Um participante do congresso fotografa uma imagem que descreve ataques globais ocorridos via internet, 16 de agosto de 2016, 4º Congresso Chinês de Segurança na Internet (*Internet Security Conference*, ISC) em Pequim. Tendo atingido um nível de sofisticação que torna até mesmo os sistemas de proteção da internet mais avançados vulneráveis a contínuos ataques de hackers, o furto de informações proprietárias de todos os tipos patrocinado pelo governo chinês (por exemplo, industrial, científica, militar, econômica e pessoal), tanto dos EUA quanto de outras nações, alcançou proporções pandêmicas. (Foto: Ng Han Guan, Associated Press)

Tirar a Lenha de Debaixo do Caldeirão

O papel do furto de propriedade intelectual na estratégia global chinesa

Cap Scott Tosi, Exército dos EUA

Em setembro de 2015, os Estados Unidos da América (EUA) e a China concluíram as negociações preliminares de um acordo que especificava, entre outras estipulações, que "nem os EUA nem o governo chinês conduzirão ou apoiarão conscientemente o uso de crimes cibernéticos para o furto de propriedade intelectual (PI)"[1]. No entanto, menos de dois anos depois, o uso de crimes cibernéticos para o furto de PI pelos chineses foi descrito, sem rodeios, na "Estratégia de Segurança Nacional de 2017", que declarou que "todos os anos, concorrentes como a China furtam PI dos EUA avaliada em centenas de bilhões de dólares"[2]. A prática de crimes cibernéticos para o furto de PI representa um problema mais amplo desse tipo de conduta pela China e abrange diversos métodos e meios. De acordo com estimativas, o valor total anual em furto de PI pela China varia de USD 225 bilhões a USD 600 bilhões; além disso, a China é responsável por 50% a 80% de todos os furtos de PI ocorridos contra os EUA[3].

O furto de PI pela China tem amplas implicações para o Exército dos EUA e o Departamento de Defesa (DOD), especialmente à medida que o foco estratégico dos EUA muda da contrainsurgência para operações de combate em larga escala entre grandes potências[4]. O furto de PI de ativos e pesquisas do Exército e do DOD ameaça a superioridade tecnológica militar dos EUA nas décadas futuras, pois a China afirma que atualizará suas capacidades militares, de modo que "em meados do século XXI, as forças armadas chinesas tenham sido totalmente transformadas em forças armadas de classe mundial"[5].

O início dos furtos de PI pelos chineses: ocultar nossas capacidades e esperar o momento oportuno

A mira sistemática da China em PI estrangeira começou no início de sua modernização, sob a liderança de Deng Xiaoping em 1978, quando implementou as "Quatro Modernizações" (agricultura, indústria, ciência e tecnologia e defesa). Naquele mesmo ano, a China obteve apoio do Programa das Nações Unidas para o Desenvolvimento e do Banco Mundial para o desenvolvimento econômico e tecnológico do país e, após cerca de dez anos, começou a enviar milhões de estudantes chineses ao exterior para estudar. As "Quatro Modernizações" incluíram dois grandes esforços projetados para estabelecer indústrias de ciência e tecnologia na China. O primeiro desses esforços, o Programa Nacional de Pesquisa e Desenvolvimento de Alta Tecnologia, buscava enfatizar a ciência e a tecnologia nas universidades chinesas sob a direção de um comitê do governo central e do Exército de Libertação Popular (ELP). O segundo, o Programa Tocha, buscava levar de volta para a China milhares de acadêmicos chineses treinados no Ocidente[6]. Juntos, esses programas serviram como a primeira tentativa do governo de centralizar a pesquisa e o desenvolvimento de ciência e tecnologia dentro do Partido Comunista da China (PCC) e do ELP, a fim de estabelecer as primeiras formas de empresas estatais (conhecidas em inglês como *state-owned enterprise,* SOE) que trabalham lado a lado com o PCC, ELP e empresas privadas estrangeiras para adquirir tecnologia.

Já em 1998, o furto de PI estadunidense pelos chineses havia se tornado problemático o suficiente para justificar a criação do Comitê Seleto da Câmara sobre Segurança Nacional e Assuntos Militares/Comerciais dos EUA com a República Popular da China (RPC). Em 1999, o comitê divulgou um relatório que destacava os esforços da China, já na década de 1970, de focar nos laboratórios nacionais estadunidenses para adquirir tecnologia sensível[7, NT1]. O relatório também destacou o principal meio de aquisição na época: transferência ilegal de tecnologia de outros países, exploração de produtos de dupla utilização (ou uso dual), utilização de empresas de fachada

O Cap Scott Tosi, do Exército dos EUA, é o Comandante da Companhia de Comando da *501ª Brigada* de Inteligência Militar, em Camp Humphreys, Coreia do Sul. É bacharel em Educação com licenciatura em História e Ciências Sociais pela Illinois State University e possui mestrado em Administração Pública pela University of Illinois–Springfield. Serviu em missões em Yongsan, na Coreia do Sul; Fort George G. Meade, em Maryland; e Camp Lemonnier, em Djibouti.

[NT1] W. Longo e W. Moreira, O acesso a "tecnologias sensíveis", Tensões Mundiais, v. 5, n. 9, p. 74, 22 nov. 2018. "Tecnologia sensível é aquela que um determinado país (ou grupo de países) considera que não deva conceder acesso a terceiros, durante certo tempo, hipoteticamente por razões de segurança." Acesso em 26 out. 2020, https://revistas.uece.br/index.php/tensoesmundiais/article/download/669/557/.

para adquirir tecnologia ilegalmente ou participações em empresas de tecnologia dos EUA[8]. No entanto, ao entrar no século XXI, a China buscou um meio mais agressivo de aquisição de tecnologia sensível.

