecomunicações Internacionais (WCIT – sigla em inglês) em 2012 para que o tratado de Regulamentos Internacionais de Telecomunicações da União Internacional de Telecomunicações (UIT) fosse alterado e passasse a incluir a Internet em seu âmbito. Isso conferiria à UIT alto grau de autoridade sobre muitos aspectos da governança da Internet.

A WCIT se desfez pela falta de acordo entre as partes em decorrência do choque de visões sobre o modelo de governança global – tendo os delegados dos Estados Unidos chegado a abandonar a reunião. Em 2014, algumas questões contenciosas foram retomadas e resolvidas na Reunião de Plenipotenciários da UIT, entretanto, chegou-se "ao consenso de que temas relacionados à privacidade, vigilância e direitos humanos são importantes, mas estão fora do escopo do trabalho da UIT" (PRESCOTT, 2014).

Segundo Lambach (2020, p. 22, tradução nossa), essas "disputas podem ser lidas como uma competição entre 'projetos territoriais', onde os multilateralistas vislumbram uma internet mais verticalmente integrada aos territórios estatais e com possibilidade de cooperação interestatal. Os multisetorialistas, por sua vez, preferem uma internet mais aberta e descentralizada, onde estados e partes privadas interessadas venham a trabalhar juntos. Segundo Aronczyk e Budnitsky (2017), a posição multisetorial converge com as regulações extraterritoriais, enquanto a multilateral as vê como uma invasão dos territórios nacionais.

O fato de presenciarmos um antagonismo de ideias entre países que de um lado são tidos por boa parte da comunidade internacional como "autocráticos" e do outro ter-se países tidos como democracias consolidadas tende a influenciar o olhar desse debate. Porém, a melhor compreensão do debate entre multilateralistas e multissetoriais, bem como a sua real importância política e estratégica só é alcançada quando se olha para como as grandes potências tem se valido da infraestrutura da Internet e dos ciberterritórios.

Como Krasner (1999) bem traz, fala e ação nem sempre coincidem. “Os governantes podem consistentemente reafirmar o seu compromisso com a não intervenção, mas ao mesmo tempo tentar alterar as estruturas institucionais domésticas de outros estados”. Em um mundo que passa por um processo de forte integração entre os Estados desde a Segunda Guerra, os mecanismos de intervenção se tornam cada vez mais sofisticados, como os casos em que estados se valem de mecanismos econômicos – seja fornecendo empréstimos ou aplicando sanções. Por vezes, entretanto, tais mecanismos podem ser invisíveis, como os que permeiam a parte “virtual” do ciberespaço, ou visíveis, mas não perceptíveis como ameaças à soberania nacional – casos dos equipamentos que constituem a infraestrutura da Internet.

A seção seguinte se destina a mostrar como os Estados Unidos têm se valido do seu pioneirismo nas Tecnologias da Informação e Comunicação, do seu poderio econômico, da sua influência no estabelecimento de padrões e regulações para a territorialização do ciberespaço global, de modo a estender sua soberania e o poder de agência dela decorrente de um modo extraterritorial e de modo assimétrico.

3.2 O ciberpoder

Os norte-americanos foram fundamentais no surgimento das Tecnologias da Informação e Comunicação (TICs). Sendo esse processo de desenvolvimento tecnológico fruto da interação entre o complexo militar dos Estados Unidos com seus acadêmicos e seu setor industrial no contexto da Guerra Fria. O que também ocorreu no processo de conversão dessas tecnologias de origem militar para o âmbito civil. Sendo esse o caso, também, da Internet. De modo que desde a origem dessas tecnologias os Estados Unidos exercem papel de liderança e ditam os rumos dos processos de fragmentação produtiva e de difusão tecnológica, estabelecendo padrões tecnológicos e detendo patentes de tecnologias estratégicas, influenciando regulações internacionais e também a atuação de organismos internacionais de controle.

O processo de liberalização global foi fundamental para a difusão da Internet e para que os EUA emergissem como os dirigentes na “governança global da Internet” em seu processo de ascensão. Sendo as multinacionais norte-americanas beneficiadas nesse processo (MARZINOTTO, 2022).

Sendo assim, o modo como a Internet é usada hoje foi amplamente influenciada pelos Estados Unidos, o que confere vantagem estrutural aos norte-americanos. O que

fica mais evidente ao analisarmos o Comando Militar Cibernético dos Estados Unidos, que se estrutura especialmente após os atentados de 11 de setembro e toda a regulamentação decorrente da comoção nacional e sensação de ameaça geradas pelos atentados.

Diante do contexto da Guerra ao Terror iniciada no governo Bush, o desenvolvimento de tecnologias biométricas, de comunicação e de monitoramento se deu de maneira muito rápida, movidas por um senso de perigo iminente e de emergência. O emprego de tais tecnologias buscava levar a cabo a filtragem daqueles percebidos como perigosos, mesmo havendo reconhecida imprecisão na definição do conceito de inimigos, podendo abarcar a qualquer um cujo a subjetividade dos parâmetros dos agentes responsáveis pelo monitoramento assim nominasse.

A fim de monitorar esses perigos invisíveis e iminentes, as agências de segurança dos Estados passaram a apoiar medidas provisórias e decretos executivos por parte do governo que flexibilizavam leis e direitos, tornando possível ações preventivas, antes que novos ataques ocorressem. O que possibilitou que as agências de inteligência norte-americanas tivessem acesso a um número praticamente ilimitado de dados que circulavam pela infraestrutura de Internet norte-americana.

A partir da autorização do então presidente George W. Bush, desde o dia 4 de outubro de 2001, a Agência Nacional de Segurança (NSA, na sigla em inglês) se viu dotada de capacidade de monitorar comunicações que ocorriam dentro do território norte-americano (como ligações ou e-mails) sem a necessidade de permissão e regulação por parte do Tribunal de Vigilância de Inteligência Estrangeira (FISC, na sigla em inglês).

> (U//FOUO) No dia 4 de outubro de 2001, o Presidente W. Bush emitiu um memorando intitulado ‘AUTORIZAÇÃO PARA ATIVIDADES DE VIGILÂNCIA ESPECÍFICAS POR PERÍODO LIMITADO PARA DETER E PREVENIR ATOS DE TERRORISMO DENTRO DOS ESTADOS UNIDOS.’ O memorando se baseia na determinação do Presidente de que após os ataques de 11 de setembro nos Estados Unidos, uma emergência extraordinária existia para propósitos de defesa nacional. (NSA, *ST-09-002 Working Draft*, 2009, p.1. tradução nossa)

Para que a interceptação acontecesse, um dos lados da comunicação deveria ser oriundo de um país estrangeiro e que estivesse sob suspeita de envolvimento com atividades terroristas. O que permitiu que cidadãos em território norte-americano tivessem suas comunicações monitoradas sem necessidade de autorização judicial. Essas atividades de vigilância eram chamadas de Programa de Vigilância do Presidente (PSP, na sigla em inglês) (HARRIS, 2014).

A autorização dessas atividades de vigilância conduziu a NSA a acessar um volume de dados tal que praticamente impossibilitava a distinção de sua origem, sendo difícil saber se provinha de comunicação doméstica ou estrangeira. A solução ofertada pelo PSP fora inicialmente apontada como temporária às questões jurídicas acerca do FISA, tanto no tocante a defasagem da legislação com relação às novas tecnologias, como quanto à necessidade de sigilo acerca das operações das agências de inteligência. Porém, ocorreu uma escalada da atividade de vigilância do Estado norte-americano (HARRIS, 2014).

A estruturação do aparato de vigilância norte-americano seguiu com a criação do *Metadata Analysis Center*, o MAC, um centro de vigilância 24h da NSA, situado no *Signals Intelligence Directorate*, parte da NSA. Tendo sido autorizado pelo então presidente Bush no dia 4 de outubro de 2001 passou a funcionar 3 dias depois, no dia 7 de outubro daquele ano. Segundo Harris (2014), o MAC era responsável pela interceptação e armazenamento dos dados de comunicações digitais. O MAC, passaria a ser chamado pelo codinome de *Starburst*, e posteriormente de *Stellar Wind*.

O novo aparato tecnológico desenvolvido permitia o mapeamento de contatos entre pessoas, das suas interações e relações. A partir dos dados interceptados o método *Contact Chaining* organizava os contatos de uma pessoa suspeita, estabelecendo através das informações obtidas, tais como a duração, frequência e hora que ocorreu a comunicação, as relações sociais que esse monitorado mantinha com outras pessoas, por sua vez, em uma outra camada de vigilância, todos os contatos das pessoas com as quais o primeiro monitorado se comunicou também eram monitorados. Essa dinâmica continuava de maneira progressiva e em algumas camadas de vigilância poder-se-ia chegar a milhões de pessoas a terem seus dados coletados (HARRIS, 2014).

Dada ao nível de volume de dados acessados e acumulados, o processo demandava o desenvolvimento de formas cada vez mais automatizadas de representação desses dados coletados, o que gerava gráficos e mapas para auxiliarem os analistas a fazerem suas leituras de inteligência. O *Stellar Wind* ainda possibilitava a integração e o compartilhamento de informações e ações com outras agências de segurança, não apenas militares, mas também civis e domésticas, de policiamento (HARRIS, 2014).

Posteriormente, a Lei de Proteção à América (*Protect America Act)* de 2007 ampliou amplamente os poderes das agências de inteligência, permitindo pleno acesso a instalações de empresas privadas em solo americano e condução de vigilância de cidadãos sem necessidade de mandato, desde que estes fossem o foco da investigação ou que se

comunicassem com suspeitos. Permitiu a mineração de dados de maneira mais ampla e complexa, empreendida por *softwares* capazes de realizar *contact chaining* (um método de mapeamento de contatos entre pessoas, bem como da interação e relação entre elas, realizada por camadas ou níveis). Como resultado, a Lei de Proteção à América, seguido pelas emendas a Lei de Vigilância de Inteligência Estrangeira (*Foreign Intelligence Surveillance Act* - FISA) de 2008, lançaram as bases para o sistema massivo de vigilância global mais sofisticado e robusto até então, o PRISM.

De acordo com Harris (2014), cerca de um mês após a submissão do *Protect America Act*, o programa de vigilância e coleta de dados, PRISM, já estava operante. Empresas como Microsoft, Yahoo, Google, Facebook e YouTube, responsáveis por quantidades gigantescas de tráfego de dados da internet, dentro e fora dos EUA (HARRIS, 2014, p.44), aderiram ao programa PRISM.

Como Harris (2014, p. 44-45) explica, na internet a informação é fragmentada em pacotes de dados e enviada de maneira dispersa por caminhos mais eficientes e rápidos, sendo reagrupada no seu destino; esse destino, contudo, é – até então – frequentemente o servidor das próprias empresas que oferecem serviços de internet. Por exemplo, ao se enviar um e-mail por um endereço eletrônico da Google ("*gmail*"), o destino final geralmente são os servidores da Google, e não o destinatário da mensagem – o que possibilita o monitoramento pela NSA.

Dentro dessa realidade factual, a NSA se vê dotada de vigiar e espionar, quase que sem limites, uma quantidade gigantesca de usuários da internet (civis, militares, chefes de Estado, empresas públicas e privadas), de todas as partes do globo. O PRISM portanto, de acordo com os documentos divulgados em 2013 pelo ex-funcionário da CIA, Edward Snowden, armazenava e organizava não apenas metadados, mas também informações e conteúdo de caráter pessoal. Sendo essas informações compartilhadas com outras agências de inteligência, polícia e investigação (HARRIS, 2014).

O que se vê é uma crescente importância e um crescente investimento em tecnologias de monitoramento e vigilância dos meios digitais vivenciados desde os atentados de 11 de setembro, que se manteve em crescimento em importância dentro da estrutura de segurança norte-americana, como apontam os dados do governo Obama. Cabe, porém, novamente a observação que diz respeito à materialidade do assunto em tela e que se refere também às relações de poder intracampo. A discussão quanto às tecnologias de comunicação em massa, internet e vigilância cibernética tendem a fazer referência majoritariamente ao mundo virtual.

Souza Filho (2018) analisa que o “mundo virtual” tende a ser caracterizado como um “espaço não material", onde se encontram sujeitos que geograficamente não poderiam se relacionar, em termos de intensidade, velocidade e constância, fora desse espaço virtual. Entretanto, o caráter virtual da internet é indissociável do material” (SOUZA FILHO, 2018, p.31).

A análise da cibersegurança demanda que pensemos também nos aspectos materiais constituintes da Internet: os cabos ópticos submarinos que constituem a rede, seguido dos servidores, e finalmente grandes empresas e companhias fabricantes de tecnologias que possibilitam acesso à internet, como modems, roteadores, softwares e hardwares. Bauman *et al*. (2014) aborda a questão dessa materialidade estratégica do espaço virtual, aponta que embora o foco quando se discute cibersegurança geralmente esteja voltado para *softwares* e perícia em codificação, os *hardwares* também são de suma importância. Estando os discos de armazenamento, os cabos submarinos e demais elementos tecnológicos e de engenharia da maquinaria a serviço da liberdade de comunicação e do monitoramento e controle (BAUMAN *et al*, 2014, p.139).

A importância da materialidade do assunto fica mais nítida ao analisarmos como o governo dos EUA passou a tratar a infraestrutura do setor nos anos recentes, em especial no governo Obama. Em maio de 2009, numa conferência na Casa Branca, Obama proferiu um discurso sobre o novo status que a cibersegurança iria gozar em sua administração:

> Minha administração irá seguir uma nova abordagem para dar segurança à infraestrutura digital da América. […] De agora em diante, nossa infraestrutura digital - as redes e computadores dos quais dependemos todos os dias - será tratada como deveria; com valor estratégico nacional. Proteger essa infraestrutura será uma prioridade de segurança nacional. (OBAMA apud HARRIS, 2014, p.156. tradução nossa)

Assim, toda a infraestrutura digital dos EUA – as redes e computadores dos quais se dependem todos os dias – seriam tratados com valor estratégico nacional. Passando a proteção dessa infraestrutura a ser uma prioridade de segurança nacional (Harris, 2014). Pouco tempo depois, cerca de um mês, o então Secretário de Defesa, Robert Gates, anuncia a criação do *US Cyber Command*, também conhecido como *CyberCom*. O *CyberCom* conferiu aos agentes de cibersegurança e à sua matéria grande importância, figurando o ciberespaço como uma das outras quatro esferas de guerra reconhecidas pelo governo estadunidense; mar (Marinha), terra (Exército), ar (Aeronáutica) e espacial (NASA), e agora ciberespaço (*CyberCom*). Mais ainda, sua criação demonstra a disposição do governo dos EUA de pensar o ciberespaço como uma matéria

predominantemente estratégica e de domínio militar. A decisão do presidente Obama de transformar a infraestrutura digital do país em matéria de segurança estratégica nacional englobava em grande parte as empresas e companhias civis e privadas.

Em 2010, durante o governo Obama, a preocupação quanto à emergência de guerras cibernéticas constou no *Quadrennial Defense Review* (DAGGETT, 2010) e no NSS-2010. O NSS-2010 detalha que as ameaças de segurança cibernética representam uma das mais sérias questões de segurança nacional, de segurança pública e econômica. Aponta que as mesmas tecnologias que capacitam o Estado norte-americano a liderar e criar também capacitam aqueles que o intentam perturbar e destruir. Sendo o domínio em tais setores tecnológicos que permitem a superioridade militar dos EUA. Dependendo a vida diária e a superioridade militar da infraestrutura digital, se faz necessário considerá-la como um ativo nacional estratégico, e, por conseguinte, protegê-la - salvaguardando a privacidade e liberdades – conferindo-lhe o status de prioridade de segurança nacional. Buscando assim, deter, prevenir, detectar e defender-se (NSS-2010).

A produção de tecnologias de ponta é protagonizada pelos países centrais do capitalismo e reflete a localização dos maiores servidores do mundo. Sendo assim, as limitações e desigualdades sociais, econômicas e militares entre os países e as desigualdades e assimetrias cibernéticas se retroalimentam e intensificam questões geoestratégicas e políticas. Países da Europa, EUA e China possuem densidades de conexões de cabos ultramarinos completamente desiguais com o resto dos países do mundo.

Ademais, os valores empenhados nos países centrais agravam a desigualdades e deixam evidentes a suscetibilidade de países da periferia global quanto a assuntos cibernéticos. Existindo mesmo entre os países centrais discrepância entre os valores investidos em suas agências responsáveis por suas seguranças cibernéticas, por exemplo, a NSA, em 2014, possuía um orçamento de U$10.8 bilhões (7.8 bilhões de euros) por ano, enquanto na Europa, o orçamento da sua agência equivalente britânica, o Centro Governamental de Comunicações (*Government Communications Headquarters* – GCHQ), trabalhava com um orçamento de €1.2 bilhões, muito abaixo do orçamento da NSA, que era, entretanto, mais que o dobro do orçamento anual de agências equivalentes, como por exemplo, o Serviço Federal de Informações Alemã (*Bundesnachrichtendienst* ou BND) (BAUMAN et al., 2014).

Diante desse contexto de extrema complexidade, onde o elemento material aguça assimetrias e desigualdades entre os Estados – sejam elas tecnológicas ou geoestratégicas

– e o virtual permite o estabelecimento de uma rede transnacional – que permite intenso fluxo de dados entre os Estados e aproxima métodos e interesses de diferentes agentes da (in)segurança pelo mundo – constrói-se um cenário onde aliados e inimigos tornam-se cada vez mais difíceis de serem distinguidos.

