

## A CHINA E A ECONOMIA POLÍTICA INTERNACIONAL DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Esther Majerowicz<sup>1</sup>

**Resumo:** Objetiva-se, aqui, analisar a posição da China na economia política internacional das TIC em relação aos EUA, com foco na disputa pelo 5G. Para tal, o artigo considera a concorrência no ecossistema de TIC, apoiado em relações estreitas entre estado e capital, sob três prismas: o econômico, o militar e o de vigilância internacional. Postula-se que a renovação da infraestrutura global de telecomunicações coloca em jogo a redefinição das fronteiras dos sistemas internacionais de vigilância e o reposicionamento das firmas de tecnologia e das economias no sistema industrial, enquanto consagra a infraestrutura civil crítica como um alvo central nos cálculos militares. Embora a China seja líder no 5G, os EUA detêm poder estrutural no ecossistema de TIC e podem obstruir seus avanços.

**Palavras-chave:** China. 5G. Tecnologias da informação e comunicação. Sistema industrial. Infraestrutura. Vigilância.

## CHINA AND THE INTERNATIONAL POLITICAL ECONOMY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

**Abstract:** We aim to analyze here China's position in the international political economy of ICT relative to the US. To this end, we consider competition in the ICT ecosystem – which is supported by close ties between the state and capital – under three dimensions: economic, military, and in international surveillance. We postulate that the global telecommunication infrastructure's renewal puts at stake the redefinition of boundaries between international surveillance systems and the repositioning of tech firms and national economies in the modern industrial system, while it consecrates critical civilian infrastructure as a central target in military calculations. Although China leads in 5G, the US has structural power in the ICT ecosystem, being able to obstruct China's advances.

**Keywords:** China. 5G, Information and communication technologies. Infrastructure. Industrial system. Surveillance.

## CHINA Y LA ECONOMÍA POLÍTICA INTERNACIONAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

**Resumen:** El objetivo aquí es analizar la posición de China en la economía política internacional de las TIC en relación con Estados Unidos, con un enfoque en la disputa 5G. Para ello, el artículo considera la competencia en el ecosistema de las TIC, sustentada en estrechas relaciones entre Estado y capital, bajo tres prismas: económico, militar y de vigilancia internacional. Se postula que la renovación de la infraestructura global de telecomunicaciones pone en juego la redefinición de las fronteras de los sistemas de vigilancia internacional y el reposicionamiento de las empresas tecnológicas y economías en el sistema industrial, al tiempo que consagra la infraestructura civil crítica como un objetivo central en los cálculos militares.

---

<sup>1</sup> Universidade Federal do Rio Grande do Norte, Departamento de Economia, Programa de Pós-Graduação em Economia, Natal, Rio Grande do Norte, [estherzinhamj@yahoo.com.br](mailto:estherzinhamj@yahoo.com.br), 0000-0001-6055-2788.

Aunque China es líder en 5G, Estados Unidos tiene poder estructural en el ecosistema de las TIC y puede obstaculizar sus avances.

**Palabras clave:** China. 5G. Tecnologías de la información y la comunicación. Sistema industrial. Infraestructura. Vigilancia.

## Introdução

As tecnologias da informação e comunicação (TIC) desenvolvidas a partir da microeletrônica e da computação surgiram como tecnologias americanas. Seu desenvolvimento foi, em larga medida, resultado das demandas militares e do suporte governamental dos EUA, tendo sido posteriormente difundidas para o setor civil, revelando sua natureza eminentemente dual<sup>2</sup>. O desenvolvimento das TIC possibilitou novos armamentos e a reestruturação organizacional, tática e estratégica militar, provocando uma Revolução nos Assuntos Militares, enquanto as indústrias e os produtos associados a essas tecnologias tornaram-se os setores mais dinâmicos da economia mundial nas últimas décadas. Ademais, o processo de desenvolvimento e difusão das TIC, capitaneado pelas grandes potências tecnológicas e seus grandes capitais, forjou uma ampla infraestrutura digital de vigilância internacional e de controle social das populações domésticas.

Do ponto de vista econômico, a centralidade do setor de TICs e de seus produtos manifesta-se em distintas dimensões, em especial na ascensão das empresas de tech às primeiras posições entre as maiores empresas do mundo em capitalização de mercado (PwC 2018). As TIC e seus produtos têm caráter-chave para a atual onda de modernização da indústria e serviços associados. Ademais, a indústria de TIC foi tanto viabilizadora quanto substrato do processo de fragmentação produtiva internacional nas últimas décadas, conformando as cadeias globais de valor, em larga medida uma história da indústria de eletrônicos.

A globalização produtiva das TIC, entretanto, foi controlada pelas economias desenvolvidas, respondendo tanto a medidas governamentais quanto às estratégias das empresas transnacionais (ETNs). Aqueles sub-setores, produtos e estágios produtivos de alto valor agregado associados ao controle e desenvolvimento tecnológico foram, em geral, preservados nas economias sede das ETNs, porque não apenas são esses os elementos que permitem altas margens de lucro e rendas tecnológicas, como também possibilitam vantagens militares e de vigilância.

A China realizou significativos avanços nos segmentos a jusante do moderno sistema industrial, que resultaram de suas elevadas ambições econômicas, militares

---

<sup>2</sup> Por exemplo, os casos da ARPANET e do NAVSTAR, que levariam à Internet e ao GPS.

e tecnológicas guiadas por políticas industriais, sua estratégia militar e a internacionalização das empresas chinesas (Autor, 2018). Os objetivos do país e seus avanços concretos desencadearam respostas dos EUA e aliados, consubstanciadas em uma retração da globalização por aqueles que previamente a capitanearam, particularmente os EUA. Essa retração é resposta ao acirramento da concorrência no mercado mundial, espalhando-se para os estágios de maior valor adicionado da produção industrial e para a determinação dos fluxos de rendas tecnológicas, mas principalmente pela busca de dominância nos novos campos de batalha da guerra contemporânea e nos sistemas internacionais de vigilância. O presente artigo tem como objetivo discutir e avaliar a posição da China na economia política internacional das TIC em relação aos EUA, focando na atual dinâmica da concorrência global em torno da implementação dos sistemas de telecomunicação sem fio de quinta geração (5G). Além dessa introdução, o artigo possui seis seções. A primeira discute as relações orgânicas entre Estado e capitais características do capitalismo contemporâneo no desenvolvimento das TIC, conferindo-as sua natureza civil-militar e caracterizando-as enquanto tecnologias de vigilância. A segunda aborda as TIC na constituição de sistemas de vigilância internacionais a partir do caso dos EUA, tal como revelado por Snowden, como marco para a concorrência entre distintos sistemas de vigilância internacional. Destacando as vantagens chinesas e da Huawei, a terceira seção trata da nova rodada de renovação da infraestrutura de telecomunicações que se aproxima com o 5G, enquanto a quarta postula tal renovação como uma fissura significativa no espaço da concorrência internacional entre capitais e Estados em distintas dimensões. A seção discute seu potencial impacto para o aprofundamento e espalhamento dos sistemas de vigilância das grandes potências, para o posicionamento das economias no sistema industrial e para a consagração da infraestrutura civil crítica como alvo central dos cálculos militares. A quinta seção aborda o poder estrutural americano no ecossistema de TIC, bem como sua alavancagem contra a China. A última seção é dedicada às considerações finais.

### **As relações orgânicas entre Estado e capitais no desenvolvimento das TIC**

Como em muitas outras indústrias tecnologicamente inovadoras e pioneiras, a indústria de TIC é estruturalmente dependente de ecossistemas de inovação dirigidos pelo estado e de suporte financeiro governamental para o desenvolvimento tecnológico, bem como de apoio estatal para a viabilização comercial de novos

produtos tecnológicos. Essa afirmação não implica que todo novo produto, inovação incremental e descoberta seja dependente do Estado, embora ela seja particularmente verdade para a emergência de tecnologias de uso geral como circuitos integrados e redes de computadores.

As TIC emergiram do complexo militar-acadêmico-industrial dos EUA (Medeiros, 2003). Foi por meio da definição de um conjunto de problemas e da busca por realizações específicas para melhorias em seu poderio militar que o estado americano mobilizou, coordenou e apoiou esforços coletivos concentrados em departamentos e agências governamentais, universidades e empresas privadas – simultaneamente perseguindo diferentes linhas de investigação para resolver e atingir seus requerimentos –, que as TIC surgiram. Com amplo financiamento e procura garantida pelo Estado, o desenvolvimento das TIC não foi restrito por razões de custos; e as máquinas desenvolvidas nesse processo (e.g. computadores, equipamentos de telecomunicações), bem como a maneira de empregá-las, resultaram das considerações e necessidades militares (Medeiros 2003).

O Estado não está apenas implicado na emergência de novas tecnologias que criam novos ramos industriais com suas correspondentes empresas líderes. O Estado também é fundamental para os grandes movimentos das últimas ao longo da fronteira tecnológica, para defender ou desafiar os incumbentes industriais, para dar apoio à expansão em mercados externos e para sustentar estratégias de catch-up. Essas não são características do assim chamado “socialismo de mercado” ou da propriedade estatal, elas descrevem relações orgânicas entre estados e capitais em uma época do capitalismo, inaugurada nas duas últimas décadas do século XIX, na qual a ciência se tornou “a última – e depois do trabalho a mais importante – propriedade social a tornar-se um adjunto do capital” (Braverman, 1998, p. 107).