Em 2006, sob o presidente Hu Jintao, a China lançou o "Plano Nacional de Médio e Longo Prazo para o Desenvolvimento da Ciência e Tecnologia (2006-2020)", ou política de "inovação local". Essa política implementou regras de aquisição que obrigaram as empresas estrangeiras a entregar a PI em troca de acesso aos mercados chineses[9]. Além disso, a inovação local aumentou o financiamento de pesquisa e desenvolvimento tecnológico domésticos, ao mesmo tempo que pressionou para "aumentar a inovação original por meio da coinovação e da reinovação com base na assimilação de tecnologias importadas"[10]. Medidas adicionais dentro da política incluíam testes de produtos administrados pelo Estado para estudar métodos estrangeiros de design e produção, políticas de compras governamentais que bloqueavam produtos não projetados e produzidos na China para encorajar empresas estrangeiras a divulgarem métodos de produção dentro das fronteiras chinesas e leis antimonopólio protegendo as SOEs que cooperassem sob o controle direto ou em estreita coordenação com o PCC e ELP[11]. Juntas, essas políticas promoveram a aquisição legal e ilegal de PI de exportação controlada dos EUA e outros países como uma relação do tipo *quid pro quo* para conduzir negócios na China continental.

Uma mudança na política chinesa: a reflexão de Xi Jinping sobre o socialismo com características chinesas para uma nova era

Em seu discurso no 19º Congresso Nacional do PCC em 18 de outubro de 2017, Xi Jinping delineou seu plano para a China se tornar "líder global em termos de força nacional composta e influência internacional" até 2050, ultrapassando os EUA e o Ocidente como força mundial dominante, tanto econômica quanto militarmente[12]. Esse tom está em forte contraste com a "Estratégia em 24 Caracteres" de Deng dos anos 1990, que afirmava "observar com calma; assegurar nossa posição; lidar com os assuntos com calma; esconder nossas capacidades e esperar o momento oportuno; ser bom em manter um perfil discreto; e nunca reivindicar liderança"[13]. Embora a meta geral da China de alcançar proeminência no cenário global não tenha mudado desde a época de Deng até a de Xi, o tom e a agressividade com que as metas econômicas, tecnológicas e militares são perseguidas mudaram drasticamente.

Mudanças na política e legislação nacionais complementaram essa mudança de tom a partir de 2016 com sua Lei de Cibersegurança. Dentre inúmeras outras alterações e restrições, essa lei determina que todas as empresas que geram "dados importantes durante as operações no território continental da República Popular da China, devem armazená-los na China continental"[14]. Se for necessário que os dados sejam transferidos para fora da China para fins comerciais, eles devem ser analisados e aprovados pelas autoridades chinesas antes da divulgação, abrindo a possibilidade de coleta generalizada e furto de dados privados entre as empresas que operam na China[15].

Além disso, a China aprovou a Lei de Inteligência Nacional em 2017, que estabeleceu um nível sem precedentes de cooperação entre agências estatais (como o Ministério da Segurança do Estado [MSE] e o ELP), organizações privadas e pessoas. O artigo 7º da lei estabelece a cooperação privada com a segurança do Estado, afirmando que "Todo cidadão ou organização deve apoiar, auxiliar e cooperar com o trabalho de inteligência do Estado, nos termos da lei, e manter os segredos do trabalho de inteligência nacional fora do alcance do público. O Estado protege indivíduos e organizações que apoiam, auxiliam e cooperam com o trabalho de inteligência nacional"[16]. O artigo 12 atinge um tom cooperativo semelhante entre a coleta de inteligência pelo Estado e as empresas privadas, afirmando que "A organização de trabalho de inteligência do Estado pode, de acordo com as regulamentações pertinentes, estabelecer relações de cooperação com indivíduos e organizações relevantes e confiar trabalhos relevantes"[17].

A mudança de tom sob Xi marca uma transformação em uma política externa chinesa cada vez mais beligerante — econômica, tecnológica e militarmente — que refletiu o aumento do furto de PI de tecnologias estadunidenses. O furto de PI complementa diretamente a meta do ELP de se modernizar e se tornar uma potência global em meados do século XXI. O Gabinete de Informação do Conselho de

Dra. Nita Patel, diretora de descoberta de anticorpos e desenvolvimento de vacina, levanta um frasco contendo uma vacina potencial contra o novo coronavírus em 20 de março de 2020 no laboratório da empresa Novavax em Gaithersburg, no Estado de Maryland. O FBI declarou que o atual esforço dirigido pelo governo chinês, por meio de hacking, para furtar pesquisas relacionadas ao desenvolvimento de uma vacina contra o novo coronavírus, bem como outras pesquisas industriais e militares, atingiu um nível sem precedentes. (Foto: Andrew Caballero-Reynolds, Agence France-Presse)

Estado delineou os futuros objetivos para o ELP no novo papel global da China em um livro branco de 2015 intitulado "Estratégia Militar da China". O livro branco afirmava que o ELP "acelerará a modernização da defesa nacional e das forças armadas [...] para alcançar o objetivo estratégico nacional dos 'Dois Centenários' e para realizar o sonho chinês de alcançar o grande rejuvenescimento da nação chinesa"[18].

Simultaneamente à inovação militar, o Ministério da Indústria e Tecnologia da Informação (MIIT), sob a liderança do Primeiro-ministro Li Keqiang, anunciou sua campanha "Made in China 2025" ("Fabricado na China 2025", em tradução livre) em 2015. O "Made in China 2025" enfatizou o desenvolvimento de tecnologia emergente, inovação doméstica e uma mudança da produção baseada na quantidade para a produção baseada na qualidade para permitir que a China se torne o fabricante líder inovador global até 2049[19]. A meta geral é diminuir a dependência chinesa de nações estrangeiras para tecnologia avançada e produtos de qualidade, produzindo 70% de materiais de alta tecnologia internamente até 2025[20]. De acordo com uma política de 2018 do Gabinete de Política Comercial e de Fabricação da Casa Branca, o investimento chinês em tecnologia estrangeira está alinhado com os investimentos descritos no "Made in China 2025"[21].