Os aliados que somam forças na árdua tarefa de garantir a cibersegurança para os seus Estados podem se valer da estrutura criada para se espionarem. Um exemplo disso foi construído pelo somatório da inciativa 'Cinco Olhos' ('Five Eyes') e os vazamentos de documentos secretos da inteligência norte-americana por Edward Snowden. Como detalha Bauman *et al*. (2014) o chamado 'cinco olhos' ('five eyes') (inicialmente Estados Unidos - Reino Unido – Canadá – Austrália - Nova Zelândia, e que agora conta com outros países europeus) é a rede de serviços de inteligência para monitoramento de dados circulantes na internet. Essa rede parece ter sido o principal veículo pelo qual a NSA aumentou sua capacidade de vigilância além das suas próprias possibilidades técnicas, conseguindo assim, um alcance global. Sendo os cabos submarinos de suma importância para atingir esse fim (BAUMAN *et al*., 2014, p.127).

Os vazamentos de informações confidenciais da NSA, realizados por Edward Snowden, mostraram um uso da ampla rede e mecanismos de vigilância que foi muito além dos objetivos inicialmente acordados para o combate ao terrorismo global. Os vazamentos revelaram, entre outras coisas: espionagem industrial, vigilância de populações para identificar perfis de consumidor, bem como de tendências políticas relativas aos possíveis resultados eleitorais destes países, além de espionagem de mensagens pessoais de importante figuras políticas, não só de países europeus, mas também de outros como o Brasil, por exemplo (BAUMAN *et al*, 2014; SOUZA FILHO, 2018).

As assimetrias do elemento material não só interferem nas capacidades de cada agência de inteligência, mas também demonstram a existência de relações de poder e que essas não são negligenciáveis. De modo que mesmo ao nos atermos a casos envolvendo países com grande investimento em cibersegurança é possível constatar violação do pressuposto de soberania, o que se constitui uma relação muito mais assimétrica ao nos atermos a países com baixa capacidade de investimento.

As atividades de vigilância e espionagem não são novas nas relações entre Estados, bem como o reconhecimento do uso da Internet e sua infraestrutura para tais fins. Também não se faz novo o reconhecimento das vantagens detidas pelos EUA para o exercício dessas práticas em decorrência do seu pioneirismo e alto investimento no

tocante a Internet. O que se constitui como novo é a tentativa chinesa de incrementar seu ciberpoder e os resultados disso sobre o poder norte-americano como um todo.

A novidade exposta decorre do fato que o 5G desenvolvido pela Huawei possui larga vantagem sobre as versões concorrentes europeias; da atuação do Estado chinês para estabelecer os padrões tecnológicos da "nova Internet"; das políticas do Estado chinês de financiamento de infraestrutura ao redor do mundo e do investimento do Estado chinês em tecnologias como Inteligência Artificial, aprendizado de máquina e análise de *Big Data*.

A Huawei e o governo chinês, anos antes de 2019, já atuavam de modo a investir na infraestrutura das TICs e a influenciar as regulamentações e as especificações no âmbito internacional da tecnologia 5G, por meio da estratégia que Adam Segal chamou de Ciber diplomacia chinesa (SEGAL, 2016; SEGAL, 2017).

Como detalhado em Segal (2017), o governo chinês tem usado o comércio e o investimento em infraestrutura de TICs com fins econômicos, mas também como ferramenta política indireta. O que se vê é uma atuação chinesa na África, Sudeste Asiático e Ásia Central buscando acesso à mercados, bem como criar apoio para a política externa de Pequim e normas do ciberespaço.

Embora o investimento nem sempre se transforme em influência – devido ao foco empresarial voltado para os lucros e mesmo as empresas estatais serem altamente motivadas por incentivos econômicos que podem ser contrários aos objetivos de Pequim – ainda assim, há uma preocupação no âmbito internacional no tocante a possibilidade dos laços econômicos fornecem a Pequim influência direta e indireta e alavancagem. Simplesmente fornecendo fontes alternativas de financiamento, minando com isso os esforços dos Estados Unidos e da Europa no desenvolvimento de normas (SEGAL, 2017).

A ajuda dos Estados Unidos e da Europa muitas vezes vêm acompanhadas de condicionalidades em relação à democracia, transparência e responsabilidade. Como o Instituto de Estudos de Segurança da União Europeia (IESUE) colocou em um relatório sobre capacitação cibernética: "A realidade é que, como doador, a União Europeia (UE) não opera no vácuo e, portanto, deve ser prudente; os destinatários podem ir para a China para financiamento se acharem que a UE espera muito deles." (ISS apud SEGAL 2017, p.12, tradução nossa)

Grande parte do investimento e comércio chinês atual ocorre como parte do programa Um Cinturão, Uma Estrada (*One Belt, One Road* - OBOR), uma estratégia de desenvolvimento que visa a conectividade e cooperação em países entre a China e a

Eurásia. O OBOR possui duas ramificações: o Cinturão Econômico da Rota da Seda, que conecta a China ao Golfo Pérsico, Mediterrâneo e Índia Oceano por terra; e a Rota da Seda Marítima do Século XXI, que liga hidrovias regionais.

A China previa um investimento de cerca de US$51,1 bilhões para a construção de uma rede de ferrovias, estradas, oleodutos, portos, minas, e redes de serviços públicos. Sendo os maiores investimentos em energia e mineração, infraestrutura e setores de manufatura. Documentos oficiais chineses enfatizaram a necessidade para construir uma "rota da seda da informação" através de cabos ópticos transfronteiriços e outros redes de linhas troncais de comunicações, projetos de cabos ópticos submarinos transcontinentais e comunicação espacial (via satélite) (SEGAL, 2017).

Em dezembro de 2016, o Ministério da Indústria e Tecnologia da Informação projetou a construção e atualização das redes de telecomunicações na África, com investimentos previstos para totalizar US$173,73 bilhões. Tendo uma série de outros investimentos realizados por empresas chinesas em nós ao longo do *Belt and Road*, e uma série de outros investimentos na África e no Sudeste asiático já planejados (SEGAL, 2017).

A China *Comservice*, uma subsidiária da China Telecom, anunciou a "Construção conjunta da superestrada da informação da África entre a China e a África (*Joint Construction of Africa's Information Superhighway between China and Africa*), com um investimento orçado em US$15 bilhões, que visa alcançar 150.000 quilômetros cobertura de cabo óptico em quarenta e oito países africanos. A China *Unicom*, uma operadora de telecomunicações chinesa, trabalha de modo a instalar cabos ópticos para conectar a Central Ásia, Sudeste Asiático, África e América do Sul (*China go Abroad* 2016). Em 2016, a ZTE concordou em adquirir a empresa turca Netas *Telekomünikasyon* por até US$101,28 milhões, visando expandir a sua atuação nos principais mercados coberto pelo OBOR. (PEREZ, 2016; PEREZ, 2017)

O Estado chinês tem trabalhado de modo a transformar comércio e investimentos em capacidade de influenciar a próxima geração de padrões de tecnologia. Tendo ingressado na Organização Mundial do Comércio (OMC), a China passou a atuar para influenciar padrões de tecnologia em software, hardware e comunicação tecnologias. Segundo Segal (2017), os legisladores chineses acreditavam que ao controlarem um padrão isso garantiria a captura de grande parte do valor de mercado.

A China tem atuado de modo a aumentar sua habilidade e sofisticação em organizações de padrões globais, tendo focado seus esforços na próxima geração de

tecnologias de Internet e comunicação – como transparece o envio de grandes delegações para reuniões de normas técnicas. Como se deu em uma reunião de uma força tarefa de Engenharia da Internet, onde a China enviou mais de quarenta delegados para uma reunião de 2015.

A China também tem estado ativa na *International Telecommunication Union* (ITU) trabalhando de forma a liderar o grupo de arquitetura digital – *Digital Object Architecture* (DOA), um sistema de gestão que pode ser relevante na "Internet das coisas" (McDOWELL; GOLDSTEIN, 2016; SEGAL, 2017). O número de representantes enviados para as reuniões que visam estabelecer padrões tecnológicos é significantemente maior que o visto habitualmente em outras delegações. Como noticiado pelo *Wall Street Journal*, a Huawei enviou o dobro de representantes que outras telecomunicações para uma reunião, em 2016, em Viena, para definir as capacidades e especificações de celular de quinta geração (5G) (VERBERGT, 2017; SEGAL, 2017).

Cabe ressaltar, entretanto, que a atuação chinesa não se dá de forma casual, à aleatoriedade de uma mão invisível e de modo desmembrado de uma estratégia nacional. O empenho das forças chinesas em tais medidas converge com a declaração feita por Xi Jinping em 2014 de transformar a China em "uma potência cibernética". Para o presidente chinês, o desenvolvimento das tecnologias da informação e comunicação e a segurança cibernética são "como as 'duas asas de um pássaro'", sendo elas indissociáveis e interdependentes. De forma que a China deveria desenvolver "[...] uma boa infraestrutura e uma poderosa economia de informação, e um contingente de profissionais altamente qualificados para garantir a segurança cibernética e a aplicação da tecnologia da informação" (XI, 2014, p. 238–239).

Conforme Shen (2017) traz e a atuação chinesa reafirma, esse projeto não se tratara de um isolacionismo cibernético chinês por trás do seu "grande *firewall*", sendo dotado da busca por tornar suas corporações do setor da tecnologia da informação e comunicação competitivas em âmbito internacional. Aprofundou-se um processo que já se tornara evidente desde a segunda metade da década de 2000, em especial após a crise de 2008. Período em que se viu a Tencent lançar seu sítio eletrônico em inglês em 2009 e Alibaba e Baidu realizarem parcerias e constituírem *joint-ventures* com Rakuten e Softbank, por exemplo, para adentrarem no mercado japonês (BORELLI, 2022).

Uma das iniciativas que sucederam as falas de Xi Jinping foi o projeto "Internet Plus", adotado em 2015 e que, entre outras coisas, especificou a busca pela integração entre todos os setores da economia e da sociedade à Internet. Objetivava-se com isso uma

maior eficiência e qualidade de setores manufatureiros, agrícolas, energéticos, bem como no *e-commerce* e *fintechs* se valendo da integração da "economia real" e da "economia da Internet" por meio da IoT – o que conferiu grande importância a modelos de negócios pautados pelos serviços e tecnologias digitais, tais quais a computação em nuvem e a Inteligência Artificial (BORELLI, 2022).

Um dos resultados desse projeto foi o expressivo crescimento de empresas digitais chinesas no cenário internacional, em especial ao se falar de Baidu, Tencent e Alibaba – (BAT). Essas companhias chinesas acabaram por se consolidar enquanto conglomerados concorrentes das *Big Techs* norte-americanas. Ainda que essas empresas somente consigam concorrer em certa medida com as gigantes norte-americanas, a Comissão Nacional de Segurança em Inteligência Artificial (*National Security Commission on Artificial Intelligence* – NSCAI, sigla em inglês), através da apresentação de título "Visão Geral do Cenário Tecnológico Chinês", expressou a preocupação norte-americana em manter a liderança das suas companhias no tocante a Inteligência Artificial.

Dentre os apontamentos do documento, destaca-se o fato que na visão chinesa a Inteligência Artificial constitui-se enquanto mais do que um instrumento fundamental para enfrentar os desafios macroeconômicos, mas também um meio e uma oportunidade para atingir a liderança tecnológica global (NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE, 2019, p. 621). O documento norte-americano ainda ressalta a importância das parcerias entre o governo chinês com "campeãs nacionais de Inteligência Artificial" (*National AI Team*) através de contratos que possibilitem seus crescimentos. Essa importância deriva do fato que o governo chinês considera que através do acesso aos dados produzidos pelos usuários dessas companhias, ele pode se valer dos mesmos para diversas aplicações utilizando ferramentas como o aprendizado das máquinas (*machine learning*), em especial o aprendizado profundo (*deep learning*) – recurso tecnológico que busca possibilitar que os dados sejam conseguidos e interpretados de maneira mais próxima a "humana" (NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE, 2019, p. 623; 627).

Como sintetiza Majerowicz (2021, p. 8), a Inteligência Artificial diz respeito "[...] a aplicação dessas técnicas [estatísticas] às grandes massas de dados, possibilitando determinado tipo de automação parcial ou completa de diversos processos de trabalho e atividades humanas". Conforme Borelli (2022, p. 148) explica, a Inteligência Artificial é componente básico do desenvolvimento dos algoritmos que são centrais para os serviços digitais das *Big Techs*, constituindo-se como um *locus* concorrencial intercapitalista e

interestatal importante atualmente. De forma que quanto maior o montante de dados coletados através das *Big Techs*, mais dados também estarão disponíveis para o aprendizado das máquinas (*machine learning*), o que resulta em um maior aprimoramento da Inteligência Artificial. Como produto final, tem-se ferramentas de predição cada vez mais precisos e dispositivos cada vez mais "inteligentes" (BORELLI, 2022).

O artigo elaborado pelo Serviço de Pesquisa do Congresso dos Estados Unidos (Congressional Research Service) intitulado "Inteligência Artificial e Segurança Nacional" detalha como a Inteligência Artificial se articula com o sistema de armas autônomas letais (LAWS, na sigla em inglês); a capacidade de inteligência, vigilância e reconhecimento; controle e comando; veículos autônomos; logística e controle do ciberespaço. As autoridades no assunto, esperam que nos próximos anos o montante de dados produzido e analisados por Inteligências Artificiais mudem completamente a dinâmica de poder existente. Além disso, trazem o alerta quanto a necessidade de um trabalho articulado com o setor privado.

Para além do fato da grande massa de dados que são gerados nos ciberterritórios privados, destaca-se a existência de uma inversão da dinâmica vista desde o surgimento das TICs até o começo do século XXI. Se no passado as tecnologias surgiam no âmbito militar e estatal, hoje, a inovação tecnológica associada à Inteligência Artificial é liderada pelo setor privado. O artigo chama atenção para os riscos decorrentes da dinâmica existente entre os governos dos Estados rivais dos Estados Unidos e suas companhias do setor de tecnologia da informação e comunicação, enxergando um claro trabalho em conjunto sem os filtros dos "valores americanos" que salvaguardariam os direitos dos usuários – sendo a china nominalmente citada como exemplo e ameaça.

Se Zuboff (2020) olha para o tema através do termo que denomina como Capitalismo de Vigilância e chama a atenção para a incrível rentabilidade que as *Big Techs* conseguem através das tecnologias de extração de dados do cotidiano social dos seus usuários, a posterior revenda para anunciantes, os altos investimentos para aprimoramento de tais tecnologias e o riscos disso para democracia, o documento sobre a Estratégia Nacional de Segurança dos Estados Unidos de 2017 (NSS – 2017, sigla em inglês) aponta para o tema da Inteligência Artificial como uma das "tecnologias emergentes críticas para o crescimento econômico e a segurança" e entende que o seu desenvolvimento é prioritário ante ao objetivo de manter as vantagens competitivas norte-americanas (THE UNITED STATES OF AMERICA, 2017, p. 20 - tradução nossa), bem

como proteger os valores democráticos que, segundo o documento, norteiam os Estados Unidos.

Em 2020, Eric Schmidt, ex-CEO e presidente do Google/Alphabet, e também presidente da Comissão de Segurança Nacional em Inteligência Artificial, através do artigo intitulado “Eu liderava o Google. O Vale do Silício pode perder para a China” faz alusão aos riscos à segurança nacional e a estabilidade global decorrentes de uma não resposta ao engajamento chinês no desenvolvimento de Inteligência Artificial e a perda norte-americana da liderança no campo. De forma que o governo norte-americano deveria agir em prol da manutenção da competitividade dos Estados Unidos no tocante às tecnologias tidas como emergentes e de grande importância estratégica. Schmidt (2020) aponta, portanto, para a necessidade de um estreitamento das parcerias entre o governo dos Estados Unidos e as *Big Techs* norte-americanas como estratégia para enfrentar a concorrência e os riscos vindos da China.

Já em 2021, Schmidt através do artigo “A revolução da IA e a competição estratégica com a China” reafirma a China como um país que embora parceiro também é um competidor tecnológico. Segundo ele, a China

> é organizada, repleta de recursos e decidida a vencer esta competição tecnológica e reformular a ordem global para servir a seus próprios e estritos interesses. A IA e outras tecnologias emergentes são centrais para os esforços chineses de ampliar sua influência global, ultrapassar o poder econômico e militar dos EUA e isolar sua estabilidade doméstica. A China vem executando um plano sistemático centralmente direcionado para extrair conhecimento de IA do exterior por meio de espionagem, aquisição de talentos, transferência de tecnologia e investimentos (SCHMIDT, 2021, p. 1).

Para Schmidt (2021), a Inteligência Artificial, no território chinês, é utilizada de forma perturbadora para as sociedades que valorizam liberdade individuais e direitos humanos. Mas mais que isso, o padrão chinês de utilização da Inteligência Artificial estaria sendo exportado para outros países como ferramenta de repressão, vigilância e controle social de cidadãos. Segundo Schmidt, os financiamentos chineses de suntuosos projetos de infraestrutura digital pelo mundo, não buscariam somente “estabelecer parâmetros globais que refletem valores autoritários. Sua tecnologia está servindo para facilitar o controle social e reprimir dissidências” (SCHMIDT, 2021). Schmidt afirma que

> o crescimento acelerado e o foco em controle social da China estão tornando o modelo tecno-autoritário do país atraente para governos autocráticos e é tentador para democracias frágeis e países em desenvolvimento. Há muito trabalho a ser feito para garantir que os EUA e o mundo democrático possam combinar tecnologia economicamente viável com diplomacia, auxílio externo e cooperação na área de segurança para competir com o autoritarismo digital exportado da China (SCHMIDT, 2021, tradução nossa).