Descrevendo essa passagem de períodos, Braverman (1998, p. 107-108) afirma: “inicialmente, a ciência nada custa ao capitalista visto que ele meramente explora o conhecimento acumulado das ciências físicas, mas, posteriormente, o capitalista sistematicamente organiza e controla a ciência, pagando pela educação científica, a pesquisa, os laboratórios, etc. com o grande produto social excedente que ou pertence diretamente a ele ou que a classe capitalista como um todo controla na forma de receita tributária”. Essas afirmações, ao lançarem luz sobre a natureza capitalista do estado, proveem inteligibilidade à razão pela qual sistemas nacionais de inovação dirigidos pelo Estado e movidos por seus requerimentos de defesa, concentrando recursos e impulsionando o sistema em direções específicas, são em

grande medida focados em tecnologias de “uso dual”, ou na busca da conversão dos desenvolvimentos tecnológicos militares para o emprego em esferas de acumulação capitalista mais amplas (e vice-versa, especialmente no caso de países distantes da fronteira tecnológica). Conseqüentemente, nesse caso, o estado não disputa o excedente com os capitalistas ao buscar seus objetivos militares, mas ele promove a acumulação de capital muito além da indústria de defesa estrita. Tal caracterização é verdadeira tanto para os EUA quanto para a China contemporânea<sup>3</sup>.

Não obstante, as formas particulares por meio das quais as relações orgânicas entre Estado e capitais assumem na produção de tecnologias e novos produtos variam entre estados nacionais distintos, que são emblematicamente divergentes nos casos da China e dos EUA, ou em diferentes momentos na trajetória de um país<sup>4</sup>. Nos EUA, Weiss (2014) argumenta que especialmente desde os anos 1980, o complexo-militar-industrial, tendo no seu centro grandes empreiteiras de defesa, deu lugar ao Estado de Segurança Nacional – não no sentido da primazia da segurança nacional para os estados, mas de uma empresa tecnológica, “um cluster particular de agências federais que colabora intimamente com o setor privado na busca de objetivos relacionados à segurança”, para o qual as empresas de alta tecnologia são fundamentais (Weiss, 2014, p. 4).

Nem as empresas privadas de alta tecnologia ocidentais, nem as chinesas podem ser contrapostas aos estados como uma solução para garantir a segurança e o direito à privacidade; elas estão todas imbricadas com seus estados nacionais e são estruturalmente dependentes dos amplos sistemas nacionais de inovação guiados pelo Estado, cujos objetivos primordiais no desenvolvimento das TIC são vantagens militares e de vigilância. O envolvimento de grandes empresas tecnológicas nos aparatos de vigilância doméstica e imperial não deveria ser visto como exceção, mas como o padrão, independentemente de suas declaradas estruturas proprietárias e de ligações mais ou menos formais com o Estado. Ademais, vigilância e/ou insegurança estão no coração dos modelos de negócios de diversas grandes empresas de tecnologia, como o Facebook, o Grupo NSO de Israel – que vende ferramentas de hackeamento para estados nacionais –, ou a HiKvision

---

<sup>3</sup> Diferentemente dos EUA, a China depende de sua capacidade de adaptar tecnologias usadas por empresas comerciais de países desenvolvidos para modernizar e fortalecer seu setor militar (Trobat e Medeiros 2014). Todavia, a busca do Estado chinês por atingir seus objetivos de defesa é importante para a capacitação dos capitalistas no setor civil na tarefa de absorção tecnológica, assim como para a provisão de demanda e de financiamento aos últimos. Em diversos casos, o Estado chinês assume diretamente a tarefa de acumulação de capital para além da indústria de defesa.

<sup>4</sup> Essas diferenças afetam a eficiência desses arranjos na produção tecnológica e de novos produtos, mas não afetam a natureza da relação entre Estado e capitais.

– a estatal chinesa que é a maior do mundo em equipamentos de vídeo para vigilância. Enquanto a visão econômica liberal não se sustenta quando confrontada com a realidade da produção tecnológica e o escopo das operações empresariais, ao propor o mercado como uma solução, a visão estado-cêntrica sobre a tecnologia e inovação não nos leva a nenhum lugar melhor.

Essa última visão definitivamente tem o mérito de esclarecer o papel do Estado no desenvolvimento tecnológico e as relações entre o setor público e o privado nos sistemas de inovação por meio de análises histórico-concretas. Mazzucato (2014) é uma expoente da abordagem estado-cêntrica, com importantes investigações sobre muitos desenvolvimentos tecnológicos particulares e suas conversões em produtos comerciais por meio de arranjos e configurações entre o setor público e o privado nos EUA. Sua visão, todavia, apela para um conceito de Estado que busca interesses gerais, consubstanciados no “bem nacional”<sup>5</sup>: “o que temos é um caso de Estado direcionado, proativo, *empreendedor*, capaz de assumir riscos e criar um sistema altamente articulado que aproveita o melhor do setor privado para o bem nacional em um horizonte de médio e longo prazo” (Mazzucato, 2014, para 10.32).

Esse estado, movido pelo “bem nacional” – que no caso de países imperialistas como os EUA e o Reino Unido, os principais estados nacionais tratados por Mazzucato, pode não ser o “bem do resto do mundo” – é em ampla medida autônomo da sociedade. Apenas em casos particulares de falha (de humor), o estado pode ser “submetido” por “interesses privados”: “De fato, quando não se mostra confiante, o mais provável é que o Estado seja ‘submetido’ e se curve aos interesses privados. Quando não assume um papel de liderança, o Estado se torna uma pobre contrafação do comportamento do setor privado em vez de uma alternativa real” (Mazzucato 2014: para 9.26). Ainda que Mazzucato reconheça a imbricação entre os setores militar e civil no sistema nacional de inovação e para o desenvolvimento das TIC, a autora “foca apenas nos aspectos ‘positivos’ da inovação e iniciativas estatais, sem mencionar a evolução das tecnologias militares e de vigilância [...] Certamente armas nucleares, urânio enriquecido e drones também

---

<sup>5</sup> “A falta de análise das relações capitalistas de produção em Mazzucato, na verdade, pavimentava uma visão do Estado como uma entidade externa, super-societária, representando o interesse ‘público’ e ‘coletivo’, incluindo assim os interesses dos trabalhadores também. A consequência disso é que os trabalhadores e o trabalho desaparecem completamente da sua análise. Incorporando o processo de inovação na produção capitalista e nas relações de trabalho levantaria as questões de ‘quem controla’ o processo de inovação e com ‘quais objetivos’.” (Pradella 2016: 6, tradução nossa).



precisam ser levados em conta se formos devidamente avaliar o caráter do estado empreendedor” (Pradella 2016: 8).

O estado capitalista somente pode ser visto como uma alternativa real ao desenvolvimento tecnológico liderado por capitais individuais, se se abstraírem a natureza do Estado e os objetivos que informam os estados e os capitais no desenvolvimento, desenho e uso da tecnologia. A tecnologia não é neutra e não pode ser vista como um mero instrumento aberto a servir aos propósitos dos usuários (Feenberg, 2006). Nas TIC, diversos casos caracterizam essa não-neutralidade da técnica, como, por exemplo, quando cavalos de troia são inseridos no desenho/manufatura de chips para que esses se comportem como artefatos técnicos de vigilância de terceiros ou quando a Agência Nacional de Segurança dos EUA (National Security Agency, NSA) introduz backdoors nos padrões técnicos. Snowden revelou que, em 2006, a NSA desenvolveu backdoors no próprio padrão criptográfico internacional: “o algoritmo falho foi padronizado pela ANSI e, subsequentemente, pela NIST e ISO e foi implementado em hardware da internet e dezenas de bibliotecas de software” (Rogers e Eden 2017, p.6). Consequentemente, a tecnologia não foi um instrumento neutro aberto à “soberania do usuário”, que decidiria proteger ou não sua privacidade; antes, o desenho da tecnologia<sup>6</sup> realizado pelo Estado determinou que todos ao redor do mundo utilizando esse padrão não teriam o direito à privacidade, especificando o conteúdo social dessa tecnologia como uma tecnologia americana de vigilância das comunicações.

Aqueles que especificam os objetivos do desenvolvimento tecnológico sabem muito bem que a tecnologia não é neutra; essa é a razão pela qual os estados nacionais estão revelando crescente desconfiança na aquisição de artefatos técnicos estrangeiros para implementar em seus sistemas de informação e comunicação, particularmente em suas infraestruturas. Destarte, deve-se questionar quais seriam os objetivos do estado capitalista na liderança do desenvolvimento tecnológico, liderança que é amplamente respaldada pela literatura acadêmica a respeito dos sistemas nacionais de inovação. É o Estado uma real alternativa aos

---

<sup>6</sup> “Os valores de um sistema social específico e de suas classes dominantes são instalados no próprio desenho dos procedimentos racionais e nas máquinas mesmo antes de elas terem objetivos específicos designados. A forma dominante de racionalidade tecnológica não é nem a ideologia (uma expressão discursiva do interesse de classe), nem o reflexo neutro de leis naturais. Mais apropriadamente, ela está em uma interseção entre a ideologia e a técnica onde os dois se juntam para controlar os seres humanos e os recursos em conformidade com aquilo que eu irei chamar de “códigos técnicos”. A teoria crítica mostra como esses códigos invisivelmente sedimentam valores e interesses em regras e procedimentos, dispositivos e artefatos que tornam rotineira a busca de poder e de vantagem pela hegemonia dominante” (Feenberg 2006: 14-15).

capitais individuais? Na medida em que esse age mais eficientemente que capitais individuais, como uma espécie de capitalista coletivo, a resposta deve ser afirmativa. Todavia, o que é concretamente o “papel visionário que assume riscos corajosamente” (Mazzucato 2014) do estado nacional capitalista? Que visões ele guarda a respeito do “bem nacional”?