Enquanto os especialistas argumentam que as empresas públicas chinesas de defesa estão tentando alcançar inovação e produção locais, a China ainda continua a ter dificuldades com o desenvolvimento de tecnologia crítica[22]. A modernização do ELP, portanto, ainda requer a aquisição de tecnologia sensível e pesquisa e desenvolvimento, algo que é muito mais difícil de adquirir por meio de leis comerciais sob o programa de "inovação local" do que outras tecnologias comerciais. Portanto, o PCC e o ELP dependem fortemente do furto de PI para adquirir toda ou parte da tecnologia crítica para fazer engenharia reversa de armas produzidas internamente.

Métodos empregados pela China no furto de PI: tirar a lenha de debaixo do caldeirão

Os "36 Estratagemas", uma coleção de provérbios que se acredita serem do Período dos Três Reinos da China, descrevem uma estratégia para derrotar um inimigo superior: "tirar a lenha de debaixo do caldeirão"[23]. Esse provérbio descreve a abordagem indireta de remover a fonte de força do inimigo — nesse caso, a superioridade tecnológica dos militares estadunidenses e ocidentais. Esse método foi resumido na revisão de 2013 de *The Science of Military Strategy* ("A Ciência da Estratégia Militar", em tradução livre), publicada pela Academia de Ciências Militares do ELP, que afirmou: "Após a eclosão da Guerra do Golfo, o Comitê Central do Partido e a Comissão Militar Central previram que a situação de guerra causou grandes mudanças [*sic*], e a política estratégica militar de defesa das forças armadas foi ajustada em tempo hábil, aumentando o uso de alta tecnologia"[24]. Os autores continuam delineando a necessidade futura de paridade ou superioridade tecnológica sobre o Ocidente, dizendo que "o desenvolvimento da ciência e da tecnologia abriu o caminho para a evolução da forma de guerra"[25].

Sob Hu em 2004 e atualmente sob Xi, e destacado em *The Science of Military Strategy*, o ELP enfatizou os esforços para igualar o Ocidente em alta tecnologia militar[26]. No entanto, como afirmado antes, a ciência e a tecnologia domésticas da China não são avaliadas como avançadas o suficiente para competir de forma independente com a base industrial de defesa (BID) dos EUA e do Ocidente e dependem do furto de tecnologias atuais e em desenvolvimento. Para conseguir isso, a China utiliza vários meios, tanto legais quanto ilegais, para minar a tecnologia militar, pesquisa e desenvolvimento, e métodos de produção da BID estadunidenses e ocidentais. A "Estratégia de Segurança Nacional" descreve os métodos básicos que a China usa para furtar PI dos EUA: "Os adversários têm usado meios sofisticados para enfraquecer nossos negócios e economia como facetas da guerra econômica via ataques cibernéticos e outras atividades maliciosas. Além desses meios ilegais, alguns atores usam, em grande parte, transferências e relações legais legítimas para obter acesso a campos, especialistas e programas de fornecedores confiáveis"[27]. Os quatro métodos de furto de PI na China são coletas em fontes abertas, comercial, meio acadêmico e cibernético.

> "A ciência e a tecnologia domésticas da China não são avaliadas como avançadas o suficiente para competir de forma independente com a base industrial de defesa dos EUA e do Ocidente."

Primeiro método: coletas em fontes abertas

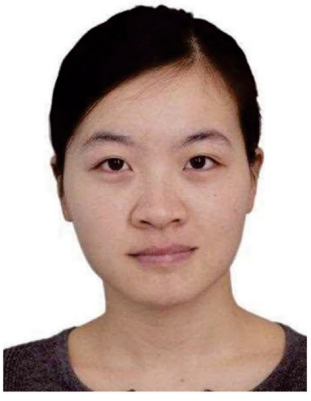
De acordo com James Mulvenon, a coleta em fontes abertas e a criação de banco de dados de informações publicamente disponíveis são os principais recursos da inovação científica e tecnológica. Ele afirma que "a inovação na China é impulsionada por desenvolvimentos estrangeiros, rastreados por meio de fontes abertas"[28]. Como todos os aparatos burocráticos chineses, a estrutura de coleta de informações em fontes abertas é complexa e redundante. Organizações como o Instituto de Informação Científica e Técnica da China operam sob a fachada

de bancos de dados e catalogação inócuos, mas têm como alvo documentação técnica pública de ciência e tecnologia para engenharia reversa e produção doméstica, informações publicamente disponíveis que possam ser utilizadas pelo setor de inteligência estatal contra organizações de pesquisa e seus funcionários e informações incorretamente desclassificadas ou classificadas, mas que foram divulgadas

WANTED BY THE FBI

YANQING YE

Acting as an Agent of a Foreign Government; Visa Fraud; Making False Statements; Conspiracy



DESCRIPTION

Date(s) of Birth Used: July 22, 1990	**Place of Birth:** Longhai, Fujian, China
Hair: Dark Brown	**Eyes:** Brown
Height: Approximately 5'4"	**Weight:** Approximately 110 pounds
Sex: Female	**Race:** Asian
Nationality: Chinese	**Languages:** English, Chinese

REMARKS

Ye is believed to be in China.

CAUTION

Yanqing Ye is a Lieutenant in the People's Liberation Army (PLA), the armed forces of the People's Republic of China, and a member of the Chinese Communist Party (CCP). Ye studied at the National University of Defense Technology (NUDT), a top military academy directed by the CCP in China. It is alleged that, on her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the NUDT. During Ye's time in the United States on her J-1 visa, she maintained close contact with her supervisor at the NUDT and other colleagues. While studying at Boston University's Department of Physics, Chemistry and Biomedical Engineering from October of 2017 to April of 2019, Ye allegedly continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing United States military websites, and sending United States documents and information to China.

On January 28, 2020, a federal arrest warrant was issued for Ye in the United States District Court for the District of Massachusetts, Boston, Massachusetts, after she was charged with acting as an agent of a foreign government, visa fraud, making false statements, and conspiracy.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Boston

Imagem de um alerta do FBI para uma pessoa suspeita de ser uma agente chinesa (2020).

por engano[29]. Embora o sistema seja executado de forma semelhante a um catálogo baseado em bibliotecas, ele é dirigido e administrado por especialistas em inteligência chineses que estão trabalhando sob ordens do partido, servindo como um atalho para a indústria chinesa desenvolver pesquisa e tecnologia, e é catalogado e disseminado em coordenação com desenvolvedores e fabricantes privados ou de SOE[30].