Ao longo do artigo, Schmidt (2021) acentua a importância da cooperação internacional no tocante aos assuntos digitais entre países que defendem os mesmos valores democráticos, evoca a necessidade da construção de organismos internacionais que atuem em prol de melhorar a cooperação no desenvolvimento de parâmetros, infraestrutura de telecomunicações, biotecnologia e cadeias de fornecimento. Existindo a necessidade, para ele, de se desenvolver e operacionalizar padrões e normas de apoio a valores democráticos e ao desenvolvimento de tecnologias seguras, estáveis e confiáveis. Medidas que requerem um trabalho conjunto através de parcerias entre governos, setor privado e a academia, parceria essa que ele chama de "uma vantagem assimétrica chave que os Estados Unidos e o mundo democrático têm sobre nossos competidores" (SCHMIDT, 2021)

A despeito de possíveis interesses oriundos de sua ligação com o setor privado e como suas recomendações acabariam por direcionar um grande montante de capital para as empresas privadas, as afirmações de Schmidt convergem com a importância conferida ao tema pelas Estratégia Nacional de Segurança (NSS, na sigla em inglês) de 2017, 2021 (ínterim) e 2022. O NSS-2017 na sua página 19 traz que os Estados Unidos se basearão na mesma "engenhosidade que lançou indústrias, criou empregos e melhorou a qualidade de vida no país e no exterior". Para manter sua vantagem competitiva, os Estados Unidos entendem ser necessário priorizar tecnologias como ciência de dados, criptografia, tecnologias autônomas, edição genética, novos materiais, nanotecnologia, tecnologias avançadas de computação e Inteligência Artificial de modo a salvaguardar o crescimento econômico e a segurança nacional. O documento faz clara menção à necessidade de incentivar os cientistas do governo, da academia e do setor privado a alcançarem avanços em todos os espectros.

Mais a frente, nas suas páginas 34 e 35, o NSS-2017 traz claro aviso que os riscos à segurança nacional dos Estados Unidos aumentarão à medida que os concorrentes integrarem as informações derivadas de fontes pessoais e comerciais a recursos analíticos de dados baseados em Inteligência Artificial (IA) e aprendizado de máquina. O documento cita nominalmente a China como exemplo de quem se vale da combinação de dados e Inteligência Artificial e reforça a importância do setor privado dos Estados Unidos ao afirmar o interesse das companhias norte-americanas "em apoiar e ampliar as vozes que defendem a tolerância, a abertura e a liberdade."

O NSS-2021, de caráter ínterim, formulado no primeiro ano do governo Biden, traz que as principais potências do mundo correm para desenvolver e implantar tecnologias emergentes, como inteligência artificial e computação quântica, que "podem moldar tudo, desde o equilíbrio econômico e militar entre os estados até o futuro do trabalho, riqueza e desigualdade dentro deles." O documento afirma que "a infraestrutura de telecomunicações de próxima geração (5G) preparará o terreno para grandes avanços no comércio e no acesso à informação." Mas as consequências da revolução tecnológica permanecem incertas. Segundo o NSS-2021 (p. 8-9),

> as tecnologias emergentes permanecem amplamente desgovernadas por leis ou normas destinadas a centrar direitos e valores democráticos, fomentar a cooperação, estabelecer proteções contra uso indevido ou ação maligna, e reduzir a incerteza e gerenciar o risco que a competição levará ao conflito. Os Estados Unidos devem reinvestir na manutenção de nosso conhecimento científico e tecnologia e mais uma vez liderar, trabalhando ao lado de nossos parceiros para estabelecer as novas regras e práticas que nos permitirão aproveitar as oportunidades que os avanços da tecnologia no presente.

Em uma consonância já esperada com o documento publicado em 2021, o NSS-2022 reforça textualmente a importância fundamental da tecnologia para a competição geopolítica de momento e também para o futuro da economia, democracia e segurança dos Estados Unidos. Em um cenário prospectado como de grandes mudanças oriundas do surgimento de tecnologias críticas, como as são a Inteligência Artificial e o aprendizado de máquina, a manutenção da liderança tecnológica global dos Estados Unidos, juntamente com seus aliados tecnológicos, é, mais do que nunca, tida como fundamental.

Segundo o documento estratégico, os Estados Unidos já está a reunir atores com ideias e valores semelhantes para promover um "ecossistema de tecnologia internacional que proteja a integridade do desenvolvimento de padrões internacionais e promova o livre fluxo de dados e ideias com confiança, protegendo nossa segurança, privacidade e direitos humanos" (THE UNITED STATES OF AMERICA, 2022, p. 32 - tradução nossa). O NSS-2022 ainda traz que os Estados Unidos, juntamente com seus aliados, buscam fechar lacunas regulatórias e legais, fortalecendo a segurança da cadeia de suprimentos e aprimorando a cooperação em privacidade, compartilhamento de dados e troca. De forma a garantir que os concorrentes estratégicos não possam explorar tecnologias fundamentais dos Estados Unidos ou de seus aliados, seus *know-hows* ou dados para minar a segurança norte-americana ou aliada.

Por último, citamos o compromisso expressado no documento quanto ao combate "a exploração de dados norte-americanos sensíveis e uso ilegítimo de tecnología,

incluindo spyware comercial [*software* que coleta de dados de forma não consentida] e tecnologia de vigilância, e vamos nos posicionar contra o autoritarismo digital." Com vistas a salvaguardar a segurança e os demais interesses norte-americanos, o documento afirma a necessidade de se trabalhar com uma ampla gama de parceiros para promover a resiliência da infraestrutura de rede 5G e outras comunicações tecnologicamente avançadas, conduzindo a promoção da diversidade de fornecedores e protegendo as cadeias de suprimentos. De modo que

> esses investimentos não podem ser feitos apenas em países ricos; também devemos nos concentrar em fornecer serviços de alta qualidade para a infraestrutura digital em países de renda baixa e média, eliminando divisões digitais, enfatizando o acesso entre grupos marginalizados. Para garantir que esses investimentos apoiem resultados tecnológicos, faremos parceria com a indústria e os governos na formação de padrões que garantem a qualidade, a segurança do consumidor e a interoperabilidade global, e para promover o processo de padrões aberto e transparente que permitiu inovação, crescimento e interconectividade por décadas. E em tudo o que fizermos, nos esforçaremos para garantir que a tecnologia apoia, e não prejudica, a democracia, e é desenvolvida, implantada e governada em acordo com os direitos humanos.

A necessidade de trabalhar em conjunto entre o governo dos Estados Unidos e as companhias norte-americanas também é expressa na Ciberestratégia Nacional, onde o governo dos Estados Unidos afirma que trabalhará com o setor privado para facilitar a evolução e a segurança do 5G. Por evolução e segurança da infraestrutura 5G, entenda-se controle sobre os dados por ela circulantes. Tanto pelo empenho dos adversários em se valerem deles em benefício próprio, quanto pela necessidade de se manter em vantagem no tocante ao ciberpoder global. Portanto, a Inteligência Artificial pode ser compreendida como o "fim último", a infraestrutura do 5G como o meio e os dados como o grande recurso em disputa.

Ao se pensar em dados como recurso, talvez nenhuma frase venha tão rápido à mente e seja tão adequada quanto a cunhada pelo matemático britânico Clive Humby, em 2006: "dados são o novo petróleo". Na palestra dada pelo cientista de dados em uma conferência da Associação de Anunciantes Nacionais (*Association of National Advertisers* – ANA, na sigla em inglês) a ideia central era demonstrar que assim como o petróleo, o verdadeiro valor dos dados advém da capacidade de refiná-los às aplicações mercadológicas (HUMBY *apud* PALMER, 2006). Nenhum aparato tecnológico sugere ser tão eficaz e adequado ao objetivo do refino de dados como o uso da Inteligência Artificial e do aprendizado de máquina, entretanto, como visto, as aplicações que disso decorrem não se restringem ao viés mercadológico – em semelhança com o que se deu ao próprio petróleo.

3.3 Dados – recursos estratégicos

Desde abril de 1855, quando Benjamin Silliman Jr, então professor de química da Universidade de Yale, divulgou seu relatório sobre as propriedades do petróleo aos investidores que o contrataram, o petróleo adquiriu grande importância em decorrência de suas aplicabilidades após o refino. Se no começo da exploração petrolífera o refino gerou subprodutos como o querosene e lubrificantes de máquinas industriais que impactaram majoritariamente o comércio de iluminantes, com a criação de motores de combustão interna e a descoberta da utilidade dos subprodutos petrolíferos para tal invenção, o petróleo adquiriu uma importância maior dentro da dinâmica capitalista, mas também uma importância militar (YERGIN, 1993).

Com o surgimento da iluminação elétrica, os derivados do petróleo perderam importância no que fora seu primeiro mercado, entretanto com a criação do motor de combustão interna sua importância se tornou ainda maior. A descoberta da existência de abundantes fontes de petróleo no mundo, o desenvolvimento de carros propulsionados por motores de combustão e sua posterior produção em série e difusão tornaram o petróleo em artigo de grande importância comercial. Porém, mais do que isso, a utilização dos novos motores propulsionados à óleo em outros meios de transporte mudaram a própria dinâmica militar e por consequência a dinâmica geopolítica até então existente (YERGIN, 1993).

É bem verdade que o querosene foi a alternativa encontrada pelos nortenhos a supressão imposta pelos sulistas ao envio de canfeno durante a Guerra da Secessão norte-americana, tendo isso um importante papel na difusão, aumento, uso e exportação do petróleo e seus derivados (GARCEZ, 2020). Mas é no final do século XIX e começo do século XX, em meio a ascendente disputa naval entre Alemanha e Inglaterra, que o petróleo passa a ter status de recurso estratégico dentro dos assuntos de Estado.

Em meio ao acirramento das disputas no Sistema Interestatal Capitalista no final do século XIX e começo do século XX, a recém-unificada Alemanha demandava que novos espaços dotados de recursos naturais fossem conquistados ou que a influência alemã fosse assegurada sobre eles. Segundo Fernandes (2016), a existência de uma única rota de navegação, pelo Mar do Norte, a garantir acesso ao Oceano e a existência de poucos locais no Mar do Norte com capacidade de navegação dos navios mercantes que destinavam-se a seu território – sob riscos de bloqueios pelos rivais da Alemanha,

constituíam-se enquanto preocupação das pretensões alemãs de ascensão na hierarquia global. Essas pretensões ainda necessitavam lidar com os riscos oriundo da supremacia naval inglesa em alto-mar, a armada naval mais poderosa da época, e também com o fato que muitas das possessões ultramarinas desejadas pelo Estado alemão estarem sob o domínio do império inglês.

Diante dessas condicionalidades, a Alemanha passou então a investir na tentativa da construção de uma armada capaz de rivalizar com o poder naval britânico, esforços que incluíram testes de navios e submarinos movidos à combustão de derivados do petróleo – o que incrementava a velocidade e aceleração dos veículos, bem como aumentava a distância que poderia ser percorrida até o reabastecimento, além de reduzir o número de pessoas envolvidas no reabastecimento e o espaço demandado para armazenar o combustível, trazia também a possibilidade de reabastecimento em alto mar. Fatores que diminuíam os custos logísticos e davam um grande vantagem tática no combate (GARCEZ, 2020).

Embora os alemães tenham sido pioneiros nas pesquisas para construção de navios propulsionados por motores de combustão a óleo, devido à falta de acesso seguro a fontes de petróleo e dependência da importação junto a *Standard Oil Company* – empresa norte-americana, eles mantiveram seus maiores e principais navios de guerra movidos unicamente a carvão (GARCEZ, 2020). Reconhecendo a importância do amplo e resguardado acesso ao petróleo, o governo alemão buscou formas de assegurar suas demandas. Um dos projetos expoentes dessa busca foi a ferrovia Berlim-Bagdá, que possibilitaria acesso às jazidas petrolíferas no Oriente Médio, em especial no Golfo Pérsico. Uma vez concluída a ferrovia, cuja construção fora firmada em 1899, a Alemanha incrementaria suas capacidades industriais e militares.

Em resposta à construção da armada alemã, os ingleses iniciaram o processo de uso do óleo como combustível da sua armada. Em 1905, o Reino Unido construiu os primeiros *destroyers* propelidos somente à óleo e, ainda no mesmo ano, todos os principais navios passaram a possuir um sistema de combustível auxiliar movido à óleo (YERGIN, 1993). Mas somente com a crise de Agadir – no Marrocos, quando a Alemanha enviou a canhoneira *Phanter* ao porto estratégico de Agadir em uma resposta (com tom de ameaça) a possibilidade de a França anexar o Marrocos ao seu território, depois que tropas francesas intervieram em uma revolta popular no país africano, é que os ingleses superaram as discordâncias internas e a adotaram a combustão à óleo para toda a sua armada naval (YERGIN, 1993).

Como resultado dessa mudança, a necessidade de suprir a demanda energética da armada britânica passou a ser uma prioridade estratégica, se fazendo necessário encontrar fontes de petróleo suficientes e oferecer-lhes segurança. Uma das ações estratégicas foi a aquisição pelo governo britânico de 51% das ações da Anglo-Persian, em 1914, e a tomada da companhia de distribuição British Petroleum (no início da Primeira Guerra), que anteriormente era controlada pelo Deutsche Bank, para incorporá-la à Anglo-Persian. Assim, através da fusão, formou-se uma empresa sob controle do Estado inglês capaz de ser autossuficiente e integrada no mercado petrolífero (YERGIN, 1993).

Nessa mesma época, os ingleses negociaram pela permissão para extração de petróleo em Maidan-i-Naphtun, território persa perto da fronteira com a Mesopotâmia. Também estabeleceram acordos pela exploração no Kuwait. Assegurando acesso a duas áreas abundantes em petróleo, bem como através de sua influência na importante região mesopotâmica buscar atrapalhar as pretensões germânicas que se consolidariam com a ferrovia Berlim-Bagdá.

Como Visentini (2012, p. 27) expressa:

> o imperialismo alemão tinha como prioridade a expansão para o leste da Europa e para o Oriente Médio, onde se encontravam os recursos naturais necessários a seu crescimento industrial. A aliança com a Áustria-Hungria, a ideologia pangermanista, os investimentos no petróleo turco e a construção da ferrovia Berlim-Bagdá evidenciavam esta orientação. [...] Já a Grã-Bretanha, que era o maior e mais populoso império na época, desejava destruir a capacidade comercial e naval alemã, apoderar-se do império Turco e dividir as colônias alemãs com a França (VISENTINI, 2012, p. 27).

Como sintetiza Garcez (2020, p. 63), “com essas mudanças, o governo e empresas inglesas puderam continuar seu plano de busca por terras com abundantes reservas de petróleo. Essas terras encontradas seriam alvos de disputas que transformariam suas histórias”. Essa corrida em busca do recurso estratégico é bem nítida no transcorrer da Primeira Guerra, onde, inclusive, o surgimento do avião para fins militares e do tanque de guerra conferiram importância ainda maior ao petróleo – importância que impactou as políticas estatais energéticas posteriores ao conflito (YERGIN, 1993).

No transcorrer do conflito, por ação rival, a Alemanha se viu impossibilitada de acessar as fontes de petróleo turco que pretendia, bem como incorreu em insucesso ao tentar conseguir o recurso avançando sobre território da Romênia, após a autodestruição romena da infraestrutura de exploração. Além de, mesmo após assinar com a Rússia o tratado de Brest-Litovsk para acessar o petróleo da região de Baku, ter tido que lidar com a oposição da Comuna Bolchevique de Baku – o que possibilitou a atuação inglesa na

região e impossibilitou as intenções alemãs de conseguir acessar o petróleo da região em um momento crítico de escassez (YERGIN, 1993).

A Inglaterra, por sua vez, embora tenha conseguido manter as suas fontes de petróleo seguras da intervenção rival, teve problemas logísticos para acessar o recurso estratégico. Seu abastecimento se dava principalmente pelas jazidas do Golfo do México e de Bornéu – que eram operadas pela Royal-Dutch Shell e pela Standard Oil – e também pelas jazidas da Pérsia, que a Anglo-Persian Oil operava. Além da existente limitada capacidade de transportar o combustível, a qualidade e a quantidade do produto refinado do petróleo persa foi um problema para os ingleses (BROWN, 2003). Segundo Brown (2003, p. 157, tradução nossa), "a falta de navios foi o principal obstáculo para abastecimento da marinha com o petróleo, não uma escassez de petróleo em si. À medida que a guerra se aproximava do fim, a Marinha era dependente do petróleo americano"

Embora o carvão tenha se mantido como recurso de grande importância no transcorrer da Primeira Guerra Mundial, as grandes potências passaram a considerar o petróleo como recurso de valor estratégico, se enveredando em uma intensa disputa para garantir acesso seguro e irrestrito a territórios com abundância petrolífera, bem como a buscar as melhores formas de utilizá-lo para a indústria, o comércio e para a guerra.

A analogia proposta por Clive Humby, comparando dados ao petróleo, permite que se olhe para o passado e se perceba uma repetição no tocante a tecnologia 5G com relação a forte conexão entre Estados e Capital na busca das grandes potências por acesso seguro e irrestrito a territórios com abundância do novo recurso estratégico. De modo que, se por um lado tem-se a inovação da ciberterritorialidade, com múltiplos territórios a se transpassarem com seus dados abundantes dotados de importância estratégica, por outro a construção discursiva do conflito entre Estados Unidos e China recorre ao tradicional argumento do dilema de segurança.