No domínio das TIC, a visão que assumiu riscos foi primordialmente a de aumentar o poderio militar, tal como no desenvolvimento de armas para matar populações estrangeiras sem a necessidade de perder seus operativos humanos, como munições de precisão; de aumentar o controle sobre a população trabalhadora, com a vigilância e o controle remoto dentro e fora do processo de trabalho; de abrir novas esferas de acumulação de capital, permitindo a mercantilização de crescentes aspectos da vida social. Não houve nada de inevitável na forma pela qual as TIC se desenvolveram como um massivo aparato de vigilância e guerra contra as populações e como um potencializador da exploração e precarização do trabalho, essa apenas foi a visão que o Estado e os capitalistas tiveram para seu desenvolvimento. Orientado por esse mesmo conteúdo visionário, o desenvolvimento do aparato de TIC está na iminência de sofrer um salto qualitativo com a implementação do 5G.

### **As TIC na constituição de sistemas de vigilância internacionais: emergência americana e concorrência internacional**

Os EUA têm alertado seus protetorados militares e seus aliados sobre potenciais ameaças à segurança nacional colocadas pelo crescente papel da China nas TIC, particularmente nos equipamentos de 5G. Os EUA afirmam que a Huawei, a ZTE e outras empresas chinesas possuem laços estreitos, ainda que obscuros ou informais, com o partido-estado, particularmente com o Exército de Libertação Popular, e que elas poderiam cooperar ou serem compelidas legalmente a colaborar com o partido-estado em seus objetivos políticos e militares, bem como em espionagem industrial. Em sua defesa, a China enfatiza a ausência de provas incontestes de que suas empresas estejam envolvidas em tais tipos de atividades.

Em 2019, a Huawei e suas subsidiárias foram adicionadas à “lista de entidades” do Escritório da Indústria e Segurança do Departamento de Comércio dos EUA (Bureau of Industry and Security, BIS), ficando barradas de realizar



negócios com empresas americanas ou comprar produtos com tecnologias americanas sem aprovação oficial do estado (BIS, 2019, 2019a). O banimento foi justificado pelo argumento de que “os adversários estrangeiros estão crescentemente criando e explorando vulnerabilidades em tecnologias e serviços de comunicações e informações, que armazenam e comunicam vastas quantidades de informações sensíveis, facilitam a economia digital e sustentam infraestrutura crítica e serviços vitais de emergência” (Trump 2019). Ainda, de acordo com a justificativa, “a aquisição irrestrita ou uso” dessas tecnologias e serviços provenientes de adversários estrangeiros aumentaria a capacidade dos últimos de criar e explorar essas vulnerabilidades, de forma a criar ameaças não apenas à segurança nacional, como também à política externa e à economia dos EUA (Trump 2019).

Não obstante, pode-se argumentar que essas declarações dos EUA estão mal colocadas, uma vez que descrevem características constituintes das relações orgânicas entre capitais e estado no desenvolvimento e operação das TIC em economias capitalistas modernas. Elas descrevem, de forma especialmente adequada, o sistema internacional de vigilância dos EUA.

#### *A lógica do sistema internacional de vigilância dos EUA*

As revelações de Snowden mostraram como o aparato de TIC, abrangendo hardware, software, serviços e infraestrutura foi desenhado e/ou usado por agências governamentais e empresas dos EUA como uma estrutura de controle social doméstico e de poder imperial, contra não apenas atores estatais, mas também massas de cidadãos estrangeiros. Snowden revelou que o sistema de vigilância internacional dos EUA, em cooperação com os demais Cinco Olhos (agências de inteligência da Austrália, Reino Unido, Nova Zelândia e Canadá), operava em todas as distintas camadas do sistema de telecomunicações: da camada física, com o grampo de cabos de fibra óptica submarinos por meio da colaboração com as empresas comerciais operadoras dos cabos, tais como as “parceiras interceptadoras” BT, Vodafone Cable e Verizon Business (Guardian, 2013a, 2013b); passando pela cooperação com operadoras de telecomunicação, tal como a AT&T, para acoplar equipamentos de vigilância em roteadores e switches da empresa e redirecionar os dados para a NSA (Gallagher e Moltke, 2016); até a camada de aplicações, em parceria com os provedores de serviços de internet (e.g. Google, Facebook, Microsoft, Apple) no quadro do PRISM (NSA, 2013).

As agências de inteligência dos EUA atuaram nos órgãos de padronização técnica internacionais para inserir vulnerabilidades nos próprios padrões

criptográficos internacionais, bem como interceptaram e/ou receberam rotineiramente hardware americano para exportação, fisicamente inserindo implantes maliciosos que criavam backdoors em roteadores e switches da Cisco (Rogers e Eden, 2017; Greenwald 2014, p. 169). No caso da China, a NSA, entre outras ações, buscou criar vulnerabilidades nos produtos Huawei para ter acesso às comunicações que os atravessavam ao redor do mundo (NSA, 2014) e acessou “o arquivo de email, mas também os códigos fonte secretos de produtos Huawei individuais” (Spiegel, 2014)

A sofisticação, amplitude e os detalhes dessa estrutura e suas operações podem deixar-nos perplexos, mas o fato de que elas existam não deveria, pois são manifestações do desenvolvimento tecnológico dirigido pelo estado para atingir objetivos essenciais aos estados nacionais há muito trazidos à luz por Maquiavel, nomeadamente, a submissão dos governados e a submissão de seus pares. O direito humano à privacidade e o respeito à soberania nacional são meros componentes retóricos das políticas de estados com o poder de desenvolver e implementar as TIC mundialmente. As razões que compeliram a formação do sistema internacional de vigilância dos EUA, em cooperação com os Cinco Olhos, não foram limitadas aos motivos já ampla e escorregadiamente definidos como de “segurança nacional”. Os motivos foram também políticos, econômicos e tecnológicos, entre outros.

Ademais, a espionagem industrial foi planejada e executada pelos Cinco Olhos<sup>7</sup>. Por exemplo, foi planejada para um possível cenário em 2025, no qual os EUA poderiam perder a liderança tecnológica e em inovação, tanto se um bloco de estados “pudesse negar acesso a tecnologias emergentes chave”, quanto se “a capacidade tecnológica de corporações multinacionais estrangeiras superassem aquela das corporações dos EUA” (ODNI, 2009, p. 12). A comunidade de inteligência dos EUA aventava a necessidade de construir uma “proteção estratégica” de “aquisição tecnológica por todos os meios”, no qual “empregaria agressivamente um mix de meios abertos, penetração clandestina e táticas de contra-inteligência para lidar com a severa erosão tecnológica dos EUA vis-à-vis competidores em quase paridade e corporações globais” (ODNI, 2009, p. ii).

O objetivo-síntese da NSA de “adquirir os dados de SIGINT [inteligência de sinais] que nós precisamos vindos de qualquer um, a qualquer momento, em

---

<sup>7</sup> Por exemplo, o Reino Unido e os EUA espionaram empresas de telecomunicações alemãs para identificar “as futuras tendências tecnológicas nos seus setores de negócios” (Poitras et al., 2014).

qualquer lugar” (NSA, 2013a) implicava que os alvos<sup>8</sup> e os métodos de coleta fossem variados, guiados para a produção de pontos de exploração e vulnerabilidades redundantes e não por uma lógica de otimização de custo-benefício. Operando sob a diretriz “colete tudo” (Greenwald, 2014), a natureza do sistema internacional de vigilância dos EUA definiu o padrão para a concorrência internacional dos sistemas de vigilância para qualquer grande potência tecnologicamente capaz.

O mesmo imperativo de coleta indiscriminada de dados também se afirmou para as grandes empresas de TIC, ainda que sob outras lógicas. A coleta massiva de dados permitiu que a Google e o Facebook se tornassem gigantes mundiais, auferindo grandes massas de lucro por meio da otimização de um modelo de publicidade customizado que reduz os custos e aumenta a eficácia da publicidade, ao mesmo tempo em que começaram a utilizar essa mesma massa de dados para treinar algoritmos de inteligência artificial, cujos serviços passam a ser vendidos para terceiros (Robinson, 2015; Husson, 2018). Contando com tecnologias desenvolvidas pelo estado americano, elas coletavam dados, auferiam grandes lucros e disponibilizavam tais dados para as agências de inteligência dos EUA.

O acesso a massas de dados por tais agências também serviu para que elas treinassem seus próprios algoritmos de vigilância como, por exemplo, algoritmos de reconhecimento de voz de ponta, desenvolvidos muito antes da Siri e da Alexa, por meio de contratos da NSA com os laboratórios do MIT/Lincoln (Cusmariu, 2006; Kofman, 2018). O desenvolvimento algorítmico no contexto dos avanços em inteligência artificial pós-2010 podem aumentar sobremaneira a capacidade de processar os dados captados pelos sistemas de vigilância, ajudando em problemas do tipo encontrado na operação contra a Huawei, na qual a NSA declarava que “nós atualmente temos bom acesso e tantos dados que nós não sabemos o que fazer com eles” (Spiegel, 2014). Esses algoritmos aproximariam a NSA de um objetivo central posto para o sistema internacional de vigilância dos EUA, isto é, de “por meio de espionagem avançada e automação, dramaticamente aumentar o domínio sobre a rede global” (NSA, 2013a). Há, como ressalta Morozov (2018), uma divisão de tarefas entre o setor privado e o Estado americano nas atividades de vigilância.