Desde 2013, o programa de coleta em fontes abertas extraiu e catalogou mais de 4,7 bilhões de títulos e resumos, 644 milhões de documentos de texto completo, 1,2 milhão de documentos de congressos, 1,8 milhão de relatórios estrangeiros de ciência e tecnologia e 9,8 milhões de produtos microfilmados[31]. Essa vasta coleção de informações públicas e privadas não classificadas, não confidenciais e classificadas indevidamente reduz custos, tempo e riscos para o desenvolvimento militar e civil da China. O programa de coleta em fontes abertas tem sido tão bem-sucedido que o ex-diretor do Instituto de Informações Científicas e Técnicas da China, He Defang, se gabou de que, com ele, "os pesquisadores da China reduziram seus custos em 40% a 50% e seu tempo em 60% a 70%"[32].

As implicações de uma coleta tão completa e direcionada de informações em fontes abertas para o Exército e o DOD são profundas. A responsabilidade pública e a transparência nos EUA e países ocidentais podem ser usadas para mirar o desenvolvimento e desenvolvedores de tecnologia militar. Por exemplo, as concessões de contratos governamentais publicadas quase diariamente na página de notícias sobre "Contratos" do DOD oferecem informações sobre tecnologia em desenvolvimento, custos, contratados, subcontratados, durações de contratos, locais, filiais atendidas, etc.[33] Além disso, os sites dos beneficiários do contrato geralmente fornecem informações sobre a estrutura organizacional, pessoal, localização das instalações e informações não classificadas ou não confidenciais sobre pesquisa e desenvolvimento. Essas informações, junto com outras informações de inúmeros outros sites governamentais ou privados de acesso público, fornecem à China uma imagem clara das prioridades de pesquisa e desenvolvimento dos EUA, intenções de longo prazo, estratégias, prioridades para as forças militares e oportunidades de coleta por outros meios destacados abaixo.

Segundo método: comercial

Embora a China tenha passado de uma nação maoísta comunista durante o governo Nixon para uma economia de mercado mista hoje em dia, a distinção entre privado, público e acadêmico é muito menos profunda do que nos EUA. Hoje, as estatais direta ou indiretamente de propriedade do PCC ou ELP ou por eles financiadas constituem cerca de 23% a 28% do produto interno bruto (PIB) da China[34]. Algumas SOEs e empresas privadas na China trabalham sob o comando ou em nome do PCC ou ELP, direta ou indiretamente, para mirar e adquirir tecnologia dos EUA para importação, engenharia reversa e produção doméstica que apoie as metas de pesquisa e desenvolvimento do PCC ou ELP[35]. Os subcontratos concedidos a empresas chinesas por empresas contratadas principais em contratos com o governo dos EUA oferecem uma visão dos métodos de produção e da capacidade e habilidade de compilar e fazer engenharia reversa de tecnologia para produzir internamente tecnologia de ponta.

As SOEs estão vinculadas a empresas estadunidenses e ocidentais pela Associação Chinesa de Ciência e Tecnologia por meio de centros nacionais de transferência de tecnologia. Esses centros estabelecem relações de cooperação com empresas e institutos acadêmicos estadunidenses para estimular transferências de tecnologia[36]. O PCC e o ELP financiam as estatais para empregar especialistas em ciência e tecnologia dos EUA e do Ocidente, que respondem por cerca de metade dos 440 mil estrangeiros que atualmente trabalham na China[37]. Outros programas estatais, como o "Programa 863", financiado e administrado pelo Ministério da Ciência e Tecnologia para desenvolver e adquirir tecnologias

Próxima página: Uma variedade de aeronaves militares chinesas de asas fixas e rotativas parecem estranhamente semelhantes em design às desenvolvidas pelos EUA e outros países, incluindo diversas fabricadas pela Rússia. Por exemplo, acredita-se que o helicóptero chinês Z-10 (acima), que se assemelha muito ao helicóptero Apache AH-64 dos EUA (abaixo), foi desenvolvido a partir de informações obtidas por uma combinação de espionagem, hacking de computador e transferência de segredos comerciais classificados por meio de acordos fraudulentos com empresas legítimas que trabalham sob a presunção de cooperação com a China para desenvolver um helicóptero de "uso dual". (Foto de cima: Wikipédia, CC BY-SA 2.0. Foto de baixo: Exército dos EUA, Sgt Técnico Andy Dunaway)

de alto nível, foram implicados em espionagem, como a condenação de Kexue Huang em 2011 por furtar segredos comerciais das empresas Dow AgroSciences LLC e Cargill Inc.[38]

Conforme descrito no "Made in China 2025", a China mudou o foco industrial de produtos baratos e de baixa qualidade para inovação de alta qualidade impulsionada pela tecnologia[39]. Para tanto, a China mudou o financiamento apoiado pelo governo da aquisição de "recursos naturais essenciais", antes do lançamento da política, para "adquirir áreas de alta tecnologia, especialmente da economia dos EUA"[40]. A China utiliza SOEs, empresas privadas chinesas com laços com o governo chinês e fundos de investimento apoiados pelo Estado para conduzir fusões, aquisições, investimentos e financiamento de risco para adquirir alta tecnologia dos EUA[41]. Essas práticas consistem em meios legais, ilícitos ou, às vezes, ilegais para solicitar, furtar ou coagir pessoas a obter informações e tecnologia de empresas privadas dos EUA e de outras nações. De acordo com um relatório do Departamento Federal de Investigação dos EUA (FBI) sobre ações judiciais relacionadas à China desde 2018, "cerca de 80% de todas as ações judiciais por espionagem econômica impetradas pelo Departamento de Justiça dos EUA (DOJ) alegam conduta que beneficiaria o Estado chinês, e há pelo menos algum vínculo com a China em torno de 60% de todos os casos de furto de segredo comercial"[42].