John Herz, em seu texto seminal "Internacionalismo idealista e o dilema da segurança", publicado em 1950, ao olhar para o mundo bipolar sob a "benção" da bomba atômica, expressa que a situação é "apenas a manifestação extrema de um dilema com o qual as sociedades humanas tiveram que lutar desde o início da história" (HERZ, 1950, 157, tradução nossa). Para Herz (1950), a existência de uma sociedade anárquica irremediavelmente resulta no que pode ser chamado de "dilema de segurança" de homens, grupos ou seus líderes. Assim,

> grupos ou indivíduos que vivem em tal constelação devem estar, e geralmente estão, preocupados com sua segurança de serem atacados, subjugados, dominados ou aniquilados por outros grupos e indivíduos. Esforçando-se para

> obter segurança de tal ataque, eles são levados a adquirir cada vez mais poder para escapar do impacto do poder dos outros. Isso, por sua vez, torna os outros mais inseguros e os obriga a se preparar para o pior. Uma vez que ninguém jamais pode se sentir totalmente seguro em tal mundo de unidades concorrentes, a competição pelo poder segue, e o círculo vicioso de segurança e acúmulo de poder inicia sua marcha (HERZ, 1950, 157, tradução nossa).

De modo que para o autor, se o homem é dotado de uma natureza pacífica que tende à cooperação, ou dominador e agressivo, não é a questão. Seu olhar não está voltado para o ser biológico ou antropológico, mas para o ser social. Em sua análise, a luta pela "segurança é elevada do nível individual ou do grupo inferior para o nível do grupo superior" (HERZ, 1950, 157, tradução nossa). Como resultado,

> famílias e tribos podem superar o jogo de poder em suas relações internas para enfrentar outras famílias ou tribos; grupos maiores podem superá-lo para enfrentar outras classes unidas; nações inteiras podem compor seus conflitos internos para enfrentar outras nações. Mas, em última análise, em algum lugar, os conflitos causados pelo dilema de segurança estão prestes a surgir entre as unidades políticas de poder (HERZ, 1950, 158, tradução nossa).

Assim, o elemento da segurança, enquanto fator que determina as ações dos atores, é capaz de levar que cidadãos renunciem a direitos, que empresas atuem em conjunto com o governo em circunstâncias menos vantajosas no curto prazo e que Estados atuem no tabuleiro global de forma a garantirem sua própria segurança, estando atentos às dinâmicas de poder. Mearsheimer (2001, p. 34, tradução nossa) aponta que:

> os estados dedicam muita atenção à forma como o poder é distribuído entre eles e eles fazem um esforço notável para maximizar sua parcela de poder mundial. Procuram, especificamente, oportunidades para alterar o equilíbrio de poder, adquirindo poder adicional às custas de rivais potenciais. Os Estados utilizam vários meios - econômicos, diplomáticos e militares - para alterarem o equilíbrio de poder a seu favor, mesmo que ao fazê-lo provoquem a desconfiança ou mesmo a hostilidade dos outros estados. Como os ganhos de poder de um estado são a perda de outro estado, as grandes potências tendem a possuir uma mentalidade de soma zero ao lidarem umas com as outras.

De acordo com as lentes do realismo ofensivo desenvolvido por Mearsheimer (2001), as grandes potências atuam de forma ofensiva, no sentido de acumular o máximo possível de poder relativo. Isso se deve ao fato que, para o autor, os estados "entendem" que estão, quase sempre, em uma posição melhor quando têm mais poder. Porém, para ele, os estados não buscam acréscimos absolutos de poder, eles ponderam os ganhos que seus potenciais rivais possam vir a ter e abdicam de acrescer poder se o saldo for mais benéfico a outro estado. Somente em caso de conquista do domínio sobre o sistema, um estado se transforma em uma potência situacionista. Conforme as palavras do autor, "todos os estados são influenciados por essa lógica, o que significa que não só procuram

oportunidades para se aproveitarem uns dos outros, mas também se esforçam por assegurar que outros estados não se aproveitam deles" (MEARSHEIMER, 2001, p. 35, tradução nossa).

Nessa ótica, o sistema que rege o mundo é, portanto, marcado por estados preocupados tanto com a defesa quanto com o ataque. Essa busca incessante de maximizar os seus próprios ganhos e minimizar os ganhos dos rivais em potenciais resulta "inexoravelmente em um mundo de permanente competição de segurança, no qual os estados estão dispostos a mentir, ludibriar e usar a força bruta, se isso os ajudar a ganhar superioridade sobre os seus rivais" (MEARSHEIMER, 2001, p. 36, tradução nossa).

Dada a incapacidade de prever as reais intenções dos demais estados, os Estados Unidos não podem ter certeza se a China ao acrescentar poder apenas o faz pensando em fins pacíficos e no seu desenvolvimento econômico, como frequentemente discursa seu presidente Xi Jinping. Além disso, as intenções do hoje podem não serem as mesmas do futuro, um estado pode, portanto, acrescer poder pensando em melhorar sua capacidade de defesa e no futuro passar a intentar o ataque sem que o mesmo fosse uma possibilidade pensada no início. Se em 16 de outubro de 2022, no 20º Congresso do Partido Comunista Chinês, o presidente Xi Jinping discursou em nome de uma China pacifista, que

> persegue uma visão de governança global com crescimento compartilhado por meio de discussão e colaboração. A China defende o verdadeiro multilateralismo, promove maior democracia nas relações internacionais e trabalha para tornar a governança global mais justa e equitativa. A China é firme em salvaguardar o sistema internacional com as Nações Unidas em seu núcleo, a ordem internacional sustentada pelo direito internacional e as normas básicas que regem as relações internacionais com base nos propósitos e princípios da Carta da ONU. Opõe-se a todas as formas de unilateralismo e à formação de blocos e grupos exclusivos dirigidos contra determinados países. (XI apud DE WEI, 2022, p. 39)

Não há certezas, entretanto, que no futuro não se guiará pela máxima de Norbert Elias, que, nesse sistema, "quem não sobe, cai." Afinal, conforme aponta Mearsheimer (2018), as grandes potências raramente estão em uma posição para prosseguir uma política externa liberal em grande escala. A existência de duas, ou mais, grandes potências no mundo acaba por forçar que prestem muita atenção à sua posição no equilíbrio global de poder e a agir de acordo com os ditames do realismo. A natureza anárquica do sistema faz com que grandes potências liberais regularmente falem como liberais e ajam como realistas.

Porém, a ascensão tecnológica de uma rival como a China se mostra como um momento crítico. Seja porque o progresso técnico tende a resultar em ganhos econômicos

e esses, na leitura realista que rege as respostas norte-americanas, pode se transformar em acréscimos de capacidades militares. Ou porque grandes populações são vistas pelos realistas como potenciais grandes e poderosos exércitos. A esse segundo elemento, em um cenário de veículos não tripulados atuando autonomamente nos conflitos, se junta o fato da quantidade de dados a serem produzidos por uma população do tamanho da chinesa e como as ferramentas de Inteligência Artificial e aprendizado de máquina tendem a evoluir mais rápido quanto mais dados disponíveis existirem, conferiria uma grande vantagem no desenvolvimento das novas tecnologias militares.

Ademais, a pulverização da vantagem global norte-americana no tocante ao acesso aos dados dos usuários em outros países resultaria em um grande decréscimo de poder como um todo ao longo do tempo, seja em decorrência da grande presença de componentes com tecnologia chinesa, ou pela difusão da visão chinesa de governança sobre a Internet – como restrições ao acesso a ciberterritórios de origem estrangeira e também a imposição de maior controle governamental sobre os usuários locais.

Como Fiori observa, a natureza do Sistema Interestatal Capitalista é expansionista e o poder, por ser fluxo, demanda que seja exercido. Assim,

> nesse tipo de sistema, portanto, todos os poderes soberanos são e serão sempre expansivos, se propondo em última instância à conquista de um poder cada vez mais global, até onde alcancem seus recursos e suas possibilidades e, independentemente de quem os controle, em distintos momentos de sua expansão (FIORI, 2010, p. 134)

Através das suas políticas de incentivo às empresas de tecnologia, influência para a abertura comercial de outros países, estipulações de padrões tecnológicos, leis de proteção à propriedade intelectual e diversas outras medidas político-econômicas, os Estados Unidos se viram capazes de atuar nos mais distintos locais do mundo através do seu ciberpoder, ofertando, ainda, alta rentabilidade às suas *Big Techs*. Se valendo, para tal, do acesso privilegiado proporcionado pela união característica do Sistema Interestatal Capitalista entre poder e capital.

Ante a isso, pender o balanço de poder para si, no tocante a difusão da tecnologia 5G, é de fundamental importância para os Estados Unidos de acordo com os documentos produzidos nos últimos anos. Ao se pensar (1) nas características disruptivas e seus possíveis impactos nas dinâmicas do poder global, (2) bem como o pioneirismo norte-americano nas TICs foi determinante para seu progresso econômico, (3) além do acréscimo e exercício de poder militar nas últimas décadas, compreende-se a leitura norte-americana que ter perdas de poder relativo no setor para a China impactaria o poder norte-

americano em todas as suas dimensões – dado seus impactos nos avanços tecnológicos comerciais, industriais e militares. O que é algo dissonante da visão realista adotada pelos Estados Unidos quanto ao caso.

4 – Estados Unidos vs Huawei

Desde 2019, a Huawei sofre impactantes sanções por parte do governo estadunidense sob a alegação de espionagem. As sanções impactam os negócios da gigante companhia chinesa, que se viu impedida de negociar livremente com empresas como Intel, Google, Qualcomm e Microsoft. Posteriormente, em novembro de 2020, o comércio de ativos financeiros envolvendo a empresa chinesa foi proibido e criminalizado. Tal proibição alcança norte-americanos, pessoas dentro dos EUA, empresas nacionais ou empresas estrangeiras com filiais nos EUA.

Como resultado, o constante e acelerado crescimento que a Huawei apresentava nos anos anteriores deu lugar a um crescimento mais modesto em 2020 e, em especial, 2021. Esse crescimento, porém, também esteve muito ligado à capacidade do próprio mercado chinês em absorver a oferta de equipamentos da empresa. Esse fenômeno contrasta com a tendência de mercado esperada, dada ao crescimento exponencial que a Huawei tinha em seu setor de produção de Smartphones e também dada a importância da tecnologia 5G para o novo modo de produção que irrompe.

Cabe salientar que acusações desse tipo não são novas. A Huawei já sofreu acusações de espionagem industrial pela Motorola e pela Cisco, gigantes do ramo de telecomunicações (SEGAL, 2016). Outro caso se deu no ano de 2012, quando a Huawei foi o centro de investigações conduzidas por agências de inteligência dos EUA que não encontraram evidências de espionagem ativa, mas que desaconselharam o emprego de equipamentos de redes da Huawei pela existência de vulnerabilidades nos mesmos que poderiam trazer sérios riscos. Um relatório do Congresso dos EUA, sobre o mesmo caso, alertou contra a permissão para as empresas chinesas Huawei e ZTE fornecerem infraestrutura crítica de telecomunicações.

Bill Plummer – porta-voz da Huawei nos EUA – alegou que: “A Huawei é uma multinacional independente de US$32 bilhões que não colocaria em risco seu sucesso ou a integridade das redes de seus clientes para qualquer governo ou terceiro.” (MENN, 2012). Desde então, ambas as empresas foram banidas de fato da infraestrutura da Internet norte-americana pelas operadoras dos EUA. Independentemente disso, eles continuaram a vender dispositivos de usuário (como aparelhos, roteadores ou tablets) para clientes nos

Estados Unidos, ao mesmo tempo em que fortaleceram relacionamentos com fornecedores como Intel, Microsoft e Qualcomm.

À medida que as tensões entre EUA e China se intensificaram e ante o advento da incorporação maciça do 5G na infraestrutura da Internet, o governo Trump começou a direcionar sua atenção para os fornecedores chineses de redes de telecomunicação. Em fevereiro de 2018, o diretor do FBI, Chris Wray, alertou quanto à compra de telefones celulares da Huawei e ZTE, alegando a possibilidade de serem conduzidas 'espionagens não detectadas' através deles.

> Estamos profundamente preocupados com os riscos de permitir que qualquer empresa ou entidade que esteja em dívida com governos estrangeiros que não compartilhem de nossos valores ganhe posições de poder dentro de nossas redes de telecomunicações [...] Isso fornece a capacidade de exercer pressão ou controle sobre nossa infraestrutura de telecomunicações", disse Wray. "Ele fornece a capacidade de modificar ou roubar informações de forma maliciosa. E fornece a capacidade de realizar espionagem não detectada (WRAY apud SALINAS, 2018, tradução nossa).

Em agosto de 2018, o governo dos EUA promulgou a Lei de Autorização de Defesa Nacional John S. McCain para o ano fiscal de 2019 (a NDAA – sigla em inglês ou 'McCain Act'). Além da autorização dos gastos militares anuais dos EUA, na Seção 889 da lei há compromissos amplos para proibir a compra federal de equipamentos de telecomunicações e vídeo vigilância. Com isso, ZTE, Huawei, Hytera Communications, Hangzhou Hikvision e Dahua foram atingidas pela proibição.

Em dezembro de 2018, Meng Wanzhou, diretora financeira da Huawei (e filha do fundador da empresa), foi detida no aeroporto de Vancouver por supostamente fraudar o banco HSBC em relação à afiliada iraniana da Huawei, a Skycom. Como consequência, ela foi colocada em prisão domiciliar por quase três anos (CORERA, 2021).

Durante a administração Trump, intensificaram-se as medidas com o objetivo de restringir o 5G chinês. Embora houvesse movimentação interna política nos EUA em prol do estabelecimento de proibições contra a Huawei e a ZTE e suas presenças no estabelecimento da tecnologia 5G em andamento (LEE-MAKIYAMA, 2021), somente em maio de 2019 o governo norte-americano deixou de se abster e anunciou sua primeira série de sanções contra o 5G desenvolvido pelos chineses. Uma Ordem Executiva declarou emergência nacional e impôs oficialmente sanções à utilização de equipamentos de telecomunicações produzidos por empresas chinesas por representarem um "risco à segurança nacional".

Sanções não são mecanismos novos. Ao longo da história, é possível verificar o uso de mecanismos similares com fins parecidos, ou seja, buscando limitar o acesso de nações inimigas a determinados mercados (DREZNER, 1999). Entretanto, na contemporaneidade, é possível ver tipos de regulamentações que não só visam legitimar sua aplicação, como também a tornar mais eficiente. Contemporaneamente, os novos mecanismos de sanções também se valem da assimetria financeira e da posição ocupada pelo país no Sistema Internacional.

Drezner (1999) destaca importância do tema das sanções econômicas ao chamar atenção para o fato que o uso de tal ferramenta coercitiva aumentava desde o fim da Guerra-Fria, destacando os EUA como o ator internacional a mais utilizar tal recurso. O uso de sanções é tradicionalmente tido como um meio não violento de forçar outro agente econômico a adequar sua conduta aos anseios do sancionador, de modo que é socialmente mais aceitável que o conflito bélico (TORRES, 2018). Entretanto, é incorreto pressupor que resulta em efeitos menos destrutivos.

As sanções econômicas cujos efeitos se dão também no setor financeiro adquiriram nova roupagem a partir do ataque de 11 de setembro de 2001. Após os atentados, os Estados Unidos criaram um aparato coercitivo com o uso aprimorado de sua centralidade no sistema financeiro internacional. A montagem de tal aparato contou com o apoio imprescindível dos bancos e do SWIFT – rede de troca de informações dos pagamentos do sistema financeiro internacional (TORRES, 2018). Como Torres (2018) traz, o exemplo do SWIFT é relevante para que se entenda a extensão do poder americano sobre o Sistema Financeiro Internacional.

O SWIFT se trata de uma empresa estabelecida e localizada na Bélgica, sendo, portanto, sujeita às leis belgas e da Comunidade Europeia, não existindo obrigação formal de seguir as determinações dos Estados Unidos. “Mesmo assim, o engajamento dessa rede à ‘Guerra contra o Terrorismo’ não precisou de muito tempo nem de muito convencimento” (TORRES, 2018, p. 4). A partir desse momento, as instituições financeiras em todo o mundo que fossem veículo de transações atribuídas ao terrorismo e outros ilícitos passaram a ser consideradas e tratadas como cúmplices de tais atividades, o que inclui o risco de sofrerem medidas punitivas.

Torres (2018) explica que o sistema financeiro opera em rede, logo qualquer problema reputacional implica na imediata exclusão pelos seus pares e pelos investidores em decorrência do medo de “contágio” ou de perda patrimonial. Isso leva à sua eliminação como unidade econômica em muito pouco tempo. Como consequência,

bancos por todo o mundo passaram a cooperar com os Estados Unidos na imposição de sanções, já que estavam sob risco de serem excluídos do Sistema Financeiro Internacional pelos Estados Unidos.

Essa condição privilegiada norte-americana decorre de um longo processo histórico, no qual uma série de medidas político-econômicas impuseram a centralidade da sua moeda ao resto do mundo. Como Torres (2022) destaca, seu início está relacionado à 1ª Guerra Mundial, com a criação do *Federal Reserve* (FED, na sigla em inglês) e do mercado de câmbio de Nova Iorque, bem como de uma elevada dívida de guerra em dólares das principais potências europeias para com os Estados Unidos. Esses elementos conduziram a moeda norte-americana ao centro das finanças internacionais, retirando-a da sua, até então, condição periférica.

Com o advento da Segunda Guerra Mundial e posteriormente a ela com o Acordo de Bretton Woods de 1944, os norte-americanos deram um novo passo rumo à centralidade do dólar no Sistema Financeiro Internacional. Strange (1994) aponta o sistema de Bretton Woods como resultado da posição assimétrica ocupada pelos EUA que possibilitou que tais normas fossem impostas aos europeus "mornos" e aos países do terceiro mundo. Sendo no Acordo de Bretton Woods que o padrão ouro-dólar foi instituído.