---

<sup>8</sup> O programa BLARNEY, por exemplo, teve entre seus alvos “o FMI, o Banco Mundial, o Banco do Japão, a União Europeia, a ONU e ao menos 38 países distintos, incluindo aliados dos EUA, tais como Itália, Japão, Brasil, França, Alemanha, Grécia, México e Cyprus” (Gallagher e Moltke 2016).

As “parcerias estratégicas” da NSA com ETNs americanas vão muito além daquelas empresas às quais a coleta de dados indiscriminada era vital para o modelo de negócios e para os lucros derivados desses, embora possam ter acesso e/ou oferecer acesso a grandes massas de dados. Slides da NSA afirmavam a existência de mais de 80 parcerias corporativas estratégicas nos distintos segmentos do ecossistema de TICs (Greenwald, 2014, p. 114). A cooperação entre as ETNs e a NSA na conformação e operação do sistema de vigilância internacional dos EUA ocorreu tanto de forma voluntária como compulsória, obrigadas por “ordens legais de vigilância” (Timberg e Gellman, 2013). Essa colaboração também envolvia vastos recursos monetários pagos pelo governo a muitas das empresas envolvidas, o que pode ensejar a cooperação para além do estritamente necessário devido à busca de lucros por meio da monetização dos serviços de vigilância prestados (Timberg e Gellman 2013). Estimava-se, à época das revelações de Snowden, que o setor privado absorvia por meio de contratos e pagamentos 70% do orçamento dos EUA de inteligência nacional (Shorrock *apud* Greenwald 2014).

Ademais, é preciso considerar uma característica essencial das tecnologias que sustentam essas operações de vigilância: “em questões de infraestrutura digital, a política interna também é política externa” (Morozov, 2018, p.124). Uma vez descobertas as vulnerabilidades introduzidas por um estado ou firma na estrutura digital, elas tornam-se exploráveis por terceiras partes para múltiplos objetivos. A consideração de que a estrutura de vigilância em TIC é a um só tempo doméstica e internacional tem sido constantemente reconhecida pelos EUA e pela China em suas políticas. Enquanto os EUA proibiram a aquisição de certos produtos de firmas chinesas e a realização de investimentos chineses em empresas de alta tecnologia americanas, a China busca expurgar tecnologia dos EUA de setores institucionais e econômicos chave, promovendo tecnologias “seguras e controláveis”.

Apesar desse reconhecimento concreto, ironicamente, os EUA e a China encontram-se em um “negacionismo antagônico” a respeito do caráter de suas infraestruturas digitais enquanto estrutura de controle social e de poder imperial. Após as evidências concretas a respeito do seu sistema de vigilância internacional, os EUA esforçam-se para negar que tenham usado essa estrutura para controle social doméstico<sup>9</sup>. Entrementes, a China abertamente implementa sua estrutura digital para controle social doméstico, mas nega que a usaria para vigilância

---

<sup>9</sup> Ver Greenwald (2014) para uma discussão sobre a vigilância das comunicações domésticas.

internacional. Ainda que não existam provas indiscutíveis sobre o envolvimento de firmas chinesas em vigilância internacional, os EUA já demonstraram o poder que se pode obter da infraestrutura e dos serviços de TIC.

Assim, pela compulsão das dinâmicas de acumulação de poder e capital pelos estados nacionais e seus grandes capitais, presume-se que esses imperativos far-se-ão presentes na atuação da China e de suas empresas. Ademais, na China, também há uma divisão de tarefas entre partido-estado e setor privado na constituição de sua estrutura de controle social doméstico de TIC, que é de grande importância econômica e tecnológica para a internacionalização e a posição das empresas chinesas de TIC no mercado mundial.

Enquanto alguns defendem a posição dos EUA devido aos seus supostos “valores democráticos”, outros apoiam a China pelos alegados comportamento “anti-imperialista” e “economia socialista de mercado”. Além das inadequações de tais caracterizações, enquadrar a questão como tal perde de vista que o novo salto no desenvolvimento das TIC está se desdobrando como um meio pelo qual estados e corporações buscam não só vantagens na concorrência entre pares, mas também aumentar o controle e a dominação sobre os trabalhadores e os povos. Os últimos estão entre os próprios motores dessa competição, a despeito dos estados e capitais que emergirão como os mais favorecidos na corrente reconfiguração de poder e riqueza mediada pelo desenvolvimento das TIC. Conforme as TIC desenvolvem-se com o fito de controle social e vigilância difusa pelos estados em aliança com suas Big Tech, o escopo para distinções relevantes entre democracia burguesa e autoritarismo reduz-se significativamente. Com a postulação do 5G, viabilizando a “inteligentização” em rede do tecido produtivo e urbano e da esfera doméstica, a diretriz “colete tudo” adquire uma nova dimensão.

### **O 5G e a vantagem chinesa**

A renovação da infraestrutura global de telecomunicações por meio da implementação do 5G será um empreendimento tecnológico complexo e caro, cuja realização deverá levar mais de uma década (Triolo e Allison, 2018). Além dos impactos macroeconômicos da construção da infraestrutura de 5G em si e seus desdobramentos para o posicionamento global dos fornecedores de equipamentos, a renovação da infraestrutura de telecomunicações global coloca em questão efeitos econômicos de longo prazo.

O 5G promove a tendência a implementar a chamada Internet das Coisas (Internet of Things, IoT), que consiste na implementação de sensores e circuitos integrados (chips) nos objetos. Os sensores transformam os sinais analógicos em digitais, que os chips armazenam, processam e modulam/desmodulam em sinais de rádio frequência que são comunicados por antenas e conectados à infraestrutura de telecomunicações, permitindo utilização de dados em rede e processamento/armazenagem na nuvem. A peculiaridade do 5G é que ele é o primeiro sistema de telecomunicações intencionalmente desenvolvido para prover suporte a quantidades massivas de dispositivos conectados, a sistemas industriais e a aplicações de missões críticas.

As novidades da implementação do 5G relacionam-se principalmente com a flexibilidade da infraestrutura de comunicações para lidar com distintas necessidades dos usuários por meio do fatiamento da rede em três grandes segmentos, proporcionando serviços distintos. Esses são: o aumento substancial da velocidade de conexão; baixa latência e ultra confiabilidade da conexão – em termos práticos, a conexão é “instantânea” e sem intermitência, possibilitando o desenvolvimento de aplicações de missões críticas (e.g. veículos autoguiados, cirurgias à distância); e comunicação massiva entre máquinas, permitindo o suporte massivo de dispositivos de baixos custo e potência conectados à rede, fundamental para smart cities e IoT (Lee e Chau, 2017; Brake, 2018; Triolo e Allison, 2018).

O fatiamento da rede é viabilizado por uma combinação de tecnologias – redes definidas por software e de virtualização da função da rede –, que “permite estruturas tradicionais de uma rede de telecomunicações serem desmembradas em elementos customizáveis que podem ser combinados em distintas formas usando software” (Lee e Chau, 2017, p.22). A complexidade em definir essas funções e alocar os recursos será administrada por inteligência artificial (Triolo e Allison, 2018).

Uma das tecnologias que garante essas aplicações e define o 5G é a interface de rádio das estações de base do sistema de telecomunicações, denominada New Radio, que permite a comunicação dessas com os dispositivos da periferia da rede (e.g. smartphones, carros, objetos) (Brake 2018). Haverá duas etapas na implementação do 5G. Na primeira, o 5G “non-standalone” (não-autônomo), a New Radio será acoplada à infraestrutura existente de 4G (LTE), possibilitando o aumento da velocidade de conexão. Na segunda, o 5G “standalone” (autônomo), a renovação completa da infraestrutura de telecomunicações será



necessária para prover a baixa latência e ultra confiabilidade e a comunicação massiva entre máquinas.

O 5G autônomo redefinirá a relação entre as redes central e de acesso por rádio. Atribuições até então restritas à central serão também delegadas à periférica, transferindo boa parte da computação para a periferia (edge-computing) com o fito de reduzir o tempo de transmissão e a congestão da rede, o que torna o conteúdo das comunicações sensível à rede de acesso por rádio<sup>10</sup> (Lee e Chau, 2017). A baixa latência/ultraconfiabilidade e a conexão massiva de dispositivos serão alcançadas por meio de uma arquitetura pulverizada de pequenas estações de celular, cada uma com baixa cobertura, e da expansão do backhaul de fibra ótica, tornando a implementação d 5G “standalone” uma caríssima e complexa operação.

#### *A posição da China no 5G e as vantagens da Huawei*

A China detém a primeira e a quarta maiores empresas de equipamentos de telecomunicações do mundo, a Huawei e a ZTE, que detinham aproximada e respectivamente 28% e 8% do mercado mundial em 2018 (Pongratz, 2019). No 4G, ambas haviam provido significativa parte dos equipamentos para a rede de acesso por rádio, além de equipamentos para a rede central. Atualmente, para a implementação do 5G, apenas a Huawei oferece em grande quantidade os equipamentos necessários para montar a rede de acesso por rádio, que passa a ser também responsável pela computação na periferia da rede. Aqueles que não comprarem Huawei podem atrasar em ano ou mais a implementação do 5G (Kleinhans 2019). E, central para as operadoras de telecomunicações, a Huawei oferece o menor preço para uma infraestrutura cara: suas redes de telecomunicações custariam entre 20% a 30% mais barato que aquelas providas por outros produtores (Lewis 2018, 2018a).