Selo do Programa "Mil Talentos" (*Thousand Talents Program*)

Além disso, as empresas chinesas, incluindo as estatais, inseriram-se nas cadeias de fornecimento militares dos EUA, normalmente em subcontratos em níveis hierarquicamente mais baixos, e produziram e venderam peças falsificadas ilegais e abaixo do padrão para os EUA[43]. Exemplos recentes incluem peças componentes para as aeronaves de transporte C-130J e C-27J, o helicóptero multimissão da Marinha SH-60B, o sistema de defesa antimísseis balísticos *Terminal High Altitude Area Defense* (THAAD) e a aeronave marítima multimissão Poseidon P-8A[44]. À medida que as forças armadas dos EUA dependem cada vez mais de equipamentos comerciais de tecnologia da informação, o risco de as empresas chinesas produzirem componentes comprometidos é agravado. Isso ficou evidenciado em uma reportagem da Bloomberg de 2018, que destacou os esforços chineses para utilizar *microchips* comerciais para se infiltrar e estabelecer uma forma de acesso aos equipamentos de tecnologia da informação vendidos a agências governamentais[45]. As preocupações com essa questão são tão grandes que, em 2018, o presidente dos EUA, Donald Trump, promulgou uma lei proibindo o uso de tecnologias da Huawei e ZTE (principais fornecedores de telefones celulares para militares no exterior) em contratos governamentais[46].

Terceiro método: meio acadêmico

Além do furto de PI de fontes abertas e comerciais, a China tem empregado acadêmicos para cometer furto de PI desde o início das "Quatro Modernizações" de Deng[47]. Começando em 1978 sob Deng, a China mudou para uma abordagem mais pragmática para modernizar o país, enviando um número crescente de estudantes e cientistas ao exterior para aprender com as nações ocidentais (algo que foi considerado perigoso sob Mao após a Revolução Cultural), bem como atrair talentos estrangeiros para a China[48]. A abordagem da China para adquirir PI por meio do setor acadêmico conta com duas vias distintas: por meio de organizações abertas e estabelecidas com o apoio do governo e por meio do uso transparente ou encoberto de populações de estudantes e professores no exterior que têm a missão de adquirir PI ilegalmente. Ambas as formas efetivamente transformam alunos e professores em coletores de PI patrocinados pelo Estado sob a direção do PCC ou do ELP.

Desde o início do Movimento pela Democracia de 1989 até o Massacre da Praça da Paz Celestial, o PCC mirou estudantes chineses dentro e fora do país para assegurar a lealdade ao partido. Para tanto, o PCC expandiu as Associações Chinesas de Bolsas de Estudos e Estudantes (*Chinese Students and Scholarship Associations*, CSSAs) existentes no exterior para garantir a lealdade dos estudantes que estejam fora do país à ideologia do PCC. Além disso, em 2004, o PCC fundou o primeiro Instituto Confúcio (IC), cujo propósito declarado é "ensinar a língua, cultura e história chinesas no nível primário, secundário e universitário em todo o mundo"[49]. Atualmente, a China opera mais de 140 CSSAs e 110 ICs, todos sob a direção do Departamento de Trabalho da Frente Unida do PCC[50]. De acordo com a Comissão EUA-China de Revisão Econômica e de Segurança de 2018, na realidade, as CSSAs "recebem orientação do PCC por meio de embaixadas e consulados chineses [...] e são ativas na realização do trabalho chinês no exterior consistente com a estratégia da Frente Unida de Pequim"[51]. Da mesma forma, os ICs foram acusados de "influência indevida no ensino e pesquisa, espionagem industrial e militar, vigilância de chineses no exterior e de minar a influência taiwanesa como parte do plano de reunificação"[52]. Ambas as organizações servem para garantir que as populações de estudantes chineses no exterior estejam agindo de acordo com as orientações e desejos do PCC e ELP.

> A China utiliza atores cibernéticos estatais, empresariais e privados para comprometer e furtar de USD 180 bilhões a USD 540 bilhões em PI e segredos comerciais anualmente, ou de 1% a 3% do PIB dos EUA.

O Programa "Mil Talentos", estabelecido em 2008 para recrutar cientistas estrangeiros e atrair chineses educados no exterior a retornarem ao continente, foi criticado abertamente por agências estadunidenses por cometer furto de PI. Em 2018, o diretor assistente da Divisão de Contraespionagem do FBI afirmou que o Programa "Mil Talentos" e outros programas similares patrocinados pelo governo "oferecem salários competitivos, instalações de pesquisa de última geração e títulos honoríficos, atraindo talentos chineses do exterior e especialistas estrangeiros para trazerem seu conhecimento e experiência para a China, mesmo que isso signifique furtar informações proprietárias ou violar os controles de exportação para fazê-lo"[53]. Em janeiro de 2020, Charles Lieber, presidente do Departamento de Química e Biologia Química da Universidade de Harvard, foi indiciado por aceitar pagamento e cobertura de despesas de subsistência da Universidade de Tecnologia de Wuhan após aceitar uma bolsa de pesquisa do DOD e falsificar declarações sobre sua participação no Programa Mil Talentos[54]. O Programa Mil Talentos e outros programas similares que são financeiramente atraentes permitem que a China capitalize os sistemas de educação e o desenvolvimento de tecnologia estrangeiros de forma barata, e muitas vezes ilegal, por meio do aliciamento de cientistas e pesquisadores

que trabalham em tecnologias sensíveis e controladas para transferir PI estrangeira para o país.

Além de organizações patrocinadas pelo governo, a China foi acusada de ver todos os estudantes chineses como canais potenciais para a transferência de tecnologia estrangeira. As organizações chinesas têm defendido abertamente "expandir o papel dos cientistas chineses que vivem no exterior para fazerem pesquisas em nome dos institutos de pesquisa chineses e facilitarem a transferência de tecnologia"[55]. Os estudantes chineses que retornam do exterior são frequentemente entrevistados por funcionários do governo para identificar as tecnologias, pesquisas e pessoal científico aos quais eles tiveram acesso como parte da coleta de inteligência geral e para avaliar o potencial de cooptar ou recrutar alunos. Além disso, o MSE da China foi acusado de abordar estudantes e cientistas chineses que estão se preparando para viajar ao exterior para incumbi-los de obter informações ou "realizar outra atividade operacional" no exterior, como estabelecer relações secretas com pessoal acadêmico[56]. O uso de estudantes e professores chineses no exterior como coletores de PI representa um grande desafio para a abertura e transparência das instituições acadêmicas fora da China, que devem lutar para equilibrar a proteção da PI e promover o compartilhamento e colaboração de pesquisa científica.