No início da década de 1970, através de uma decisão unilateral, os Estados Unidos romperam com as condições negociadas em Bretton Woods, com isso deixou de existir a conversibilidade compulsória do dólar em ouro a uma taxa fixa. O Dólar se tornou uma moeda plenamente fiduciária e com a intensificação da globalização financeira adquiriu uma centralidade quase absoluta nas transações internacionais. Segundo Torres (2022, p. 8), "alcançar essa posição singular não foi uma consequência imprevista de um processo de mercado, mas, em grande medida, o resultado de uma estratégia de poder perseguida pelo e*stablishment* dos EUA".

Como aponta Torres (2018), a partir da centralidade da sua moeda no Sistema Financeiro Internacional os EUA construíram uma arma de destruição em massa, porém não operada por soldados, e sim por altos funcionários do sistema financeiro juntamente com alguns agentes do Estado norte-americano. Seu alto nível de efetividade é descrito em Torres (2018, p. 38):

> Esse arranjo dá aos Estados Unidos um poder assimétrico entre as nações. Não se trata apenas de um "privilégio exorbitante" apontado na literatura e que lhe permite financiar automaticamente seus gastos. É mais do que isso. Significa também a capacidade de usar o poder de monopólio sobre o meio de pagamento internacional, detido pela sua moeda, para operar uma

> flexibilização negativa e forçada de um país alvo, de modo a isolá-lo do sistema financeiro internacional. O impacto dessa exclusão é semelhante ao de uma economia que sofre um bloqueio militar quase que absoluto.

Conforme Lapavitsas (2013), com o processo de globalização financeira e a liberalização da economia global, as empresas comerciais e industriais se envolveram cada vez mais em processos financeiros de forma independente, muitas vezes realizando transações no mercado financeiro por conta própria. “A financeirização das empresas industriais e comerciais afetou sua rentabilidade, organização interna e perspectivas de investimento. As empresas não financeiras tornaram-se relativamente mais distantes dos bancos e outras instituições financeiras” (LAPAVITSAS, 2013, p. 794, tradução nossa).

De modo que, em um cenário de globalização econômica, as atividades financeiras e comerciais são fundamentais para que as empresas e demais atores econômicos relevantes consigam administrar seus fluxos de caixa em dólar, devido ao papel de moeda de referência no sistema internacional. Essa obrigação decorre do fato que muitas das suas obrigações relevantes e recorrentes de pagamento serem denominadas em dólar, que, pelos riscos envolvidos, necessitam estar “casadas” (*hedgeadas*) com receitas futuras ou ativos, que também tenham por base essa mesma unidade. Portanto, os atores econômicos dotados de relevância necessitam garantir a posse e o acesso constante de uma soma de dólares igual ou superior à que os seus desembolsos requerem. Um insucesso nessa condição conduz a problemas econômicos graves e que podem resultar em extinção (falência). Como afirma Torres (2022, p. 6), “todas essas operações [que ocorrem em dólar] transitam, de alguma forma, no interior do sistema financeiro americano.”

Apesar da forma financeira das sanções desenvolvida no século XXI se mostrar sobremaneira eficiente, a forma comercial das sanções econômicas continua a ser usada e também se mostra eficaz em impactar economicamente e politicamente um alvo. Por esse recurso é possível impedir que um alvo tenha acesso a recursos dotados de importância estratégica, gerando graves problemas para que se lide com seus efeitos. De modo que a Huawei e suas subsidiárias se veem sob ambas as formas de sanções.

4.1 As sanções à Huawei

A partir da descrição e análise do conteúdo de alguns documentos publicados pelo Departamento do Tesouro dos Estados Unidos, este trabalho contará com um momento

para se debruçar na questão da legalidade das sanções econômicas através da relação entre poder, governo, finanças e tecnologia. O primeiro documento, intitulado *International Emergency Economic Powers* (IEEPA) foi publicado em 1977 e discorre sobre a execução de poderes do presidente frente a ameaças contra segurança nacional, política externa ou economia dos Estados Unidos. O IEEPA confere autoridade ao presidente dos Estados Unidos (ainda que sob declaração de emergência nacional) a partir da seção 1702 do documento, que permite que o presidente dos EUA prescreva:

(a) a investigação, regulação ou proibição de transações em moedas estrangeiras, transações de crédito ou pagamento para, através de ou entre instituições bancárias, a importação ou exportação de moeda ou ativos de qualquer pessoa, entidade ou instituição que esteja sob jurisdição dos Estados Unidos;

(b) investigação - e bloqueio durante o período de investigação -, regulação, anulação, prevenção ou proibição qualquer aquisição, uso, transferência, transporte, retirada, exportação ou importação, exercício de propriedade, de poder ou privilégio de qualquer propriedade de qualquer entidade que esteja sob jurisdição dos Estados Unidos;

(c) que caso os Estados Unidos estejam envolvidos em hostilidades armadas, autoridades poderão confiscar qualquer propriedade de qualquer pessoa ou entidade - sob jurisdição do país - de qualquer país estrangeiro ou organização estrangeira que planeje, autorize, ajude ou se engaje em atividades referentes à hostilidades. Os confiscos poderão ser guardados, administrados, liquidados, vendidos ou utilizados de qualquer forma que garanta a preservação dos interesses dos Estados Unidos.

Caso as regulamentações acima não sejam observadas, a seção garante uma pena civil e criminal; enquanto a primeira prevê uma multa de até US$250.000, a segunda prevê a fiança no valor de até US$1.000.000 e/ou a prisão de pessoas naturais dos Estados Unidos em até 20 anos.

O segundo documento, a Ordem Executiva (OE) 13873 de 15 de maio de 2019, tem como título *Securing the Information and Communications Technology and Services Supply Chain*. Nessa OE, o ex-presidente Donald Trump manifesta como uma ameaça extraordinária à segurança nacional a utilização de tecnologia de informação e comunicação, bem como de serviços a ela ligados, oriundos de adversários.

> Eu, DONALD J. TRUMP, Presidente dos Estados Unidos da América, [...] considero que a aquisição ou uso irrestrito nos Estados Unidos de tecnologia de informação e comunicação ou serviços projetados, desenvolvidos, fabricados ou fornecidos por pessoas pertencentes, controladas ou sujeitas à jurisdição ou direção de adversários estrangeiros aumenta a capacidade de adversários estrangeiros para criar e explorar vulnerabilidades em tecnologia

> ou serviços de informação e comunicação, com efeitos potencialmente catastróficos e, portanto, constitui uma ameaça incomum e extraordinária à segurança nacional, política externa e economia dos Estados Unidos. Essa ameaça existe tanto no caso de aquisições ou usos individuais de tais tecnologias ou serviços, quanto quando as aquisições ou usos de tais tecnologias são considerados como uma classe (TRUMP, 2019, tradução nossa).

Embora o próprio OE não mencione empresas específicas, a Huawei e mais de sessenta de suas subsidiárias e unidades de negócios foram imediatamente designadas para a Lista de Entidades da *Bureau of Industry and Security* (BIS) por serem consideradas envolvidas em atividades contrárias aos interesses de segurança dos EUA – dada sua alegada ligação com o governo chinês. A designação de Listagem de Entidade proibiu todas as empresas dos EUA e suas afiliadas de fornecer bens, serviços e propriedade intelectual à Huawei, possíveis exceções demandam a aprovação prévia por meio de licenças de Regulamentos de Administração de Exportação.

Essa primeira sanção resultou na impossibilidade da Huawei comprar componentes fabricados por empresas norte-americanas ou dotados de tecnologia norte-americana (em especial no setor de semicondutores) ou licenciar intangíveis dos Estados Unidos (software de virtualização e middleware) para uso em seus produtos. Tendo em vista os impactos negativos sobre as empresas norte-americanas, O BIS forneceu várias exceções para que a Huawei pudesse comprar produtos limitados e participar de organizações de desenvolvimento de padronização (SDOs) formalmente reconhecidas (LEE-MAKIYAMA, 2021).

Apesar do status da Huawei como ameaça à segurança nacional nesse primeiro momento, somente em agosto daquele ano, o governo Trump começou a implementar a Seção 889 do NDAA com uma regra provisória, o que instituiu a proibição oficial das agências federais dos Estados Unidos comprarem equipamentos das cinco empresas chinesas especificadas. Em novembro de 2019, a Comissão Federal de Comunicações dos EUA (FCC – sigla em inglês) também proibiu os contratados de usar subsídios federais para comprar insumos da Huawei e da ZTE (LEE-MAKIYAMA, 2021).

Em julho de 2020, o Departamento de Defesa (DoD – sigla em inglês), pautando-se na Seção 889, proibiu os empreiteiros do governo federal de usarem equipamentos fabricados pelas mesmas cinco empresas chinesas (inclusive a Huawei) em seus processos de produção em qualquer lugar, ou seja, mesmo fora do território norte-americano. Além disso, exigiu-se a remoção e substituição de insumos existentes

produzidos pelas empresas alvo das sanções (LEE-MAKIYAMA, 2021). Os custos estimados nesse processo eram de US$11 bilhões (HOLLAND; KNIGHT, 2020).

O terceiro documento, a Ordem Executiva 13959 de 12 de novembro de 2020, tem como título *Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies.* Nessa OE, o ex-presidente Donald Trump listou a Huawei como uma companhia que se aproveita do capital estadunidense com fim de adquirir recursos para desenvolver seu aparato militar, de inteligência e segurança, como fica claro na passagem abaixo:

> Eu, DONALD J. TRUMP, Presidente dos Estados Unidos da América, considero que a República Popular da China (RPC) está explorando cada vez mais o capital dos Estados Unidos para obter recursos e permitir o desenvolvimento e modernização de seus militares, inteligência e outros aparatos de segurança , que continua a permitir que a RPC ameace diretamente a pátria dos Estados Unidos e as forças dos Estados Unidos no exterior, inclusive desenvolvendo e implantando armas de destruição em massa, armas convencionais avançadas e ações cibernéticas maliciosas contra os Estados Unidos e seu povo (TRUMP, 2020, tradução nossa)

De acordo com o documento, a China fortaleceria seu complexo militar-industrial a partir do constrangimento de civis chineses no suporte a atividades militares chinesas; como consequência, os Estados Unidos declararam "emergência nacional" - ação prevista na seção 1702 do IEEPA - como resposta a esta ameaça. Nesta ordem executiva, foram criadas algumas diretrizes:

(I) Proibição da transação de títulos públicos estadunidenses, derivativos de títulos ou ativos que forneçam exposição de investimento a títulos públicos com quaisquer empresas vinculadas ao setor militar chinês;

(II) Após a identificação de uma pessoa ou entidade como vinculada a uma empresa militar da China, qualquer transação de títulos públicos estadunidenses, derivativos de títulos ou ativos que forneçam exposição de investimento a títulos públicos não poderão ser realizados a partir do prazo de 60 dias;

(III) Qualquer violação, tentativa de fuga ou prevenção de seguimento das diretrizes da OE são proibidas, sejam por pessoas dos Estados Unidos ou pessoas de outras nacionalidades que estejam em território estadunidense;

(IV) Qualquer conspiração para descumprimento das diretrizes da Ordem Executiva está proibida;

(V) A Secretaria do Tesouro, após consulta com as Secretarias do Estado e da Defesa, com a Direção da Inteligência Nacional e outras agências executivas competentes está autorizada, a partir do poder concedido ao Presidente pela *International Emergency*

Economic Powers Act (IEEPA), de 1977, a executar todos os propósitos da OE, em conjunto com agências do Departamento do Tesouro, além de outras agências competentes.

Em 5 de janeiro de 2021, foi emitida uma ordem proibindo transações financeiras em mais oito aplicativos de software chineses, dentre os quais AliPay e WeChat. Em 17 de janeiro de 2021, ainda sobre o governo Trump, foram negados ou rescindidos os pedidos de renúncia de empresas localizadas nos Estados Unidos que eram fornecedoras da Huawei, alcançando um valor de cerca de US$119 bilhões em exportações (LEE-MAKIYAMA, 2021).

O quarto documento descrito neste trabalho é a Ordem Executiva 14032, publicada em 3 de junho de 2021 pelo atual presidente Joe Biden, intitulada *Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China.* Em adição à OE 13959, este documento adiciona novas diretrizes para enfrentar a "ameaça nacional" apresentada pela China, que estaria utilizando tecnologias de segurança também para facilitar a repressão e violação de direitos humanos em território chinês:

> Eu, JOSEPH R. BIDEN JR., Presidente dos Estados Unidos da América, considero que medidas adicionais são necessárias para lidar com a emergência nacional declarada na Ordem Executiva 13959 de 12 de novembro de 2020 (Abordando a ameaça de investimentos em títulos que financiam Companhias Chinesas Militares Comunistas), incluindo a ameaça representada pelo complexo militar-industrial da República Popular da China (RPC) e seu envolvimento em programas militares, de inteligência e de pesquisa e desenvolvimento de segurança e produção de armas e equipamentos relacionados sob a Fusão Militar-Civil da RPC estratégia. Além disso, considero que o uso da tecnologia de vigilância chinesa fora da RPC e o desenvolvimento ou uso da tecnologia de vigilância chinesa para facilitar a repressão ou graves abusos dos direitos humanos constituem ameaças incomuns e extraordinárias, que têm sua fonte total ou substancial fora dos Estados Unidos, para a segurança nacional, política externa e economia dos Estados Unidos, e por meio deste amplio o escopo da emergência nacional declarada na Ordem Executiva 13959 para enfrentar essas ameaças (BIDEN, 2021, tradução nossa).

A OE 14032 encaminhou novas diretrizes ainda mais duras, além das que já haviam sido descritas na OE 13959:

1. Proibição da compra ou venda de qualquer título público, derivativos de títulos ou ativos que forneçam exposição de investimento a títulos públicos com quaisquer empresas listadas no Anexo da OE, qualquer pessoa ou entidade determinada pela Secretaria de Estado, Secretaria de Defesa ou Departamento do Tesouro, qualquer pessoa

ou entidade que opere ou já tenha operado em setores de defesa e relacionados ou de tecnologia de vigilância da economia da China;

2. Qualquer pessoa ou entidade de possuir, controlar ou ser controlado - direta ou indiretamente - por uma pessoa ou entidade que opera ou já tenha operado em quaisquer setores descritos na OE está sujeita a proibições da OE;

3. Para além de pessoas e entidades, estão sujeitas às diretrizes da OE quaisquer parcerias, associações, trustes, *joint ventures*, corporações, grupos, subgrupos ou organizações sob jurisdição dos Estados Unidos.

No dia 16 de dezembro de 2021, o *Office of Foreign Assets Control* publicou um documento intitulado *Non-SDN Chinese Military-Industrial Complex Companies List.* O documento tem como objetivo identificar entidades sujeitas a sanções, inclusive as mais recentes - descritas na Ordem Executiva de 3 de junho de 2021, chamada *Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*. Dentro deste documento estão listadas mais de 200 companhias chinesas de diversos setores como alvos - como comunicações, aviação, indústria de semicondutores, etc., incluindo as que propomos a estudar neste trabalho: *HUAWEI INVESTMENT & HOLDING CO LTD* (ou *HUAWEI TECHNOLOGIES CO., LTD.*), *HUAWEI INVESTMENT & HOLDING CO., LTD.* (ou. *HUAWEI INVESTMENT AND HOLDING CO., LTD.*), *HUAWEI INVESTMENT AND HOLDING CO., LTD.* (ou *HUAWEI INVESTMENT & HOLDING CO., LTD.*) e *HUAWEI TECHNOLOGIES CO., LTD.* (ou *HUAWEI INVESTMENT & HOLDING CO LTD*).

Em adição a este documento, o *Office of Foreign Assets Control* também publicou uma suplementação, intitulado *Chinese Military-Industrial Complex Sanctions Regulations*, com a intenção de adicionar e especificar regulamentações à Ordem Executiva 13959 já mencionada neste trabalho. O documento especifica os procedimentos administrativos, os bancos envolvidos, as penas aplicáveis a pessoas, entidades ou organizações que violem os princípios do documento, os ativos/títulos sob jurisdição do documento, sanções aplicáveis e um anexo contendo todas as empresas incluídas no documento.

Estes documentos auxiliam no entendimento da relação entre o poder do governo norte-americano, de forma a exemplificar a imposição do seu poder sobre a estrutura das TICs a partir de dispositivos institucionais legitimados pelo aparato estatal dos Estados Unidos. Na próxima seção, faremos uma análise mais profunda sobre os impactos específicos dessas políticas na empresa chinesa Huawei.