Nem a Cisco nem qualquer outra empresa americana proveem equipamento para rede de acesso por rádio, ao passo em que o da Huawei tem sido considerado tecnologicamente superior aos rivais<sup>11</sup>. As únicas alternativas à Huawei são os produtos da Nokia e da Ericsson (europeias), que não têm condições de suprir a demanda das grandes nações desenvolvidas rapidamente, e da Samsung. Ademais, muitos países europeus utilizaram intensivamente os equipamentos chineses na rede de acesso por rádio do 4G, ainda que determinados países tenham os proibido

<sup>10</sup> “Uma operadora móvel precisará abrir sua rede de acesso por rádio a desenvolvedores e provedores de conteúdo de terceiras partes” (Lee e Chau, 2017, p. 23).

<sup>11</sup> De acordo com o executivo-chefe de tecnologia e informação da BT, a tecnologia da Huawei estaria 18 meses à frente da Ericsson e da Nokia (Watson *apud* Pham 2019).

na rede central, de forma que, atualmente, ambas as empresas detêm 40% do mercado da União Europeia (Barzic 2019). De acordo com um relatório vazado do lobby GSMA, grupo que representa 750 operadoras móveis, o banimento dos produtos chineses na Europa elevaria os custos da rede 5G e atrasaria sua implementação, incrementando o gap europeu em relação aos EUA na penetração do 5G em mais de 15 pontos percentuais em 2025 (Barzic, 2019) e afetando o gap de produtividade entre eles .

Até meados de 2020, os avanços na implementação do 5G referiam-se ao 5G nonstandalone; todavia, os principais impactos do 5G devem-se ao standalone, para o qual as perspectivas originárias de implementação da rede comercial estavam previstas para 2025 nos EUA, Austrália, Japão, União Europeia, Coreia do Sul e Canadá (Triolo e Allison 2018). Apenas a China previa essa implementação para 2020. Segundo, Triolo e Allison (2018, p.12), a China foi o país que teria dedicado mais esforços para preparar a implementação do 5G, com uma estratégia de “possibilitar que suas operadoras, particularmente a líder China Mobile, movam-se rapidamente para o 5G standalone, permitindo que a China ganhe valioso tempo na testagem e validação da tecnologia e dos modelos de negócios para aplicações avançadas que o 5G SA [standalone] irá viabilizar”.

As vantagens da China no 5G, especialmente emanadas da Huawei, e seus esforços para ser a primeira a implementar uma rede comercial de 5G standalone em grande escala proveriam inúmeras vantagens econômicas, tecnológicas e políticas ao país, além de impactos substanciais para a Huawei nos distintos segmentos do ecossistema de TIC em que opera, entre eles, smartphones, câmeras de vigilância, IoT, inteligência artificial, serviços na nuvem e cabos de fibra ótica.

### **O 5G e a fissura no espaço concorrencial internacional**

Os potenciais serviços a serem oferecidos pelo 5G standalone em larga escala, se realizados, farão que a renovação da infraestrutura de telecomunicações global seja uma possível brecha para o reposicionamento das empresas de tecnologia em aliança estreita com seus estados nacionais nos diferentes segmentos da indústria de TIC e para o reposicionamento das economias nacionais no sistema industrial como um todo. Esses potenciais rearranjos responderiam ao surgimento de novas indústrias e à renovação de indústrias tradicionais por meio das TIC, processo pelo qual as grandes empresas de tecnologia entram em segmentos industriais tradicionais disputando com seus incumbentes. Ainda que

essa última tendência já exista e venha atingindo distintos setores, o que se postula com o 5G é a aceleração e alargamento desse processo. Ademais, a difusão do 5G para a periferia capitalista ensejará o aumento da dependência, tecnológica e financeira, bem como por meio da expansão dos sistemas internacionais de vigilância. A provisão de recursos financeiros para a implementação do 5G na periferia constituirá uma esfera de concorrência em si entre as grandes potências e as economias desenvolvidas. A China intenciona alavancar esses potenciais na busca de seus objetivos de longo prazo (2049-2050) de tornar-se a líder entre as principais potências industriais e a líder mundial em ciência e tecnologia, bem como de consolidar-se como grande potência cibernética e possuir forças armadas de excelência mundial (State Council, 2006, 2015, 2015a; 2016).

Todavia, a viabilidade da implementação do 5G standalone em larga escala com cobertura nacional ainda não foi tecnicamente comprovada. De acordo com Fogarty (2019), na segunda etapa, “o 5G é mais uma declaração de direção do que uma tecnologia única”. Se tecnicamente realizável, tal implementação poderá demorar por distintos fatores, entre eles, as movidas geopolíticas e o debate sobre seus efeitos para a saúde humana (León, 2019). Ainda que muitas das aplicações que vêm sendo associadas ao 5G já existam, como educação à distância, automação industrial avançada e smart cities, o que os proponentes do 5G avaliam é que o nível de difusão e profundidade dessas aplicações será drasticamente ampliado, tornando possível, por exemplo, o uso de drones comerciais em larga escala e a aplicação difundida da realidade aumentada/virtual. Eles também afirmam que o 5G irá viabilizar aplicações de fato novas, como cirurgias remotas e veículos autônomos com elevado nível de automação por meio da comunicação entre veículos e entre veículo e infraestrutura (Delloite, 2018)<sup>12</sup>. Segundo Lewis (2018, p.5), “o 5G irá afetar as muitas indústrias que serão construídas em cima dele, da mesma forma em que a economia dos aplicativos foi construída sobre o 4G”.

A possibilidade de um salto qualitativo na difusão de semicondutores sobre a infraestrutura urbana, nos domicílios, nos transportes, nas infraestruturas críticas, na agricultura e na indústria abre espaço para novos modelos de negócios, novas plataformas e novas esferas de coleta de dados para o desenvolvimento de algoritmos de inteligência artificial, que dependem de massas de dados específicos. Existem significativas vantagens para o *first mover* na implementação da

---

<sup>12</sup> Não é certo que os mais altos níveis de automação demandarão alta conectividade (Delloite 2018).

infraestrutura de 5G standalone em larga escala ou escala nacional, impactando a competitividade nacional e o desenvolvimento tecnológico (Lewis, 2018a). Essas vantagens derivam de políticas domésticas e do mercado interno, que, uma vez alcançadas domesticamente, serão alavancadas para conquistar e/ou expandir-se nos mercados externos.

Se o 5G standalone em larga escala irá de fato tornar-se uma realidade ou não, a perspectiva dos potenciais de sua efetivação para as economias nacionais e grandes empresas impele-as a buscar o melhor posicionamento nessa concorrência. Ainda que existam questões de segurança nacional associadas ao 5G, existiria um alto impacto econômico de longo prazo em jogo para as economias caso o 5G “puro” se concretize, para além dos custos de implementação. Para os países que não têm condições de disputar o mercado de equipamentos de telecomunicações e construir suas próprias infraestruturas, banir a Huawei pode colocá-los em uma posição retardatária e desfavorável em diversos outros mercados, como em novos serviços de plataforma e veículos autoguiados, bem como atrasá-los na produção de distintas massas de dados para o desenvolvimento da inteligência artificial. Assim, a renovação da infraestrutura de telecomunicações global também abre uma brecha para o potencial reposicionamento das nações no sistema industrial como um todo.

#### *Vigilância e guerra*

Ao viabilizar a “inteligentização” em rede do tecido produtivo e urbano e da esfera doméstica, essas projetadas novas, profundas e difusas fontes de produção de dados com a postulação do 5G constituem novas avenidas para o controle e a vigilância. Elas tornam mais próximo da realidade o objetivo dos EUA de “integrar o sistema de inteligência de sinais em uma rede nacional de sensores que interativamente sentem, respondem e alertam uns aos outros em velocidade de máquina” (NSA, 2013a). A renovação da infraestrutura de telecomunicações global possibilitará o aprofundamento e extensão dos sistemas internacionais de vigilância contemporâneos das grandes potências, abrindo espaço para a redefinição de suas fronteiras. Adicionalmente, essa renovação consumará o status da infraestrutura crítica civil como um alvo central nos cálculos e estratégias militares. Tendo em vista que a condição de difícil atribuição e verificação de ataques no âmbito das TIC gera uma lógica na qual a confiança no produtor deve ser assumida, os imperativos da concorrência entre capitais e do poder econômico dos estados chocam-se com os imperativos de segurança nacional para todos aqueles estados incapazes de prover sua própria infraestrutura de telecomunicações para o 5G.

A difusão das TIC na infraestrutura civil crítica já tornou essa alvo privilegiado de ataque nas estratégias militares e armamentos modernos, por meio do comprometimento dos sistemas de informação – de seus componentes elementares de hardware aos softwares – que garantem sua operação. A nova onda de modernização industrial, urbana e de infraestrutura viabilizada pelas TIC aumenta a eficiência dessas estruturas, ao mesmo tempo em que eleva suas vulnerabilidades (Autor, 2018). O sistema de telecomunicações ao qual se acoplam essas estruturas afirma-se como um sistema de sistemas, do qual passam a depender mais profundamente a gestão dos sistemas de eletricidade, água, esgoto, trânsito, etc. O sistema de telecomunicações torna-se a infraestrutura crítica por excelência, ao lado do sistema de eletricidade (Kleinhans, 2019). Ainda que muitas unidades produtivas críticas tenham sistemas de TIC dedicados, como plantas nucleares e de energia, grande parte do aparato produtivo<sup>13</sup> será acoplada ao 5G das operadoras e à Internet. Ademais, sistemas dedicados de TIC não são imunes a ataques, como revelou o malware Stuxnet, que atingiu o sistema de controle industrial da planta Natanz de enriquecimento de urânio do Irã (Langner, 2011).