Quarto método: cibernético

A China usa meios cibernéticos para realizar o furto de PI, tanto diretamente, por meio de invasões de rede e furto de dados, quanto indiretamente, por meio, por exemplo, da coleta em fontes abertas ou em apoio à espionagem tradicional[57]. O método cibernético une os métodos discutidos anteriormente porque fornece um meio barato e fácil para furtar PI em um ambiente de baixo risco com relativamente pouca repercussão para ações que, de outra forma, teriam implicações importantes, como sanções econômicas, prisões e expulsão de atores estatais (conhecida na diplomacia internacional como *persona non grata*), se realizadas em solo estrangeiro.

O furto de PI por meio de invasões de rede e extração de dados da BID, subcontratados, setor acadêmico e redes governamentais oferece um meio barato, confiável e de baixo risco de adquirir tecnologia militar sensível em desenvolvimento e existente para engenharia reversa e produção doméstica na China. De acordo com o relatório anual do DOD de 2019 para o Congresso dos EUA, "a China usa seus recursos cibernéticos não só para apoiar a coleta de inteligência [...] mas também para extrair informações confidenciais da BID para obter vantagem militar. As informações visadas podem beneficiar a indústria de alta tecnologia de defesa da China [e] apoiar a modernização militar do país"[58]. O relatório prossegue destacando a gravidade do problema, declarando que "essas campanhas cibernéticas ameaçam corroer as vantagens militares dos EUA e colocar em risco a infraestrutura e a prosperidade das quais essas vantagens dependem"[59].

De acordo com um relatório de 2013 da Verizon, 96% de todos os casos de violação de dados de espionagem cibernética foram atribuídos a atores adversários na China[60]. A China utiliza atores cibernéticos estatais, empresariais e privados para comprometer e furtar de USD 180 a USD 540 bilhões em PI e segredos comerciais anualmente, ou de 1% a 3% do PIB dos EUA[61]. O Gen Keith Alexander, ex-diretor da Agência de Segurança Nacional e comandante do Comando Cibernético dos EUA, declarou em 2012: "Na minha opinião, trata-se da maior transferência [furto cibernético de PI] de riqueza da história"[62].

Em 2014, o DOJ dos EUA acusou cinco oficiais do ELP da Unidade 61398, 3PLA, de "espionagem econômica" e "acesso (ou tentativa de acesso) a um computador protegido, sem autorização, para obter informações para fins de vantagem comercial e ganho financeiro privado"[63], dentre outras acusações. Essa foi uma primeira ocorrência histórica de atores estrangeiros estatais acusados de infiltração a alvos comerciais dos EUA por meio de espionagem cibernética[64]. Em uma tentativa de constranger e impedir ações futuras de atores chineses, o recebimento das acusações pelo júri de acusação (*grand jury*) representou um reconhecimento público e aberto pelo governo dos EUA de que atores estatais chineses têm visado ativa e agressivamente a tecnologia militar crítica. Apesar das acusações, no entanto, as ramificações e retaliações do governo dos EUA permaneceram direcionadas contra indivíduos específicos e destacaram a natureza de baixo risco e alta recompensa da espionagem cibernética.

Professor Charles Lieber da Universidade de Harvard, cercado por repórteres ao deixar o Tribunal Federal John Joseph Moakley, em Boston, 30 de janeiro de 2020. Lieber, que era chefe do Departamento de Química e Biologia Química, foi acusado de mentir às autoridades sobre seu envolvimento com um programa de recrutamento administrado pelo governo chinês e pelo qual recebeu dezenas de milhares de dólares. (Foto: Charles Krupa, Associated Press)

O ápice do volume de atividades cibernéticas chinesas foi destacado em 2013, quando a FireEye, uma empresa privada de segurança cibernética, identificou uma diminuição acentuada nos incidentes de espionagem cibernética na China nos anos seguintes. Embora isso se deva em grande parte ao recebimento das acusações de 2014 pelo júri de acusação e às negociações preliminares do Acordo Cibernético EUA-China de 2015, a FireEye também atribuiu a diminuição à profissionalização e reorganização dos atores cibernéticos chineses[65]. De acordo com Elsa Kania e John Costello, a redução na quantidade de ataques coincide com a reorganização dos meios cibernéticos chineses sob a Força de Apoio Estratégico do ELP, que centralizou a área ciberespacial do ELP como uma Força separada sob um único comando, voltando o foco cibernético para o combate. Além disso, o MSE parece ter assumido a liderança na

espionagem cibernética comercial e na direção de atores não estatais em ataques direcionados contra os interesses comerciais dos EUA[66]. De acordo com um relatório anual de 2016 para o Congresso dos EUA, a atividade cibernética chinesa em geral mudou de ataques amadores em grande escala, como aqueles conduzidos sob o ELP antes de 2014, para uma força mais centralizada e profissionalizada, o que significa que a espionagem cibernética chinesa será mais difícil de detectar no futuro, à medida que o MSE e outras agências de inteligência chinesas, em vez do ELP, visarem redes comerciais vulneráveis[67]. Em vez de o declínio nos incidentes de espionagem cibernética da China representar um sucesso na política dos EUA, na verdade destaca um aumento potencial nas capacidades dos atores cibernéticos chineses e uma diminuição da capacidade dos EUA de detectar ameaças.