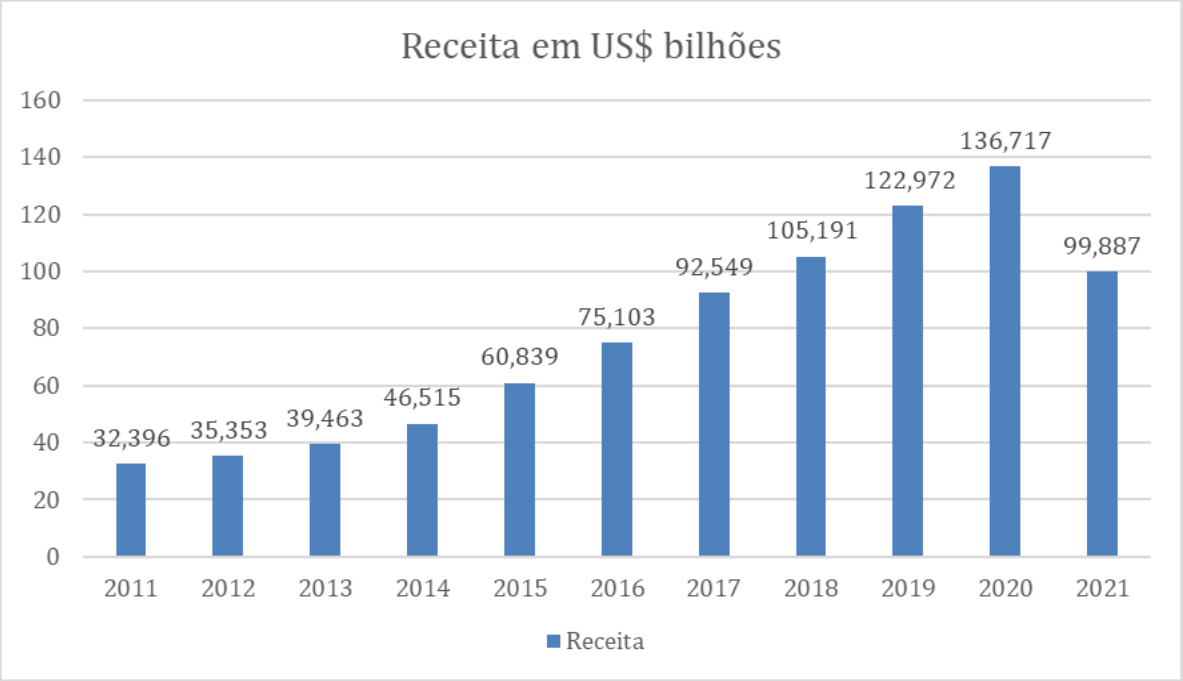
4.2 Huawei e os impactos das sanções

As sanções aplicadas contra a Huawei resultam em sérias restrições comerciais, visto que restringem: que a empresa chinesa compre equipamentos com tecnologia norte-americana, que equipamentos que contenham componentes desenvolvidos pela Huawei adentrem o território estadunidense e que empresas estadunidenses realizem livremente negócios com a gigante chinesa do setor das telecomunicações. É necessário enfatizar, entretanto, que é um setor altamente integrado, em que os prejuízos de tais sanções são disseminados por toda a cadeia produtiva global. Embora tamanha integração pareça maximizar os danos das sanções, também impede que medidas mais drásticas sejam direcionadas contra a Huawei.

Ao aplicar as sanções sobre a Huawei, o governo dos EUA atingiu também os negócios de empresas norte-americanas. A Google se viu impedida de fornecer softwares para a empresa, de modo que os celulares da Huawei – uma das maiores fabricantes de *smartphones* até então, demandaria de autorização governamental norte-americana para poder contar com o sistema operacional Android em seus celulares. A Qualcomm, gigante do ramo de fabricação de semicondutores, foi igualmente atingida pelas restrições ao restringir a venda de componentes eletrônicos. A Microsoft passou a não poder ter seus softwares em equipamentos da gigante chinesa. O mesmo ocorreu com diversas outras grandes marcas do setor de tecnologia. Tal contexto acabou por impedir que as sanções se dessem de maneira mais incisiva, e o governo acabou por conceder um grande número de exceções em um primeiro momento, de modo a amenizar a pressão feita internamente por grandes empresas.

Mesmo as sanções sendo aplicadas de maneira mais gradual, o crescimento abrupto da Huawei se viu atingido (Figura 2). A Huawei em 2011 apresentou uma receita de US$32,396 bilhões, com um lucro operacional de US$2,952 bilhões e um lucro líquido de US$1,850 bilhões. Desde então, a empresa havia apresentado crescimento constante, obtendo seus melhores números no ano de 2020: uma receita de US$136,717 bilhões, com um lucro operacional de US$11,120 bilhões e um lucro líquido de US$9,916 bilhões. Entretanto, em 2021, embora a Huawei tenha apresentado um lucro líquido de US$17,837 bilhões, também foi o primeiro ano em uma década que a companhia teve uma diminuição na receita de US$ 99,887 bilhões.

Figura 2 - Receita Huawei entre 2011 e 2021



Fonte: Produção própria baseado nos Relatórios anuais da Huawei (2012-2022)

Embora a empresa tenha apresentado crescimento, seus índices foram bem menos acentuados que nos anos anteriores. Parte dessa realidade derivou-se dos impactos das sanções sobre o setor de smartphones da companhia. Sem acesso aos chips necessários para a produção de smartphones, a Huawei foi forçada a vender sua marca de smartphones voltada para jovens, Honor, devido à "indisponibilidade persistente de elementos técnicos" (BBC, 2020, tradução nossa).

Segundo Strange (1998), a análise sobre as questões internacionais deve considerar a influência do poder para o funcionamento da economia internacional, especialmente porque não se pode desconsiderar a influência política na definição da política econômica na dimensão internacional. A análise das sanções aplicadas à Huawei não deve basear os sucessos e insucessos das sanções apenas por dados econômicos, uma vez que a hipótese defendida neste trabalho é que as sanções à Huawei objetivavam a máxima diminuição possível de componentes com tecnologia desenvolvida na China na nova infraestrutura da Internet mundial, devido a importância conferida ao acesso dos ciberterritórios e aos seus dados, tanto para o novo paradigma industrial como também para o poder militar. Assim, se faz extremamente necessário analisar se houve sucesso dos Estados Unidos em fazer com que a infraestrutura 5G de outros países não contenham equipamentos da Huawei.

Em entrevista dada ao Valor Econômico em 2021, Marcelo Motta, diretor de Cibersegurança da Huawei no Brasil, diz que dos 27 países da União Europeia, mais de 60% haviam adotado a tecnologia 5G da Huawei - cabendo a ressalva que a maioria dos países restantes não havia tomado uma decisão contrária à Huawei até a data que a entrevista foi concedida. Dentre os que se mostraram favoráveis, destaque pode ser dado à Alemanha, devido a sua importância na economia mundial.

Na América Latina, embora a maioria dos países não tenham iniciado o processo de instalação de suas redes 5G, o único país com ressalvas mais claras a adoção da tecnologia foi o Brasil. Contudo, na busca por conciliar posições contrárias, o texto da minuta do leilão ao mesmo tempo abriu possibilidade para a participação da Huawei no leilão brasileiro e trouxe instrumentos limitantes à participação da empresa chinesa apenas em setores estratégicos (SOUZA; ABRÃO; SANTOS, 2021).

Na África, a Huawei participou da construção de 70% da rede 4G (VAN STADEN, 2019) – cujos equipamentos em boa parte podem ser usados na implantação da rede 5G (VICENTIN, 2016), o que torna difícil crer que os países arcarão com os altos custos de trocar toda a estrutura para não contar com a Huawei em suas redes 5G. Na Ásia, assim como na África, os projetos de infraestruturas do governo chinês foram importantes na construção de redes de telefonia (SEGAL,2017), sendo difícil crer que a Huawei será impedida de ter seus equipamentos inseridos na nova estrutura.

Além disso, a Huawei, no que pode ser considerada como estratégia ante a dificuldade de adentrar grandes centros, vem investindo na realização de congressos em países emergentes ao redor do mundo de modo a reverter o abalo a sua imagem causadas pelas sanções e acusações norte-americanas. Tendo realizado esses congressos na América Latina, continente Africano e também Asia.

De forma que se pode dizer que o negócio de operadoras da Huawei provou ser resiliente – embora com grande dependência do mercado chinês. De fato, a Huawei foi excluída de alguns contratos de infraestrutura no Japão, Canadá e alguns países da Europa e Sudeste Asiático. Embora tenha tido perda no mercado internacional, por continuar sendo determinante na construção da infraestrutura 5G chinesa, essas perdas foram minimizadas no ano de 2021, sendo responsável por aproximadamente 60% da rede 5G da China (MAKIYAMA, 2022). A China responde por mais de 70% das estações base 5G do mundo, tendo a Huawei se beneficiado da exclusão das companhias europeias que produzem equipamentos de infraestrutura do mercado chinês.

De acordo com a empresa de análise de mercado Dell'Oro (2021), a participação de mercado da Huawei em equipamentos de rede de acesso por rádio (RAN – sigla em inglês) na América do Norte (incluindo Canadá) teve como pico 3% em 2013. Quando as sanções foram impostas em 2019, a participação de seus equipamentos era inferior a 2%. De forma que as sanções acabaram tendo pouco impacto nesse sentido.

Segundo Makiyama (2022), uma consequência claramente não intencional após as sanções sobre a Huawei é que a empresa e suas subsidiárias não poderiam mais participar da padronização internacional. No entanto, o padrão 5G depende do licenciamento cruzado de patentes essenciais ao padrão com todos os principais atores do setor, e o BIS primeiro esclareceu seus Regulamentos de Administração de Exportação (EARs, na sigla em inglês) em maio de 2019, emitindo uma licença geral temporária (uma decisão finalizada em agosto de 2020) para a Huawei no trabalho de definição de padrões. O BIS autorizou a participação da Huawei no trabalho de padronização técnica que ocorre em organizações de padronização reconhecidas internacionalmente e a liberação geral de propriedade intelectual de e para a Huawei, desde que "tal liberação seja feita com o objetivo de contribuir para a revisão ou desenvolvimento de um padrão em uma organização de padrões" (BIS, 2020, tradução nossa). Consequentemente, a Huawei tem permissão para continuar em seu papel como um dos principais contribuintes para as especificações 5G em reconhecidas organizações internacionais de desenvolvimento de padrões (SDOs – sigla em inglês), incluindo 3GPP e UTI.

Dessa forma, as sanções aplicadas à Huawei parecem ter seu sucesso condicionado a impossibilidade de a empresa chinesa disponibilizar equipamentos no mercado chinês e mundial. A esse intuito, a restrição de a Huawei acessar livremente a componentes fundamentais à confecção dos equipamentos 5G parece ser a de maior sucesso. As sanções econômicas sofridas pela Huawei criaram a impossibilidade de compra de componentes com tecnologia norte-americana, o que significa que a empresa chinesa passou a conviver com uma restrição para continuar a produzir equipamentos de ponta a longo prazo, visto ser praticamente impossível que se produza equipamentos na fronteira tecnológica sem tecnologia norte-americana (MAJEROWICZ, 2019). Além disso, as sanções impedem que a Huawei compre livremente produtos do setor de semicondutores (microprocessadores, chips, etc).

Como detalha Majerowicz (2019), a estrutura de produção de componentes semicondutores é fracionada por toda a cadeia global de produção; entretanto, ocorre sob domínio dos EUA. Enquanto as etapas simples são deslocadas de maneira global de modo

a aproveitar as vantagens de custos de produção, os processos manufatureiros mais avançados, na fronteira tecnológica e dos insumos de alta tecnologia tendem a ser submetidos a regulamentações que buscam mantê-los na economia doméstica. O mesmo processo ocorre com a produção e exportação de máquinas necessárias à sua produção.

Os norte-americanos foram fundamentais no surgimento dos semicondutores e das TICs por meio da interação entre seu complexo militar, acadêmicos e indústria, assim como no processo de conversão dessas tecnologias de origem militar para o âmbito civil. De modo que desde a origem dessas tecnologias, os Estados Unidos lideram e ditam os rumos da fragmentação produtiva dos componentes microeletrônicos.

Os componentes de microeletrônica de última geração são considerados itens de alto valor estratégico e, por isso, não se permite que sua produção ocorra em países que não sejam seus aliados militares. Mesmo que a China tenha se tornado a "fábrica do mundo" nas últimas décadas, graças ao seu impacto na diminuição dos custos de produção, determinadas máquinas e componentes eletrônicos enfrentaram e ainda enfrentam restrições para serem produzidos em território chinês.

Assim, os americanos atuaram de forma a que: (1) as etapas produtivas mais simples e demandantes de trabalho não qualificado pudessem ser alocadas globalmente de acordo com as vantagens dos custos de produção; (2) e os processos manufatureiros mais avançados que estivessem na fronteira tecnológica e submetidos a rígidas regulamentações internacionais se mantivessem na economia doméstica, bem como a produção e exportação da maquinaria para a manufatura de semicondutores de última geração (MAJEROWICZ, 2019).

Por circunstâncias geopolíticas, somente poucos países aliados militarmente aos norte-americanos foram assistidos tecnicamente e puderam receber transferência tecnológica oriunda dos Estados Unidos para produzir e desenvolver tecnologia da fronteira tecnológica. Mas, como Majerowicz e Medeiros (2018) expõe, os Estados Unidos foram bem-sucedidos, historicamente, em impedir que seus aliados rompessem os elos que os uniam no tocante à produção de semicondutores, tanto pelo uso do cerceamento político de suas indústrias (caso do Japão), quanto pelo fomento da concorrência entre os aliados militares como ferramenta para impedir que algum deles se desenvolvesse de modo suficiente para ameaçar os Estados Unidos a perderem o poder estrutural do setor – ou seja, a capacidade de determinar *quem produz*, *onde produz* e *para quem produz*.

As restrições a compras por parte de companhias chinesas de semicondutores e de máquinas para sua produção tem se agravado, o que inclui mesmo máquinas que são capazes de produzir apenas componentes de gerações anteriores, cujos componentes produzidos são destinados a uso em equipamentos eletrônicos mais simples (WU; KING; LEONARD, 2022). Diante de tal cenário, bilhões de dólares tem sido investidos pelo governo chinês nos últimos anos a fim de alcançar a tecnologia de última geração na produção de semicondutores. Busca-se com isso, salvaguardar os objetivos de liderança tecnológica apresentados em documentos como o *Made in China 2025*, as Diretrizes Nacionais para o Desenvolvimento e Promoção da Indústria de Circuitos Integrados de 2014, o Plano de Desenvolvimento da Nova Geração de Inteligência Artificial de 2017 e as Políticas para a Promoção do Desenvolvimento de Alta Qualidade da Indústria de Circuitos Integrados e da Indústria de Software de 2020.

Ao contrário do que os noticiados aumentos na produção chinesa de semicondutores possam levar a pensar, produzir tecnologia condizente com o que há de mais moderno no setor ainda é um grande desafio. As empresas chinesas buscam aumentar a produção de semicondutores em território chinês para atender a alta demanda, mas suas máquinas de litografia detêm tecnologia de ultravioleta profunda (*deep ultravioleta* – DUV), capazes de produzir *chips* de 28 nanômetros e 14 nanômetros. As máquinas de litografia mais modernas apresentam tecnologia ultravioleta extrema (*extreme ultraviolet* – EUV) capaz de produzir *chips* de 5 e 3 nanômetros. Estão a algumas gerações à frente das que podem ser encontradas na China, o que, em tese, representaria em torno de quatro ou mais anos de desvantagem na corrida tecnológica.

A holandesa ASML Holdings tem uma posição de monopólio na produção de máquinas de tecnologia ultravioleta extrema (EUV). E, mesmo não sendo norte-americana, tem ligações tecnológicas históricas com o setor de defesa dos Estados Unidos (MAJEROWICZ, 2021). Isso nos ajuda a entender o motivo pelo qual a empresa holandesa não disponibiliza máquinas EUV para a China continental, uma vez que os Estados Unidos pressionam os holandeses com o objetivo de impedir a China de fabricar *chips* semicondutores de ponta.

A tecnologia de EUV foi inventada pelos laboratórios de defesa dos EUA Sandia e é uma das mais complexas já desenvolvidas (SANDIA, 1997). Essa tecnologia surgiu no contexto da corrida tecnológica da Guerra nas Estrelas dos anos 1980, com raízes que remontam à Segunda Guerra Mundial e ao Projeto Manhattan. Inicialmente, a tecnologia de EUV teria que ser repassada para empresas norte-americanas de litografia. Entretanto,

após a pressão exercida por grandes companhias americanas de semicondutores, com destaque ao papel da Intel, que procuravam melhores custos de produção, a tecnologia foi transferida para as japonesas Nikkon e Canon e a ASML – que, embora holandesa, produzia na Ásia, mais especificamente em Taiwan (MAJEROWICZ; MEDEIROS, 2019).

De forma que apenas alguns poucos países aliados militares – por questões geoestratégicas – receberam assistência técnica e transferência tecnológica dos EUA para a produção de equipamentos na fronteira tecnológica (MAJEROWICZ; MEDEIROS, 2018). Os EUA têm se mostrado capazes de enquadrar tais aliados de modo a conseguir manter para si o domínio de tal tecnologia (MAJEROWICZ; MEDEIROS, 2018), o que impede que a Huawei tenha livre acesso a componentes essenciais para a fabricação de seus equipamentos para a rede 5G e limitando sua capacidade de atender a demanda mundial por tais equipamentos.

Entretanto, em 15 de novembro de 2022, a Huawei registrou uma patente para a tecnologia EUV (HUAWEI, 2022), o que pode mudar completamente a dinâmica de poder do setor de semicondutores se de fato a China passar a produzir internamente semicondutores na fronteira tecnológica.

5 Considerações finais:

A partir do exposto no presente trabalho, percebe-se o momento atual como decisivo para a manutenção do poder norte-americano, uma vez que a China tem buscado, e com muitos sucessos, alcançar o patamar dos Estados Unidos em termos tecnológicos. Desde a sua ascensão econômica e tecnológica ocorrida no final do século XIX, os EUA sempre ocuparam o posto de maior potência tecnológica, em especial quanto às TICs. É inegável que, hoje, os Estados Unidos ainda detém o posto de maior potência tecnológica mundial, restando ainda um longo caminho a ser percorrido para a China os alcançar.

Porém, é inegável também o grande êxito alcançado pelo projeto chinês de desenvolvimento no seguimento das TICs, estando o país, hoje, na vanguarda tecnológica intrinsecamente ligado às TICs, tanto para uso militar quanto civil. Em função disso, os Estados Unidos fazem um movimento totalmente lógico, e esperado, dentro da visão realista das relações internacionais, que consiste na tentativa de bloquear, ou pelo menos conter, o avanço tecnológico chinês sobre territórios em que o seu poder é consolidado. Para alcançar tal fim, os EUA impõem barreiras comerciais e financeiras para limitar o acesso chinês a componentes e serviços essenciais oriundos de empresas norte-americanas, e utilizam a sua influência sobre outros países e regiões subordinados para reforçar esta política.