A renovação da infraestrutura de telecomunicações implicará na colocação de novos equipamentos de rede, como células pequenas, switches e roteadores. De acordo as autoridades chinesas, os riscos potenciais associados à compra pelas operadoras de telecomunicações de produtos e serviços de rede incluiriam: i) o equipamento de infraestrutura informacional crítica parar de funcionar ou executar normalmente sua principal função; ii) vazamento, perda, corrupção ou remoção para fora do país de um grande volume de dados importantes e pessoais; iii) ameaças de segurança na cadeia de fornecimento de “proteção às operações, suporte técnico, atualizações e substituição do equipamento da infraestrutura de informação crítica” (CAC, 2019). Outros riscos à segurança nacional são elencados tais como “a possibilidade de que a infraestrutura crítica de informação possa ser controlada ou que a continuidade dos negócios possa ser prejudicada”; o comprometimento da cadeia de fornecimento de produtos e serviços “incluindo a possibilidade de comprometimento devido a fatores não-técnicos como política, diplomacia e comércio”; e “o impacto na indústria de defesa ou indústrias e tecnologias relacionadas à infraestrutura informacional crítica” (CAC, 2019).

---

<sup>13</sup> “Como a maioria das redes industriais e de automação era fisicamente isolada, a segurança não era um problema. Isso mudou quando, no início dos anos 2000, as redes industriais foram abertas à Internet pública.” (Antón et al 2017)

Na prática, o 5G implicará na renovação de toda as camadas a montante do sistema de telecomunicações. Haverá a vasta expansão dos cabos de fibra ótica, incluindo aqueles submarinos, uma vez que o volume de dados em trânsito será vertiginosamente acrescido, o que coloca outras rivalidades às operações de vigilância e imperativos de segurança. O grampo nos cabos de fibra ótica submarinos teve um papel central nas operações de vigilância internacional dos Cinco Olhos, sendo amplamente utilizado pelo Reino Unido, cuja posição estratégica tornava-o central para a junção à terra de muitos dos cabos que ligavam a Europa (Akita, 2019). Assim, a geografia da rede de telecomunicações que emergirá com a implementação do 5G e seus novos cabeamentos de fibra ótica internacionais e intercontinentais, isto é, a arquitetura global da infraestrutura de telecomunicações, é ela própria alvo de disputa.

Os EUA já estavam perdendo sua centralidade originária no tráfego mundial da Internet desde a virada do século XXI. Nas primeiras três décadas da internet, a maior parte do tráfego mundial passava pelos EUA, o que facilitava sobremaneira seu sistema de vigilância internacional (Markoff, 2008; Greenwald, 2014). Considerada pela NSA como uma “vantagem de campo doméstica” (Guardian, 2013), essa geografia foi explorada por meio da parceria com a AT&T, cuja “provisão de tráfego estrangeiro para estrangeiro foi particularmente importante para a NSA porque grandes porções das comunicações mundiais da Internet viajam através de cabos americanos” (Angwin et al., 2015). No final dos anos 1990, estimava-se que 70% do tráfego mundial ainda passasse pelos EUA, ao passo que, em 2008, esse número teria caído para 25% (Odlyzko *apud* Markoff 2008).

A China busca impedir que seu tráfego doméstico seja roteado por outros países<sup>14</sup>; enquanto busca rotear dados através dela, inclusive via Rota da Seda Digital<sup>15</sup>. De acordo com Shen (2018), a infraestrutura digital – que também inclui os cabos de fibra ótica e os links de satélite com o Beidou – é um componente crítico da estratégia chinesa de internacionalização através da Rota da Seda, uma vez que a China busca “construir uma autoestrada informacional global com a China no seu centro” (China Telecom, 2014 *apud* Shen, 2018, p. 2692). Além de equipamentos de telecomunicações, recentemente a China tornou-se uma importante fornecedora de

---

<sup>14</sup> “Se um usuário doméstico acessa a internet doméstica, seu tráfego não pode ser roteado para fora do país” (CAC 2019a)

<sup>15</sup> Por exemplo, por meio do Plano de Longo Prazo para o Corredor Econômico China-Paquistão, a China e o Paquistão implementaram um novo cabo de fibra ótica – que se aterra em Gwadar, onde um porto vem sendo desenvolvido pela Rota da Seda –, roteando fluxos de dados de e para o Paquistão pela China (Boni 2019; Page et al. 2019).



cabos de fibra ótica submarinos – mesmo que atrás dos EUA, Europa e Japão – por meio da Huawei Marine Networks, uma joint-venture criada em 2008 entre a Huawei (51%) e a britânica Global Marine (49%). A empresa expandiu-se inicialmente através de projetos de ligações curtas, especialmente no Sudeste Asiático e no Leste Russo, até 2018, quando completou o primeiro grande projeto ligando o Brasil a Camarões, tornando-se a primeira a conectar a África à América do Sul (Akita, 2019; Huawei Marine, 2018). Recentemente, a empresa tem destacado-se em inúmeros projetos na África, que “em larga medida espelham os investimentos em infraestrutura regional não digital” (Lee e Chau, 2017). Com a entrada Lista de Entidades dos EUA, a Huawei supostamente decidiu vender sua parcela na Huawei Marine para a chinesa Hengtong Optic-Eletric (Jiang, 2019).

Assim, a renovação da infraestrutura de telecomunicações ensejada pelo 5G abre espaço para a reconfiguração dos sistemas internacionais de vigilância e de suas fronteiras por meio do reposicionamento dos Estados com suas “parcerias corporativas estratégicas” nas camadas a montante do sistema de telecom. Nessas, grandes volumes de dados foram coletados pelo sistema de vigilância internacional dos EUA, orientado para “potencializar exclusivas parcerias corporativas chave para ganhar acesso a cabos de fibra ótica internacionais, switches e/ou roteadores de alta capacidade ao redor do mundo” (NSA *apud* Guardian, 2013c).

Correntemente, analistas apontam que seria difícil redirecionar e copiar todos os dados que atravessam os equipamentos de telecomunicações sem detecção<sup>16</sup>; o mesmo ocorreria no caso dos cabos de fibra ótica (Page et al., 2019). Ademais, esses procedimentos, conhecidos como “extração de dados”, para serem úteis, devem quebrar a criptografia, ainda que possam se beneficiar da captura dos metadados. Embora existam meios mais simples e/ou mais baratos de coleta de dados específicos, para espionagem industrial, e de ataques (Kleinhans 2019), a lógica do sistema de vigilância implica na criação de vetores e pontos de exploração redundantes, enquanto os Estados buscam ativamente tornar a criptografia inócua.

A questão mais sensível e central em relação à infraestrutura de 5G parece derivar de sua postulação enquanto “sistema de sistemas”: ao desligar ou comprometer as operações parcial ou completamente do sistema de

---

<sup>16</sup> Isso é controverso. Para Botton e Lee (2018, p.4): “Esses tipos de ataques são de difícil detecção, já que a informação poderia ser extraída como tráfego normal de usuários ou incrustada em outro tráfego. Ataques ao RAN poderiam também levar a outras ameaças à segurança nacional, tais como obstrução de rádio ou permitir atores hostis adaptarem as estações de base para redirecionar, modificar ou duplicar o tráfego para uma rede sombra, enquanto parecem funcionar normalmente”.

telecomunicações em cenários de guerra, há a possibilidade de interromper os sistemas de gestão urbana, energia e industrial, dentre outros, potencialmente provocando caos urbano e colapso econômico. Destarte, os equipamentos de rede do 5G podem ser um vetor de ataque à infraestrutura civil crítica. O equipamento da Huawei e/ou de qualquer outro produtor podem ser comprometidos tanto na fabricação quanto posteriormente – por atualizações de software ou pelo recebimento/interceptação dos equipamentos por agências estatais (e.g. NSA e Cisco) – para criar vulnerabilidades ou interromper os serviços. Todavia, o 5G apenas consagra esse tipo de ataque contra ou por meio do sistema de informação e comunicação à infraestrutura civil crítica, que emergem anteriormente ao nível mais elementar dos circuitos integrados, seus *building blocks* (Chu, 2013).

Como os equipamentos da Huawei dependem significativamente de chips dos EUA, deve-se considerar a hipótese de um equipamento de telecomunicações ser um vetor de ataque de dois agentes, por exemplo, via atualização de software pela China e via cavalo de troia implantado no chip pelos EUA. Não se sabe se os EUA implementaram essa via de acesso, apenas que, de forma mais geral, por meio de ferramentas de exploração de redes de computadores, a NSA (2014) tentava atingir esse objetivo: “muitos dos nossos alvos comunicam-se por meio de produtos produzidos pela Huawei, nós queremos ter certeza que nós sabemos como explorar esses produtos – nós também queremos assegurar que nós retemos acesso a essas linhas de comunicação, etc”.

Tendo oportunidades para implementar backdoors ou kill switches indetectáveis que ficam dormentes até o considerado necessário, num cenário de acentuada rivalidade interestatal e intercapitalista, por que tal ator não o faria? A questão é que nem os EUA podem suprir os equipamentos da rede de acesso por rádio do 5G, nem podem afirmar que se pudessem não o utilizariam como vetor de vigilância ou de potencial ataque, como mostra o histórico de operações da sua comunidade de inteligência e a lógica a qual obedece, como revelado por Snowden.

No fundo, a segurança dessas infraestruturas implica o suprimento próprio. Nesse sentido, é possível compreender a delicada posição de países europeus como a Alemanha ou o Reino Unido, que, não tendo alternativas endógenas de suprimento, poderiam atrasar na entrada do 5G ao banir a Huawei. Esse atraso pode levá-los a uma perda de competitividade e poder econômico ainda maior no longo prazo, sem contar os efeitos econômicos de possíveis retaliações da China, como lembra Kleinhans (2019). A profundidade da racionalidade econômica para

aceitação dos equipamentos da rede de acesso por rádio da Huawei coloca-se como um fator central vis-à-vis a crescente pressão dos EUA sobre seus aliados.