Além da invasão direta de redes e furto de PI, a China utiliza redes de informação para visar indivíduos on-line, a fim de realizar as formas mais

Yu Xue sai do tribunal federal, na Filadélfia, 31 de agosto 2018. Xue, uma pesquisadora de câncer, se declarou culpada de conspirar para furtar segredos comerciais biofarmacêuticos da GlaxoSmithKline no que os promotores disseram ser um esquema para abrir empresas na China para comercializá-los. (Foto: Matt Rourke, Associated Press)

tradicionais de furto de PI, mencionadas anteriormente. Atores de inteligência estatais chineses usaram o LinkedIn para localizar e recrutar clandestinamente um ex-funcionário da Agência Central de Inteligência e da Agência de Inteligência da Defesa, e o DOJ acusou um agente de inteligência chinês em outubro de 2018 de recrutar um engenheiro da General Electric Aviation com quem o agente fez contato inicial via LinkedIn[68]. Perfis contendo histórico profissional, diplomas e áreas de especialização oferecem informações lucrativas na identificação de possíveis alvos por agentes chineses que buscam adquirir PI de setores específicos de tecnologia.

O furto cibernético de PI, como todos os outros métodos de furto de PI utilizados pelos chineses, cobre um amplo espectro de meios e métodos e se sobrepõe aos métodos tradicionais mencionados acima. O furto cibernético de PI se destaca dentre os demais métodos pelo volume e facilidade com que pode ser realizado. No entanto, é importante notar que os dados técnicos brutos têm pouco valor sem os métodos, meios e conhecimentos técnicos necessários para fazer engenharia reversa e produzir tecnologia internamente na China, e tudo isso é obtido principalmente por meio de furto de PI comercial e acadêmica.

Mitigando o furto chinês de propriedade intelectual: lutando contra a maré

Embora as políticas e procedimentos internos do Exército e do DOD possam mitigar alguns furtos de PI, esse tipo de crime cobre um amplo espectro no governo, no setor privado e no mundo acadêmico e, portanto, o problema não pode ser resolvido somente pelo Exército ou DOD. Para mitigar e prevenir o furto de PI, o DOD deve fortalecer as parcerias governamentais, privadas e acadêmicas existentes, bem como comitês e políticas. Em primeiro lugar, as políticas, organizações e autoridades governamentais existentes podem ser aproveitadas para combater o furto de PI de tecnologia militar. No entanto, o Exército e o DOD devem tirar máximo proveito do setor privado e alterar suas políticas e regulamentações de contratação para mitigar o furto, aplicando padrões mais rígidos de proteção de informações para contratados e subcontratados. Além disso, o Exército e o DOD devem fazer parcerias com institutos acadêmicos que realizam pesquisas sobre tecnologia crítica para proteger tecnologias emergentes ou em desenvolvimento classificadas e não classificadas.

Deve-se analisar uma abordagem abrangente dentro do governo federal para priorizar altas tecnologias críticas. Uma tecnologia que tem um ciclo de vida mais curto antes de se tornar obsoleta é menos crítica para defender do que uma tecnologia que permanecerá relevante por décadas, sem substituição previsível. Além disso, o DOD e outras agências governamentais devem garantir a proteção de tecnologias do "berço ao túmulo", um termo usado para descrever a proteção de tecnologias críticas desde o seu início até o desenvolvimento, durante o ciclo de vida e até a eventual substituição por nova tecnologia. Ao defender apenas tecnologias em desenvolvimento, o DOD corre o risco de apenas atrasar um eventual furto de tecnologia e a produção nacional pelos adversários.

Além disso, o DOD e o governo federal devem tirar o máximo de proveito das políticas e organizações existentes para fortalecer a proteção da PI do setor privado. Dois exemplos incluem o Comitê de Investimento Estrangeiro nos EUA, que pode analisar aquisições e fusões estrangeiras de tecnologia estadunidense crítica; e o Programa Nacional de Segurança Industrial, que estabeleceu a política DOD 5220.22-M. Essa política é, na verdade, um manual de operação do DOD que descreve os procedimentos para empresas privadas que trabalham sob contratos governamentais classificados[69]. Ao tirar proveito de comitês como o Comitê de Investimento Estrangeiro nos EUA, o DOD poderia abordar preocupações sobre fusões ou aquisições de empresas contratadas ou subcontratadas de alta tecnologia por empresas chinesas com vínculos diretos ou indiretos com o PCC ou ELP. As políticas existentes, como a DOD 5220.22-M, a Regulamentação para Aquisições pelo Governo Federal (*Federal Acquisition Regulation*) e o Suplemento da Regulamentação para Aquisições pelo Governo Federal para a Defesa (*Defense Federal Acquisition Regulation Supplement*, DFARS), fornecem estruturas para melhorar as práticas de segurança do setor privado e fortalecer a regulamentação sobre o acesso de subcontratados a tecnologias críticas e em desenvolvimento[70]. Ao aproveitar as autoridades de agências e departamentos externos, como o FBI, o

Departamento do Tesouro ou o Departamento de Estado, o Exército e o DOD impõem ações regulatórias, financeiras ou penais a empresas não conformes nos EUA e exercem pressão internacional por meio de um órgão regulatório internacional.

Atualmente, toda universidade com um contrato federal de defesa, trabalhando com informações não classificadas controladas sob o DFARS 525.204.7012, deve estar em conformidade com a Publicação Especial 800-171 do Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology*, NIST) — Protegendo Informações Não Classificadas Controladas em Sistemas e Organizações Não Federais (*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*) — para proteger informações não classificadas controladas[71]. O DFARS 252.204.7012 estabeleceu conformidade regulatória com os padrões NIST 800-171 para todos os contratos celebrados após primeiro de outubro de 2017. No entanto, a aplicação do DFARS 252.204.7012 depende principalmente de o contratado notificar o diretor de informações do DOD sobre quaisquer deficiências no cumprimento da NIST 800-171, e não em inspeções ou verificações regulatórias por algum órgão fiscalizador. Além disso, os subcontratados são obrigados apenas a relatar deficiências no cumprimento da NIST 800-171 ao contratado principal e não ao governo federal, gerando o risco de que a conformidade do subcontratado com informações não classificadas controladas seja deficiente[72]. Essa confiança na autonotificação por parte de contratados e subcontratados promove a conduta de ignorar deficiências na orientação regulatória federal necessária e coloca as empresas e o DOD em risco de vulnerabilidade crítica de tecnologia de sistemas de informação. Emendar as orientações regulatórias federais para universidades, contratados e subcontratados que trabalham com informações não confidenciais controladas para permitir inspeções regulatórias federais e verificações de conformidade da empresa seria uma proteção contra o furto de PI.