O caso da Huawei pode ser visto como emblemático justamente por unir distintos aspectos nesse embate. Como o demonstrado, o surgimento da Huawei se entrelaçou com a busca pela redução dos custos de produções das economias centrais, que ao adotarem o modelo de produção modular acabaram por transformar a China na ‘fábrica do mundo’, possibilitando, assim, que este país colocasse em prática um projeto de desenvolvimento tecnológico centrado na absorção de tecnologia estrangeira. Como resultado desse projeto, a China se transformou na segunda maior potência mundial em poucas décadas e alcançou o posto de desafiante tecnológico.

Outro ponto que reforça a ligação da companhia com o governo chinês é o fato de o fundador da Huawei ter sido um ex-militar chinês, o que, somado aos esforços do governo chinês visando o crescimento da empresa, nutre a ideia de proximidade entre as partes – governo, militares chineses e Huawei. Tal quadro acaba por levar os Estados Unidos a preocupações, uma vez que a atuação militar norte-americana no século XXI mostra como tem sido cada vez maior a importância das TICs no campo bélico – tanto no controle de *Vants*, como na vigilância de pessoas, empresas e governos.

Porém, os esforços norte-americanos a fim de limitar a ascensão econômica chinesa esbarram em condições e características particulares apresentadas pela China. Diferentemente do que ocorre quanto a países periféricos, ou mesmo com países desenvolvidos com pequenos territórios, baixa densidade demográfica e economias mais suscetíveis às variações internacionais, a China detém meios para resistir a essa tentativa de bloqueio por parte dos EUA. Seu enorme mercado interno tem sido usado desde a década de 1980 para induzir o Ocidente a suavizar os seus ataques e a transferir tecnologia às empresas e estatais chinesas. Isto acabou por conferir à China uma enorme capacidade exportadora, conseguindo se tornar peça-chave nas cadeias globais de produção.

Assim, os EUA não podem simplesmente atacar a China e tratá-la como um mero país do qual não dependam. Tal medida feriria interesses vitais dos Estados Unidos e também de suas empresas de ponta como Amazon, Apple, Boeing, entre outras, além de boa parte do complexo industrial-militar norte-americano, que ainda depende da economia chinesa para o fornecimento de diversos tipos de bens e serviços essenciais, inclusive no setor eletrônico.

Os Estados Unidos, desde o final do século XIX, sempre estiveram na vanguarda tecnológica no tocante aos meios de produção, e isso é especialmente o caso em relação à infraestrutura da informação. Como demonstrado, a infraestrutura da internet está intimamente ligada à capacidade de monitoramento de dados pelas agências de inteligência dos países, sendo a atuação estadunidense nesse campo, via a NSA, de longe a mais significativa.

Diante da realidade de que os conflitos e ataques entre as grandes potências tornam-se cada vez mais multidimensionais, é de se esperar que os Estados Unidos não poupem esforços para manterem sua larga vantagem na corrida de capacidade cibernética, visto que essa torna-se cada dia mais central na perspectiva militar norte-americana. Essa perspectiva inclui manter a infraestrutura da internet global com a menor quantidade possível de componentes chineses desenvolvidos para a tecnologia 5G e o mais longe possível dos padrões tecnológicos desejados pela China. Salvaguardando, assim, não só o seu ciberterritório de característica supranacional, construído sobre a ligação entre o Estado norte-americano e suas companhias, com destaque para as *Big Techs*.

Porém, o fato da versão da tecnologia 5G desenvolvida pela Huawei ofertar um desempenho tão superior às versões da concorrência e ser ofertada a um custo significativamente mais baixo dificulta os objetivos dos Estados Unidos junto aos outros países centrais. Tal dificuldade se soma ao desafio trazido pela estratégia chinesa de

ofertar crédito em condições mais acessíveis à países periféricos, em especial no tocante a projetos de infraestrutura, o que acaba por facilitar que seus equipamentos, mais eficientes e com um custo menor, permeiem a infraestrutura da internet de tais países. Como resultado desse quadro, temos que 60% dos países da União Europeia já adotaram a tecnologia 5G da Huawei, sendo a aceitação do governo alemão o mais significativo. Existindo também uma forte presença de acordos para o uso da tecnologia nos territórios de países do Oriente Médio e da Ásia (Santana 2020).

O cenário para convencer as grandes potências a não adotarem a tecnologia 5G da Huawei é desafiador, principalmente mediante ao importantíssimo papel que a tecnologia 5G cumpre para a mudança de paradigma industrial, sendo a sua conexão de altíssima velocidade vital para o nível de automação que se espera implementar nas indústrias já nos próximos anos. Bem como o fato que proporcionará enormes ganhos de integração entre equipamentos domésticos e também nas cidades inteligentes através da Internet das Coisas. Além de tender a possibilitar enormes saltos tecnológicos mediante aos ganhos cognitivos ofertados pela Inteligência Artificial. Num cenário de grande competição empresarial e estatal, grandes potências não tendem a abrir mão por muito tempo dos ganhos de produtividade e das enormes possibilidades propulsionadas pela tecnologia 5G.

Ademais, os vazamentos de informações sigilosas sobre as operações de vigilância dos Estados Unidos enfraquecem os argumentos de riscos a segurança e soberania nacional, uma vez que é sabido que ações de vigilância já são uma realidade. Tal realidade conhecida conduz as decisões a serem tomadas a ponderarem mais sobre quem acessará os dados produzidos dentro do seu território nacional do que se isso de fato ocorrerá, tamanha a assimetria entre os ciberpoderes dos estados.

A natureza realista da resposta norte-americana aos riscos ao seu poder trazidos pela difusão em massa da tecnologia 5G da Huawei pelo tabuleiro global reforçam a centralidade dada pelos Estados Unidos às TICs no campo militar. A tendência, independentemente da vertente que esteja no poder nos Estados Unidos, é que a relação EUA-China se torne cada vez mais conflituosa, embora rompimentos abruptos sejam improváveis e o diálogo retome tom diplomático bem distinto do tom usado pelo governo de Donald Trump, o que de fato aconteceu desde a posse do presidente Joe Biden, em 2021.

As disputas citadas no decorrer do trabalho visam o acúmulo de mais poder e são tidas como inevitáveis segundo a ótica do Dilema de Segurança; cada qual lidando com

a realidade que lhe é imposta a seu jeito, mas atuando através da união indissociável entre poder e capital pela busca por mais poder e a construção de posições privilegiadas. Os Estados Unidos têm que lidar com os impactos econômicos, os interesses e pressões de importantes segmentos empresariais internos que se prejudicariam em caso de uma exacerbação das limitações negociais com empresas chinesas imposta pelo governo norte-americano; e a China tendo que lidar com perda de competitividade em determinados segmentos por não poder contar com componentes de ponta em setores nos quais não detêm a vanguarda do conhecimento tecnológico – como tem sido, no momento, quanto a restrições a adquirir microprocessadores e outros semicondutores de última geração.

Por fim, fica claro que os EUA buscam seguir o modelo de exercício de poder que os conduziram ao posto mais alto do tabuleiro global, entendendo que a manutenção de seu poder exige a busca constante da acumulação de mais poder. Como ensinou Norbert Elias, na esfera da competição interestatal, quem não sobe, cai. Por outro lado, a China parece ter reaprendido a lição – bem conhecida por seus antepassados milenares – que, para se manter forte e altiva, é necessário se manter na vanguarda da inovação e da tecnologia.

Referências

ABDELAL, R. National Purpose in the World Economy. Ithaca, NY: Cornell University Press. 2001.

AGAMBEN, Giorgio. **Estado de exceção**. Boitempo, São Paulo, 2004.

AL-FALAHY, N.; ALANI, O. Y. K. Technologies for 5G networks: Challenges and opportunities, **IT Professional**, vol. 19, no. 1, pp. 12-20, 2017

ARONCZYK, Melissa; BUDNITSKY, Stanislav. Nation Branding and Internet Governance: Framing Debates over Freedom and Sovereignty. Em: **The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance**, edited by Uta Kohl, 48-65. Cambridge: Cambridge University Press. 2017.

ARRIGHI, Giovanni. **O Longo Século XX: dinheiro, poder e as origens do nosso tempo.** Rio de Janeiro: Editora Contraponto, 1996.

BARREIROS, Daniel. **Projeções sobre o Futuro da Guerra: Tecnologias disruptivas e mudanças paradigmáticas (2020 – 2060)**. 2019

BAUMAN, Zygmunt. et al. **After Snowden: rethinking the impact of surveillance**. 2014. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.840.3683&rep=rep1&type=pdf Acesso: 18 de agosto de 2022

BBC. 2020. Huawei sells youth brand over tech restrictions. **BBC News** 17 de novembro de 2020 Disponível em: https://www.bbc.co.uk/news/world-asia-54970003 Acesso em: 05 de outubro de 2021.

Berman, Paul S. 2018. Legal Jurisdiction and the Deterritorialization of Data. **Vanderbilt Law Review 71** (En Banc):12-32.

BRAUDEL, F. (1949[2000]). **The Mediterranean and The Mediterranean World in the Age of Philip II**. London: Haeper Collins Publisher ltd..

BRAUDEL, F. (1969[2007]), **Escritos sobre a História**. são Paulo: editora Perspectiva.

BRAUDEL, F. (1986[1998]), **Civilização Material, Economia e Capitalismo – Séculos XV-XVIII**, vol. 03, S.Paulo: editora Martins Fontes.

BRAUDEL, Fernand. **A Dinâmica do Capitalismo.** Rocco, 1987.

BROWN, W. M. **The Royal Navy's fuel supplies, 1898-1939: the transition from coal to oil**. London: University of London, 2003. 328 p.

BUREAU OF INDUSTRY AND SECURITY. (2020). **Release of "Technology" to certain entities on the entity list in the context of standards organizations**. Federal Register. Disponível em: https://www.federalregister.gov/documents/2020/06/18/2020-13093/release-of-technology-to-certain-entities-on-the-entity-list-in-the-context-ofstandards Acesso em: 15 de Janeiro de 2023

BURLAMAQUI, Leonardo. As Finanças Globais e o Desenvolvimento Financeiro Chinês: um modelo de governança financeira global conduzido pelo Estado. In: **China em transformação: Dimensões econômicas e geopolíticas do desenvolvimento**. IPEA Disponível em: https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/150918_livro_china_em_transformacao.pdf Acesso em: 04 de junho de 2021

CAMPBELL. Karen; CRUZ, Liz; FLANAGAN, Bob; MORELLI, Bill; O'NEIL,Brendan; TÉRAI, Stéphane; WATSON, Julian. The 5G Economy: How 5G will contribute to the global economy. **HIS Markit** novembro de 2019 Disponível em: https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/the_ihs_5g_economy_-_2019.pdf Acesso em: 14 de abril de 2021

CHEY, H. **The concepts, consequences, and determinants of currency internationalization**. GRIPS Discussion Paper, National Graduate Institute for Policy Studies, n. 13-03, maio 2013. Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China, Global Times, March 13, 2017, Disponível em: www.globaltimes.cn/content/1037500.shtml Acesso em: 22/02/2021

COHEN, Julie E. 2007. Cyberspace As/And Space. Columbia Law Review 107 (1):210-56.

CRANE, G. Imagining the Economic Nation: Globalisation in China. **New Political Economy** v. 4, n. 2, p. 215–232. 1999.

DAGGETT, Stephen. **Quadrennial Defense Review 2010: Overview and Implications for National Security Planning.** Disponível em: https://apps.dtic.mil/sti/pdfs/ADA522091.pdf Acesso em: 16 de abril 2022

DE WEI, Low. Full Text of Xi Jinping's Speech at China's Party Congress. **Bloomberg, 18 de outubro de 2022.** Disponível em: https://www.bloomberg.com/news/articles/2022-10-18/full-text-of-xi-jinping-s-speech-at-china-20th-party-congress-2022?leadSource=uverify%20wall Acesso em: 01 de dezembro de 2022

DELL'ORO. (2021). **Market Research Reports on Mobile Radio Access Network (RAN)**. Disponível em: https://www.delloro.com/market-research/telecommunicationsinfrastructure/mobile-radio-access-network/ Acesso em: 15 de janeiro de 2023.

ELIAS, Norbert. **O processo civilizador.** Rio de Janeiro: Jorge Zahar, 1994. 2 v.

FERNANDES, Marisa. A Arma Submarina na Estratégia Alemã na Primeira Guerra Mundial. **Revista Nação e Defesa**, vol. 145, p.133-152, 2016. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/23869/1/FERNANDESMarisa_p133_152.pdf; Acesso em: 12 de ago. de 2022.

FERREIRA, M. M.; VIEIRA, Rosângela de Lima. Economia política dos sistemas-mundo e as novas perspectivas de pesquisas para a história econômica. In: **XXVI Simpósio Nacional da ANPUH, 2011,** São Paulo. Anais do XXVI simpósio nacional da ANPUH - Associação Nacional de História. São Paulo: ANPUH - SP, 2011.

FINNEMORE, Martha, and HOLLIS, Duncan B. Constructing Norms for Global Cybersecurity. **American Journal of International Law** 110 (3):425-79. 2016. doi: 10.1017/S0002930000016894.

FIORI, José Luís. Formação, Expansão e Limites do Poder Global. In: **O Poder Americano.** Rio de Janeiro: Editora Vozes, 2004.

FIORI, J. L. da C. . 2005. Sobre o Poder Global. **Revista Novos Estudos**, **73**(3) Novembro de 2005. Disponível em: https://novosestudos.com.br/wp-content/uploads/2017/05/17_sobre_o_poder_global.pdf.zip Acesso em: 13 de fevereiro de 2022

FIORI J. L. da C. . (2010). PREFÁCIO AO PODER GLOBAL. **Revista Tempo Do Mundo, 2(1),** 131-153. Disponível em: https://www.ipea.gov.br/revistas/index.php/rtm/article/view/129 Acesso em: 08 de fevereiro de 2022

FOUKAS, X.; PATOUNAS, G.; ELMOKASHFI, A.; MARINA, M. K. Network slicing in 5G: Survey and challenges, **IEEE Commun**. Mag., vol. 55, no. 5, pp. 94–100,Maio 2017.

FREITAS, Maria Cristina P. **A transformação da China em economia orientada à inovação**. São Paulo: Instituto de Estudos para o Desenvolvimento Industrial, ago. 2011.

GARCEZ, Nathana. **O papel da primeira Guerra Mundial na Formação da Geopolítica do Petróleo para a Região do Cáucaso.** Dissertação de mestrado apresentado em Programa de Economia Política Internacional – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020 Disponível em: https://www.ie.ufrj.br/images/IE/PEPI/disserta%C3%A7%C3%B5es/2020/Disserta%C3%A7%C3%A3o%20Nathana%20GarcezPEPI.pdf Acesso em: 20 de junho de 2021

GIBSON, Willian. **Neuromancer**. São Paulo: Aleph, 2003.

GILPIN, R. **The Political Economy of International Relations**. Princeton, NJ: Princeton University Press. 1987

GILPIN, R. **Global Political Economy**. Princeton, NJ: Princeton University Press. 2001

GOTTMANN, J. (1975[2012]) A evolução do conceito de território, **Boletim Campineiro de Geograia**, v. 2, n. 3, p. 523–545.

GRAMSCI, Antonio. **Cadernos do Cárcere**. Rio de Janeiro: Civilização Brasileira, 2000.

HAESBAERT, R. **O mito da desterritorialização: do "fim dos territórios" à multi - territorialidade.** Rio de Janeiro: Bertrand Brasil. 2004

HARRIS, Shane. **@War:The rise of the military-internet comple**x. Houghton Mifflin Harcourt, Nova Yorke, 2014.

HAN, B.; GOPALAKRISHNAN, V.; JI, L.; LEE, S Network function virtualization: Challenges and opportunities for innovations, **IEEE Commun**. *Mag.*, vol. 53, no. 2, p. 90-97, Feb. 2015.

HELLEINER, Eric, 2002, The Diversity of Economic Nationalism. **New Political Economy**

HUAWEI. **Annual Report 2011**. Disponível em: https://www.huawei.com/br/annual-report Acesso em: 25 de setembro de 2022

HUAWEI. **Annual Report 2021**. Disponível em: https://www.huawei.com/br/annual-report Acesso em: 25 de setembro de 2022

INSTITUTE FOR SECURITY STUDIES, Brussels, November 19, 2013. **Capacity Building in Cyberspace: Taking Stock, report from seminar organized by the European Union.** Disponível em: https://www.iss.europa.eu/content/capacity-building-cyberspace-taking-stock. Acesso em: 22 de fevereiro de 2021

KAGERMANN, H. Change Trhough Digitilization – Value Creation in the Age of Industry 4.0 in ALBACH, H et al. (ed) **Management of Permanent Change.** Wiesbaden: Springer Gabler, 2015.

KALECKI, M. (1993a) "The problem of financing economic development". Em J. Osiatynsky, ed., *Collected Works of Michal Kalecki*, Vol. V Oxford: Oxford University Press, 1993

KALECKI, M. (1993b) The difference between crucial economic problems of developed and underdeveloped non-socialist economies. Em J. Osiatynsky, ed., **Collected Works of Michal Kalecki**, Vol. V Oxford: Oxford University Press, 1993.

KALECKI, M. **Teoria da dinâmica Econômica**. Editora Nova Cultural Ltda, 1977.

KELLNER, Douglas. **Como mapear o presente a partir do futuro: de Baudrillard ao cyberpunk. A cultura da mídia**. Bauru: EDUSC, 2001. p.377-419.

KENNEDY, Paul (1996). **Ascensão e queda das grandes potências.** Rio de Janeiro: Campus.

KOEPSELL, David R. **A ontologia do ciberespaço: a Filosofia, a lei e o futuro da propriedade intelectual**. São Paulo: Madras, 2004.