### **O poder estrutural dos EUA no ecossistema de TIC e sua alavancagem contra a China**

Se houve uma resposta em geral rápida e homogênea das economias avançadas às tentativas de aquisição de empresas de tecnologia pela China, especialmente de semicondutores, o mesmo não ocorreu frente à pressão dos EUA sobre seus protetorados militares e aliados para banir os equipamentos de telecomunicações e produtos Huawei de seus mercados, particularmente no caso do 5G. Apesar do baixo nível de penetração dos smartphones Huawei nos EUA e da expulsão dos seus equipamentos de telecomunicações do mercado americano, a empresa tornou-se a primeira do mundo em equipamentos de telecomunicações e, no segundo trimestre de 2020, também em smartphones (Canalys, 2020). Esse quadro era inconcebível décadas atrás quando, “em muitos setores, o mercado doméstico americano era tão maior que outros mercados nacionais e formava uma tão grande parcela, por si mesmo, do mercado mundial” (Strange, 1987, p. 564). Foi a barganha pelo acesso ao mercado americano que sustentou o ajuste e as limitações impostas pelos EUA à indústria de TIC japonesa, nos anos 1980 (Autor, 2018). Todavia, o poder estrutural dos EUA no ecossistema de TIC que pode ser alavancado contra a China atualmente não se consubstancia por essa via, mas especialmente por seu domínio sobre a produção e o desenvolvimento das tecnologias fundamentais que sustenta esse ecossistema, os circuitos integrados e as máquinas que os produzem.

A China atualmente é uma grande produtora de produtos eletrônicos e de TIC e a principal importadora de circuitos integrados, expressando seu sucesso na fabricação desses produtos finais e simultaneamente seu atraso tecnológico e sua distância do estado da técnica na tecnologia de semicondutores (Autor, 2018). A China depende demasiadamente dos chips dos EUA e de seus aliados, apesar de seus avanços substanciais na indústria de semicondutores e políticas industriais. O caso Snowden colocou em evidência a vulnerabilidade chinesa em relação à integridade dos chips produzidos por rivais militares, particularmente os EUA, que estão difundidos sobre a infraestrutura civil crítica, a estrutura produtiva, os aparatos estatal e militar chineses. Não obstante, foi a vulnerabilidade do país em relação ao

suprimento de circuitos integrados que se fez sentir sistematicamente no período pós-Snowden por meio da alavancagem do poder estrutural americano no ecossistema de TIC, particularmente por meio das sanções à ZTE e à Huawei.

A dependência direta e indireta chinesa nos produtos e tecnologias americanas em circuitos integrados é o principal ponto de estrangulamento disponível aos EUA para retardar ou mesmo bloquear o sucesso chinês em outros segmentos das TIC, incluindo o 5G, e sua estratégia de modernização militar à luz da Revolução nos Assuntos Militares. O gap entre consumo e produção de circuitos integrados na China cresceu de U\$5,6 bilhões, em 1999, para U\$120,1 bilhões em 2014, quando começou a se reduzir com a nova rodada de política industrial na esteira das revelações do Snowden, totalizando U\$114,7 bilhões em 2016 (PwC, 2017). Apesar do crescimento significativo das firmas e da produção doméstica chinesa de circuitos integrados no século XXI, essa produção tem sido cronicamente insuficiente para atender sua demanda, particularmente na manufatura de chips.

Ademais, a fração do consumo chinês de chips suprida por produção doméstica depende de equipamentos e tecnologias dos EUA. Os EUA possuem empresas fabricantes de quase todos os equipamentos necessários para a manufatura de semicondutores, colocando sua importância como supridor direto para a indústria de semicondutores mundial e, em particular, chinesa: “as firmas estadunidenses como a AMAT, LAM, KLA e Teradyne têm parcelas de mercado elevadíssimas em muitos nichos de mercado. Não há linhas de produção na China que usem apenas equipamentos feitos na China, assim é muito difícil fazer qualquer chip sem equipamentos americanos” (Everbright Securities *apud* Williams 2019). Mesmo no segmento crítico de máquinas de litografia, no qual apenas empresas europeias e japonesas operam, a supridora líder, a holandesa ASML, beneficiou-se de transferência tecnológica dos laboratórios de defesa americanos para suas ferramentas exclusivas de luz ultravioleta extrema (Atta e Slusarczuk 2012). Destarte, a centralidade dos EUA para a produção de ponta em semicondutores e das máquinas que os produzem, bem como para o avanço da fronteira tecnológica nesses segmentos, torna-os capazes de intervir na rede de produção mundial (não apenas da produção americana) e ativar canais de bloqueio ao desenvolvimento da China em TIC, dada sua dependência crítica nesses segmentos industriais de base.

A estratégia americana de alavancar seu poder estrutural no ecossistema de TIC para obstruir os avanços chineses nos estratos superiores desse ecossistema, nomeadamente, os usuários de semicondutores, especialmente os equipamentos de

telecomunicações para o 5G, não ocorre sem contradições. Estima-se que 1,200 supridores americanos da Huawei seriam afetados pela entrada da empresa e suas subsidiárias na lista de entidades (Lucas et al., 2019). A complexidade do ecossistema de TIC, altamente globalizado, e a centralidade do mercado chinês para seus bens finais, intermediários e de capital inevitavelmente fraciona os interesses dos capitais americanos frente às empresas chinesas e à China, apresentando uma geometria de concorrência e complementaridade heterogênea e emaranhada, provocando resistências à estratégia do governo dos EUA de obstrução onde predomina a complementaridade.

### **Considerações finais**

Na atual época do capitalismo, a exploração da ciência por meio do avanço da fronteira tecnológica para a acumulação de capital – e mesmo a capacidade para adaptar tecnologias existentes que se aproximam da fronteira –, requer a mobilização de vastas massas do excedente social, o que torna essa exploração inexecutável sem a postulação do Estado capitalista. Tal afirmação se verificou tanto na emergência, quanto no desenvolvimento e difusão das TIC, nos quais a imbricação entre Estado e capitais não foram ocasionais, mas essenciais, constituindo relações orgânicas do capitalismo contemporâneo. Como um empreendimento que carrega os objetivos do Estado e do capital inscritos naquilo que são e naquilo que não são, isto é, em seu desenho e nas alternativas tecnológicas não desenvolvidas ou rejeitadas, as TIC desenvolveram-se como tecnologias para a dominação de povos estrangeiros, para o controle da população doméstica dentro e fora do processo de trabalho e para a mercantilização crescente de aspectos da vida social até então preservados dos circuitos de acumulação de capital. Ao mesmo tempo, sua difusão foi politicamente controlada para dar origem e comandar vastas parcelas do excedente social na forma de rendas tecnológicas.

Por essas razões, a reorganização em curso de poder e riqueza entre as grandes potências e seus grandes capitais no sistema interestatal capitalista, ensejada pela ascensão da China, passa centralmente pela disputa sobre o domínio das TIC e de sua produção. O debate contemporâneo sobre esse processo tem gravitado em torno de empresas chinesas específicas, acusadas pelos EUA de possuírem ligações com o partido-Estado e o setor militar e de engajarem-se em atividades de vigilância doméstica, dissimulando a natureza da concorrência em questão. Não se trata de quem tem pretensões ou não de poder controlar as

infraestruturas civis críticas estrangeiras quando julgar necessário e de implementar sistemas de vigilância internacionais, mas daqueles que terão o poder e domínio tecnológico suficientes para fazê-lo.

A perspectiva de renovação da infraestrutura global de telecomunicações abre uma fissura nesse espaço concorrencial, bem como nos distintos segmentos do moderno sistema industrial e do sistema industrial como um todo, que dá espaço para que ocorra um salto substancial no processo de reorganização de poder e riqueza entre as principais potências e seus grandes capitais. A China não apenas anteviu essa oportunidade como preparou-a e preparou-se para tal, com sucesso nos estratos superiores do moderno sistema industrial. Não obstante, o poder americano alicerça-se estruturalmente, embora não de forma exclusiva, no controle e domínio das tecnologias, máquinas e processos produtivos que são o fundamento tecnológico desse sistema. Esse domínio é exercido direta e indiretamente sobre a rede de produção mundial, não apenas pela capacidade produtiva dos EUA, mas principalmente pela centralidade de seu setor de defesa para o avanço da fronteira tecnológica nos fundamentos que sustentam o ecossistema de TIC.

Para os trabalhadores, todavia, pautar o debate meramente como uma rivalidade sino-americana constitui uma falsa dicotomia. Os capitais e estados engajados nesses processos têm os mesmos objetivos: um controle mais estreito sobre os trabalhadores tanto como produtores quanto consumidores em um cenário no qual a massa de trabalhadores do mundo se vê cada vez mais privada de direitos e destinada à precariedade. As infraestruturas críticas que sustentam suas vidas cotidianas tornam-se crescentemente vulneráveis às operações militares das grandes potências. Entrementes, os povos estão crescentemente opondo-se aos resultados do capitalismo neoliberal, enquanto aparatos de vigilância e guerra são confrontados por resistência interna e externa de whistleblowers e de movimentos sociais. O que concretamente emergirá das expectativas que o estado e o capital estão depositando na renovação da infraestrutura de telecomunicações será contingente na resposta das massas de trabalhadores ao redor do mundo.

## REFERÊNCIAS

AKITA, H. Undersea Cables: Huawei's Ace in the Hole. **Nikkei Review**, 28/5/2019.  
ANGWIN, J. et al. AT&T helped U.S. spy on Internet on a Vast Scale. **The New York Times**, 15 Ago, 2015.



ANTÓN, S. D. et al. Two Decades of SCADA exploitation: a brief history. **2017 Conference on Application, Information and Network Security**, Miri, 2017.

Atta, R. V.; Slusarczyk, M. M. G. The Tunnel at the end of the light: the future of the U.S. Semiconductor Industry. **Issues in Science and Technology**, 28 (3), 2012.

BARZIC, G. Europe's 5G to Cost \$62 Billion More If Chinese Vendors Banned: telcos. **Reuters**, 7 Junho, 2019.

BONI, F. Protecting the Belt and Road Initiative: China's Cooperation with Pakistan to Secure CPEC. **Asia Policy**, 26 (2), 2019, p. 5-12.

BOTTON, N.; LEE-MAKIYAMA, H. 5G and National Security: After Australia's Telecom Sector Security Review. **ECIPE Policy Brief**, n. 8, 2018.

BIS - Bureau of Industry and Security of the US Department of Commerce. Addition of entities to the Entity List. **The Federal Register**, 84 (98), 2019, p. 22961-22968.

BIS. Addition of certain entities to the Entity List and revision of entries on the Entity List. **The Federal Register**, 84 (121), 2019a, p. 43493-43501.

BRAKE, D. **Economic Competitiveness and National Security Dynamics in the Race for 5G between the United States and China**. The Information Technology & Innovation Foundation, Aug. 2018.

BRAVERMAN, H. **Labor and Monopoly Capital**: the degradation of work in the Twentieth Century. New York: Monthly Review Press, 1998.

NIIO – National Internet Information Office. **Cybersecurity Review Measures (draft for comments)**. Cyberspace Administration of China, May 21, 2019. Translated by Sacks, Samm; Creemers, Rogier; Laskai, Lorand; Triolo, Paul; Webster, Graham.

NIIO. **Data Security Management Measures** (draft for comment). Cyberspace Administration of China, May 28, 2019(a). Translated by Tai, Katharin; Laskai, Lorand; Creemers, Rogier; Shi, Mingli; Neville, Kevin; Triolo, Paul.

CHU, M.M. **The East Asian computer chip war**. London, New York: Routledge, 2013  
CUSMARIU, A. (S) Technology that Identifies People by the Sound of Their Voices. **SID Today**, Jan 4, 2006.

DELOITTE. **The Impacts of Mobile Broadband and 5G**: a literature review for DCMS. Deloitte, Jun, 2018.

FEENBERG, A. **Transforming Technology**: a critical theory revisited. Oxford and New York: Oxford University Press, 2006.

FOGARTY, K. 5G Heats Up Base Stations. **Semiconductor Engineering**, 2019.

GALLAGHER, R. e MOLTKE, H. TITANPOINTE. **The Intercept**, Nov 16, 2016.

GREENWALD, G. **Sem Lugar para se Esconder**. Rio de Janeiro: GMT Editores, 2014.

GUARDIAN. NSA Prism Program Taps in to User Data of Apple, Google and Others. **The Guardian**, June 6, 2013.

GUARDIAN. GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications. **The Guardian**, Jun 21, 2013(a).

GUARDIAN. BT and Vodafone among Telecoms Companies passing Details to GCHQ. **The Guardian**, Aug 2, 2013(b).

GUARDIAN. Snowden Document Reveals Key Role of Companies in NSA Data Collection. **The Guardian**, Nov 1, 2013(c).

HUAWEI MARINE. South Atlantic Inter Link Connecting Cameroon to Brazil Fully Connected. **Huawei Marine Press Release**, Sep 5, 2018.

HUSSON, M. Produire de la Valeur en Cliquant? **Alternatives Économiques**, Jan 14, 2018.

JIANG, S. China's Huawei to Sell Undersea Cable Business, buyer's exchange filling shows. **Reuters**, June 3, 2019.

KLEINHANS, J-P. **5G vs National Security**: a European Perspective. Stiftung Neue Verantwortung, Feb, 2019.

KOFMAN, A. Finding Your Voice. **The Intercept**, Jan 19, 2018.

LANGNER, R. Stuxnet: Dissecting a cyberwarfare weapon. **IEEE Security and Privacy**, vol. 9, i. 3, 2011, p.49-51.

Lee, E. e Chau, T. **Telecom Services**: The Geopolitics of 5G and IoT. Jefferies Franchise Note, Sep 14, 2017.

LEÓN, M. ¿Por qué la tecnología 5G representa um nuevo peligro para la vida? **Alai**, Jun 4, 2019.

LEWIS J. A. **Telecom and national security**. Center for strategic and international studies, 13 March, 2018.

LEWIS, J. A. **How 5G will Shape Innovation and Security**. A Report of the CSIS Technology Policy Program, Dec, 2018.

LUCAS, L. et al. Huawei warns Ban could Hit 1,200 US Suppliers. **The Financial Times**, May 29, 2019.

MARKOFF, J. Internet Traffic Begins to Bypass the U.S. **The New York Times**, Aug 29, 2008.

MAZZUCATO, M. **O Estado Empreendedor**: desmascarando o mito do setor público vs. setor privado. São Paulo: Editora Schwarcz, 2014.

MEDEIROS, C. A. The Post-War American Technological Development as a Military Enterprise. **Contributions to Political Economy**, v. 22, 2003, p. 41-62.

MOROZOV, E. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu, 2018.

NSA - National Security Agency. NSA Prism Program Slides. **The Guardian**, Nov 1, 2013.

NSA. **(U) SIGINT Strategy: 2012-2016**, Feb 23, 2012. Disponível em: <https://edwardsnowden.com/2013/11/23/sigint-strategy-2012-2016/>

NSA. **Huawei Powerpoint Slides**, 2010. Disponível em: <https://edwardsnowden.com/2014/03/22/shotgiant/>

ODNI – Office of the Director of National Intelligence. **Quadrennial Intelligence Community Review**, Abr, 2009.

PAGE, J. et al. U.S. Takes on China's Huawei in Undersea Battle Over the Global Internet Grid. **The Wall Street Journal**, March 12, 2019.

PHAM, M. Huawei ban would impact UK 5G customers say network chiefs. **Mobilenews**, March 25, 2019.

POITRAS, L. et al. 'A' for Angela: GCHQ and NSA targeted private German companies and Merkel. **Spiegel Online**, 29 Março, 2014.

PONGRATZ, S. Key Takeaways Worldwide Telecom Equipment Market 2018. *Delloro Group*, 2019.

PRADELLA, L. The Entrepreneurial State by Mariana Mazzucato: a critical engagement. **Competition and Change**, 0 (0), 2016, 1-9.

PWC – Price Waterhouse Coopers. **China's Impact on the Semiconductor Industry 2017 update**. New York: PwC, 2017.

PWC. Global Top 100 Companies by Market Capitalisation. **PwC**, March 31, 2018.

ROBINSON, B. With a different Marx: value and the contradictions of Web 2.0 capitalism. **The Information Society**, 31, 2015, p. 44-51.

ROGERS, M. e EDEN, G. The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures. **International Journal of Communication** 11, 2017.

SHEN, H. Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative. **International Journal of Communication** 12, 2018, p. 2683-2701.

SPIEGEL. NSA Spied on Chinese Government and Networking Firm. **Der Spiegel**, March 22, 2014.

STATE COUNCIL. **National Medium and Long-Term Plan for Science and Technology Development**. Beijing: State Council, 2006.

STATE COUNCIL. **Made in China 2025**. Beijing: State Council, 07 Jul. 2015.

- STATE COUNCIL. **China's Military Strategy**. Beijing: State Council, 2015a.
- STATE COUNCIL. **Outline of the National Informatization Development Strategy**. Beijing: Central Committee and State Council, 2016.
- TIMBERG, C. e GELLMAN, B. NSA paying U.S. companies for access to communications networks. **The Washington Post**, Aug 19, 2013.
- TREBAT, N. e MEDEIROS, C. A. Military Modernization in Chinese Technical Progress and Industrial Innovation. **Review of Political Economy**, 26 (2), 2014.
- TRIOLO, P. e ALLISON, K. **The Geopolitics of 5G**. Eurasia Group White Paper, Nov., 2018.
- TRUMP, D. J.. **Executive Order on Securing the Information and Communications Technology and Services Supply Chain**, May 15, 2019.
- WEISS, L. **America Inc.?** Innovation and Enterprise in the National Security State. Ithaca and London: Cornell University Press, 2014.
- WILLIAMS, S. China Is Still Multiple Generations Behind in Chip Manufacturing. **Wccftech**, June 13, 2019.

## NOTAS DE AUTOR

### CONTRIBUIÇÃO DE AUTORIA

**Esther Majerowicz** - Concepção. Coleta de dados, Análise de dados, Elaboração do manuscrito, revisão e aprovação da versão final do trabalho

### FINANCIAMENTO

Não se aplica.

### CONSENTIMENTO DE USO DE IMAGEM

Não se aplica.

### APROVAÇÃO DE COMITÊ DE ÉTICA EM PESQUISA

Não se aplica.

### CONFLITO DE INTERESSES

Declaro que não há conflito de interesses.

### LICENÇA DE USO

Este artigo está licenciado sob a [Licença Creative Commons CC-BY](#). Com essa licença você pode compartilhar, adaptar, criar para qualquer fim, desde que atribua a autoria da obra.

### HISTÓRICO

Recebido em: 01-10-2020

Aprovado em: 20-10-2020