KOHL, Uta; FOX. Carrie. 2017. "Introduction: Internet Governance and the Resilience of the Nation State." Em **The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance**, edited by Uta Kohl, 1-23. Cambridge: Cambridge University Press.

KRASNER, Stephen D. **Sovereignty: Organized Hypocrisy,** Princeton: Princeton University Press, 1999. https://doi.org/10.1515/9781400823260

KREUTZ, D.; RAMOS, F. M. V.; VERÍSSIMO, P. J. E.; ROTHENBERG, C. E.; AZONDOLMOLKY, S.; UHLIG, S. Software-defined networking: A comprehensive survey, **Proc. IEEE**, vol. 103, no. 1, pp. 14-76, Jan. 2015.

LACOSTE, Y. (1985[20080]), **A Geograia – Isso Serve, em Primeiro Lugar, para Fazer a Guerra**, campinas: Papirus editora.

LACOSTE, Y., org. (1989) **Ler Braudel**, campinas: Papirus editora.

LAMBACH, Daniel. 2020. The Territorialization of Cyberspace. **International Studies Review**, Volume 22, Issue 3, September 2020, Pages 482–506, Disponível em: https://doi.org/10.1093/isr/viz022 Acesso em 15/01/2023

LANTIS, Jeffrey S.; BLOOMBERG, Daniel J. Changing the code? Norm contestation and US antipreneurism in cyberspace. **International Relations** 32 (2):149-72. 2018. doi: 10.1177/0047117818763006

LEÃO, Valdemar Carneiro. Prefácio. In**: China em transformação: Dimensões econômicas e geopolíticas do desenvolvimento**. IPEA Disponível em: <https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/150918_livro_china_em_transformacao.pdf Acesso 04 de maio de 2021

LEE-MAKIYAMA, H. (2022) US Sanctions Against Chinese 5G: Inconsistencies and Paradoxical Outcomes. **Ecipe.** Disponível em: https://ecipe.org/blog/us-sanctions-against-chinese-5g/ Acesso em: 15/01/2023

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed.34, 2000.

LIST, F. The National System of Political Economy. London: Longmans, Green. 1904 McDOWELL, Robert M.; GOLDSTEIN, Gordon M., "The Authoritarian Internet Power Grab," **Wall Street Journal,** 25 de outubro de 2016, www.wsj.com/articles/the-authoritarian-Internet-power-grab-1477436573. Acesso em 02 de Janeiro de 2022

LOGHIN, D.; CAI, S.; SHEN, G.; DINH T. T. A.; FAN, F.; LIN, Q.; NG, J.; OOI, B.C.; SUN, X.; TA, Q.; WANG, W.; XIAO, X.; YANG, Y.; ZHANG, M.; ZHANG, Z. **The disruptions of 5G on data-driven technologies and applications**, 2019 Disponível em: https://arxiv.org/abs/1909.08096 Acesso em: 27 de nov. de 2022.

LOGOTA, E. *et al*. The 5G Internet. *In:* RODRIGUEZ, J. (Ed.). **Fundamentals of 5G Mobile Networks**. Chichester: John Wiley & Sons Inc., 2015, p. 29–62.

MAJEROWICS, E As tecnologias da informação e comunicação na disputa entre China e Estados Unidos. **Jornal dos Economistas,** Rio de Janeiro v. 365 p 10-11, março 2020.

MAJEROWICZ, E. A China e a Economia Política Internacional das Tecnologias da Informação e Comunicação. **Textos para Discussão** n. 001. Natal: Universidade Federal do Rio Grande do Norte, Departamento de Economia, jul. 2019. Disponível em: https://ccsa.ufrn.br/portal/wp-content/uploads/2019/07/tddepec0012019MajerowiczRev.pdf. Acesso em: 05 out. 2021.

MAJEROWICZ, E. As tecnologias da informação e comunicação enquanto sistema tecnológico e de maquinaria: implicações para as dinâmicas concorrenciais. **Texto para Discussão** n. 005. Natal: Universidade Federal do Rio Grande do Norte, Departamento de Economia, jul. 2021. Disponível em: https://ccsa.ufrn.br/portal/wp-content/uploads/2021/07/tddepec005Majerowicz-3.pdf. Acesso em: 31 out. 2021.

MAJEROWICZ, E.; MEDEIROS, C. A. Chinese industrial policy in the geopolitics of the information age: the case of semiconductors. **Revista de Economia Contemporânea**, v. 22, n. 1, p. 1–28, 2018. Disponível em: https://doi.org/10.1590/198055272216. Acesso em: 30 out. 2021.

MARZINOTTO JUNIOR, F. L. **Estados e mercados na era do Big Data: Oligopolização das Big Techs e a política norte-americana nos governos Obama e Trump (2009-2021).** Dissertação de mestrado apresentado em Programa de Economia Política Internacional – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022 Disponível em: https://www.ie.ufrj.br/images/IE/PEPI/disserta%C3%A7%C3%B5es/2022/Disserta%C3%A7%C3%A3o_Francisco_Marzinotto_final.pdf Acesso em 18 de agosto de 2022

MEARSHEIMER, John. **The tragedy of great power politics.** New York: W. W. Norton & Company, 2001

MEARSHEIMER, John**. The Great Delusion – Liberal Dreams and International Realities.** Yale University Press, 2018

MEDEIROS, Carlos. O ciclo recente de crescimento chinês e seus desafios. In: **ENCONTRO NACIONAL DE ECONOMIA POLÍTICA, 15**., 2010, São Luís, Anais… São Luís, 2010.

MENN, Joseph. White House–ordered Review Found No Evidence of Huawei Spying: Sources, **Reuters, October 18, 2012.** Disponível em: https://www.reuters.com/article/ctech-us-huawei-spying-idCABRE89G1Q920121018 Acesso em 20 de junho de 2022

MOHYELDIN, E. **Minimum technical performance requirements for IMT-2020 radio interface(s)**, 2016. Disponível em: http://archive.fo/WbPkW Acesso em: 21 de abril de 2022

MONTEIRO, S.D. O. Ciberespaço: o termo, a definição e o conceito. 2007. **Revista de Ciência da Informação** - v.8 n.3 Jun/07

MU, Qing; LEE, Keun. **Knowledge diffusion, market segmentation and technological catch-up: the case of the telecommunication industry in China**. Research Policy, n. 34, p. 759-783, 2005.

NATIONAL SECURITY AGENCY. **ST-09-002 Working Draft. Office of the Inspector General**. 24 de março 2009. Disponível em União Americana de Liberdades Civis, em: https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf Acesso: 14 jul.2021.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE (NSCAI). **Chinese Tech Landscape Overview**. NSCAI Presentation, 2019. Disponível em: https://epic.org/foia/epic-v-ai-commission/EPIC-19-09-11-NSCAI-FOIA-20200331-3rd-Production-pt9.pdf. Acesso em: 08 fev. 2022.

NEW AMERICA FOUNDATION. **Drone Wars Pakistan: Analysis**. Disponível em: http://natsec.newamerica.net/drones/pakistan/analysis. Acesso em 12 de abril de 2021.

NEWMAN, David. 2006. As linhas que continuam a nos separar: fronteiras em nosso mundo 'sem fronteiras'. **Progresso em Geografia Humana 30** (2):143-61. doi: 10.1191/0309132506ph599xx.

NISSENBAUM, Helen. 2004. **Hackers and the contested ontology of cyberspace**. New Media & Society 6 (2):195-217

NOGUEIRA, Isabela. Políticas de fomento à ascensão da China nas cadeias de valor globais. In: **China em transformação: Dimensões econômicas e geopolíticas do desenvolvimento.** IPEA Disponível em: <https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/150918_livro_china_em_transformacao.pdf. Acesso em 14 de abril de 2022

OUT OF SIGHT, OUT OF MIND. 2014. **Attacks.Plataforma Digital**. Disponível em: http://drones.pitchinteractive.com. acesso em 16 de maio de 2022.

NOGUEIRA, I.; QI, Hao. Estado e Burguesia Nacional na China: do grande compromisso à aliança tensa. In: Majerowicz; Paraná. (Org.). **A China no Capitalismo Contemporâneo**. 1ed.: 2022.

OLSON, Kathleen K. 2005. Cyberspace as Place and the Limits of Metaphor. **Convergence: The International Journal of Research into New Media Technologies** 11 (1):10-8

PALMER, M. **Data is the New Oil**. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html Acessado em: 20 de dezembro de 2022

PEREZ, Bien. China's ZTE Takes Over Netas for $101m, Eyes Expansion in Turkey, **South China Morning Post**, December 6, 2016, www.scmp.com/tech/china-tech/article/2052271/chinas-zte-takes-over-netas-101m-eyes-expansion-turkey. Acessado às 03:30 horas

PIRES, Marcos Cordeiro. O Brasil, o Mundo e a Quarta Revolução Industrial: reflexões sobre os impactos econômicos e sociais. **REVISTA DE ECONOMIA POLÍTICA E HISTÓRIA ECONÔMICA, v. 40**, p. 5-36, 2018.

PRATT, Andy C. 2000. New media, the new economy and new spaces. **Geoforum 31** (4):425-36. doi: https://doi.org/10.1016/S0016-7185(00)00011-7.

PRESCOTT, Roberta. **PP-14: entenda o que foi a Conferência Plenipotenciária da UIT.** 2014. Disponível em: https://www.abranet.org.br/Noticias/PP-14:-entenda-o-que-

foi-a-Conferencia-Plenipotenciaria-da-UIT-374.html?UserActiveTemplate=site&from%25255Finfo%25255Findex=500&tpl=printerview Acesso em: 22 de junho de 2022

RABAÇA, Carlos; BARBOSA, Gustavo G. **Dicionário de comunicação.** 2.ed. rev. e atual. Rio de Janeiro: Campus, 2001.

RAMAL, Andrea Cecília. **Educação na cibercultura: hipertextualidade, leitura, escrita e aprendizagem.** Porto Alegre: Artmed, 2002.

RATZEL, F. (1897). **Géographie politique**. Paris: Ed. Régionales européennes,1988.

RATZEL, Friedrich. **A relação entre o solo e o Estado** – Capítulo I: O Estado como organismo ligado ao solo [p. 59]. Tradução de Matheus Pfrimer. Revista Espaço e Tempo, 29: 51-58. São Paulo: GEOUSP. 2011

REICH, R. The Work of Nations. New York: Alfred A. Knopf. 1991
SAY, Jean Baptiste. **A treatise on political economy; or the production distribution and consumption of wealth**. Batoche Books Kitchener. 2001

SACK, R. **Human Territoriality: its theory and history**. Cambridge : Cambridge University Press 1986

SALINAS, Sara. Six top US intelligence chiefs caution against buying Huawei phones. **CNBC**. Disponível em: https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html Acesso em: 14 de junho de 2022

SANDERSON, Henry; FORSYTHE, Michael. **China's superbank**: debt, oil and influence – how China Development Bank is rewriting the rules of finance. Singapore: Wiley; Bloomberg Press, 22 Jan. 2013. (Versão para Kindle).

SANTANA, Ivone. Na guerra do 5G, Huawei já tem 60% da EU. **Valor Econômico**. Disponível em: https://valor.globo.com/empresas/noticia/2020/12/29/na-guerra-do-5g-huawei-ja-tem-60-da-ue.ghtml Acesso em: 22 de mar. 2021

SCHMITT, Michael N. **Tallinn Manual 2.0 on the Inter Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.** Cambridge: Cambridge University Press. 2017.

SCHUMPETER, Joseph. **The theory of economic development**. New York: Transaction Press, 1934.

SCHWAB, Klaus. **The Fourth Industrial Revolution**. 2016. Geneva- Switzerland: World Economic Forum.

SEGAL, Adam. **Chinese Cyber Diplomacy in a new era of uncertainly**. 2017

SEGAL, Adam. **The Hacked Word Order.** New York: Public Affairs. 2016

SILVA, Carlos Alberto F. da; SILVA, Michele T. Cândido da. A dimensão socioespacial do ciberespaço: uma nota. 2004. Disponível em: http://www.tamandare.g12.br/indexciber.htm. Acesso em: 20 out. 2021.

SOUZA FILHO, C. L. S. O Olhar da (in)Segurança: **NSA e os efeitos da Securitização da Internet**. 2018. 63f. Trabalho de Conclusão de Curso (Bacharelado) – Instituto de Relações Internacionais e Defesa, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018.

SVANTESSON, Dan J. B. 2016. International law and order in cyberspace—cloud computing and the need to revisit the foundations of "jurisdiction". **Aspen Review**. Disponível:https://www.aspen.review/article/2017/international-law-and-order-in-cyberspace-cloud-computing-and-the-need-to-revisit-the-foundations-of-jurisdiction/. Acesso em: 05 de maio de 2022

THE PEOPLE'S REPUBLIC OF CHINA. **National Programme on Made in China 2025 (**中国制造**2025)**. Beijing: The State Council of The People's Republic of China, 7 jul. 2015b. Disponível em: http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf. Acesso em: 28 fev. 2022.

THE PEOPLE'S REPUBLIC OF CHINA. **The National Medium- and Long-Term Program for Science and Technology Development (2006-2020**): an outline. Beijing: The State Council of The People's Republic of China, 2006. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf. Acesso em: 28 fev. 2022.

THE FOREIGN INTELLIGENCE SURVEILLANCE OF 1978 (FISA) IN JUSTICE INFORMATION SHARING, **Department of justice**. Disponível em: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286 Acesso: 14 de julho de 2021

THE PROTECT AMERICA ACT OF 2007 IN GOVERNMENT PUBLISING OFFICE. Disponível em: https://www.gpo.gov/fdsys/pkg/STATUTE-121/pdf/STATUTE-121-Pg552.pdf Acesso: 17 de julho de 2021

THE UNITED STATES OF AMERICAN. 2018. H.R.5515 - **John S. McCain National Defense Authorization Act for Fiscal Year 2019**. Disponível em: https://www.congress.gov/bill/115th-congress/house-bill/5515 Acesso em: 02 de Agosto de 2021

XI, J. **A governança global da China**. Pequim: Editora de Línguas Estrangeiras, 2014.

TILLY, Charles. **Coerção, capital e Estados europeus.** São Paulo: EDUSP, 1996.

TRIOLO, P.; ALLISON, K.; BROWN, C. **The Geopolitics of 5G.** Eurasia Group White Paper. Nova Iorque: Eurasia Group, 15 nov. 2018. Disponível em: https://www.eurasiagroup.net/siteFiles/Media/files/1811-14 5G special report public(1).pdf. Acesso em: 15 nov. 2021.

VAN STANDEN, Cobus. 2019. How the US-China conflict over Huawei could play out in Africa. The Africa Report. Disponível em: https://www.theafricareport.com/15451/how-the-us-china-conflict-over-huawei-could-play-out-in-africa/ Acesso em: 20 de dezembro de 2022

VESENTINI, José William. **Novas Geopolíticas**. 4. ed. São Paulo: Contexto, 2005.

VERBERGT, Matthias "China's Huawei Battles to Own the Next Generation of Wireless Technology," **Wall Street Journal,** February 26, 2017, https://www.wsj .com/articles/chinas-huawei-battles-to-own-the-next-generation-of-wireless-technology-1488114002.

VISENTINI, Paulo Fagundes. **As Guerras Mundiais (1914-1945)**. 2. ed. Porto Alegre: Leitura XXI, 2012.

WANDERLEY, L. A. Ciclos sistêmicos de acumulação de Arrighi e padrões de tecnologias. In: ENCONTRO NACIONAL DE ECONOMIA POLÍTICA, 14., 2009, São Paulo. **A Crise Financeira Mundial e as Alternativas de Desenvolvimento da América Latina**. São Paulo: PUC, 2009.

WALKER, Robert. International relations as political theory. In: **Inside/outside**: international relations as political theory. Cambridge: Cambridge University Press, 1983.

WEI, Lulu. Gatekeeping Practices in the Chinese Social Media and the Legitimacy Challenge. Em: **The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance**, editado por Uta Kohl, 69-80. Cambridge: Cambridge University Press. 2017.

WINTOUR, Patrick. Europe divided on Huawei as US pressure to drop company grows. **The Guardian UK.** Disponível em: https://www.theguardian.com/technology/2020/jul/13/europe-divided-on-huawei-as-us-pressure-to-drop-company-grows Acesso em: 22/03/2021

WU, Debby; KING, Ian; LEONARD, Jenny. 2022 US Quietly Tightens Grip on Exports of Chipmaking Gear to China. **Bloomberg**. Disponível em: https://www.bloomberg.com/news/articles/2022-07-29/us-pushes-expansion-of-china-chip-ban-key-suppliers-say?leadSource=uverify%20wall Acesso em: 15 de janeiro de 2023.

YERGIN, D. **O petróleo. Uma história mundial de conquista, poder e dinheiro**. Rio de Janeiro: Paz e Terra, 1993. 932p

ZHAO, Zhongxiu et al. China's industrial policy in relation to electronics manufacturing**. China & World Economy**, v. 15, n. 3, p. 33-51, 2007.

ZUBOFF, S. **A Era do Capitalismo de Vigilância:** a luta por um futuro humano na nova fronteira do poder. 1ª ed. Rio de Janeiro: Intrínseca, 2020.

ZUBOFF, S. **The Age of Surveillance Capitalism:** The fight for a human future at the new frontier of power. 1ª edição. New York: Hachette Book Group, 2019. E-book.

ZUBOFF, S. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F.; CARDOSO, B.; KANASHIRO, M.; GUILHON, L.; MELGAÇO, L. (Orgs.). **Tecnopolíticas da vigilância: perspectivas da margem**. 1ª edição. São Paulo: Boitempo, 2018.