A adição de 2019 ao DFARS 252.204-7018, que proibia as vendas por contratados ou subcontratados para o governo dos EUA de itens finais ou componentes produzidos pela Huawei e ZTE, ou qualquer de suas subsidiárias, estabeleceu um precedente para a promulgação de ação regulatória contra o furto de PI. Além disso, o DFARS 252.204-7018 exige que os contratados principais incluam a cláusula em "subcontratos para a aquisição de itens comerciais" para evitar as vendas proibidas de equipamentos Huawei e ZTE para contratados por meio de subcontratos[73]. Utilizar ações semelhantes contra SOEs conhecidas do PCC ou ELP pode servir como um impedimento contra a disposição das SOEs de se envolverem em furto de PI.

Nenhuma abordagem ou método irá neutralizar o furto de PI de tecnologia militar crítica pelos chineses. No entanto, ao fazer parcerias com outras agências e departamentos federais e estaduais, empresas privadas e universidades, bem como promulgar orientações regulatórias e ferramentas de fiscalização mais rígidas, o Exército e o DOD evitariam com mais eficácia o furto de PI e retaliariam os furtos após sua ocorrência. Por meio de uma abordagem público-privada, pode ser possível impedir o furto de PI por meio de uma combinação de prevenção, incentivos e retaliação, o que tornaria o furto de PI financeiramente insustentável.

Conclusão

As implicações do furto de PI pela China são bastante aparentes nas ações, declarações oficiais e doutrina do PCC e do ELP. Embora os métodos e técnicas utilizados para realizar o furto de PI não sejam exclusivos do PCC, o escopo e a frequência dos furtos são. Apesar das negociações preliminares de 2015 e das ações retaliatórias subsequentes do governo federal dos EUA, a China mostrou pouca propensão para conter seus furtos de PI de alta tecnologia. O furto de PI, combinado com o aumento dos gastos militares da China, ameaça fechar a lacuna com a superioridade tecnológica militar dos EUA e desafiar o domínio militar estadunidense. Embora a China possa não ser capaz de produzir armas e sistemas de alta tecnologia de qualidade superior por muitas décadas, a ameaça de paridade mesmo em poucas áreas militares de alta tecnologia ameaça a superioridade geral dos EUA no campo de batalha e leva a uma diminuição de seu status na arena global.

Os desafios impostos pelo furto de PI pela China são numerosos e podem exigir que o Exército e o DOD saiam de seu ambiente operacional normal para combater a ameaça e trabalhar com agências, departamentos e parceiros que não estão frequentemente

associados à ação militar. Embora incidentes isolados de furto de PI possam parecer irrelevantes no presente, as consequências de não agir tem o potencial de ameaçar vidas futuras no campo de batalha e o domínio militar dos EUA. Somente por meio da prevenção proativa do furto chinês de PI, o Exército e o DOD podem proteger seu domínio tecnológico e o futuro da superioridade militar dos EUA. ■

Referências

1. Barack Obama, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", The White House, 25 September 2015, acesso em 13 maio 2020, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

2. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), p. 21, acesso em 14 maio 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

3. Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Seattle: National Bureau of Asian Research, February 2017), p. 1, acesso em 14 maio 2020, http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf; Commission on the Theft of American Intellectual Property, *The IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Seattle: National Bureau of Asian Research, May 2013), p. 3, acesso em 12 jun. 2020, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

4. Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 2017), 1-1 a 1-2.

5. Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era" (speech, 19th National Congress of the Communist Party of China, Beijing, 10 October 2017), p. 25, acesso em 16 jun. 2020, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

6. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013), p. 12.

7. Select Comm. on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, H. Rep. No. 105-851, at x–xi (1999), acesso em 14 maio 2020, https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf.

8. Ibid., p. 20-21.

9. James McGregor, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, 2010), p. 2-5, acesso em 14 maio 2020, https://www.uschamber.com/report/china%E2%80%99s-drive-indigenous-innovation-web-industrial-policies.

10. Ibid., p. 4.

11. Ibid., p. 5.

12. Xi, "Secure a Decisive Victory", p. 25.

13. Chuang Meng, "Deng Puts Forward New 12-Character Guiding Principle for Internal and Foreign Policies", *Ching Pao*, no. 172 (1991): p. 84-86, cited in Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2006* (Washington, DC: Department of Defense [DOD], 2007), p. 7, acesso em 14 maio 2020, https://fas.org/nuke/guide/china/dod-2006.pdf.

14. Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]", *Cybersecurity Initiative* (blog), New America, 29 June 2018, acesso em 14 maio 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

15. Ministry of Foreign Affairs and Trade and New Zealand Trade and Enterprise, "Understanding China's Cybersecurity Law: Information for New Zealand Businesses" (Wellington, NZ: National Cyber Security Centre, September 2017), acesso em 14 maio 2020, https://www.ncsc.govt.nz/assets/NCSC-Documents/Understanding-Chinas-cybersecurity-law.pdf.

16. National Intelligence Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., 27 June 2017, effective 28 June 2017), art. 7, acesso em 16 jun. 2020, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

17. Ibid., art. 12.

18. Information Office of the State Council, "China's Military Strategy (full text)" (Beijing: The State Council, 27 May 2015), acesso em 14 maio 2020, http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm. "Dois Centenários" é uma política implementada pelo presidente Xi Jinping referente ao centenário da fundação do Partido Comunista da China em 2021, quando os chineses estabelecerão uma grande base econômica e de classe média, e a fundação da República Popular da China em 2049, momento em que a China se tornará um "país socialista forte, democrático, civilizado, harmonioso e moderno". Isso geralmente se refere à restauração da China como a potência proeminente no mundo.

19. Information Office of the State Council, "'Made in China 2025' Plan Issued", The State Council, 19 May 2015, acesso em 14 maio 2020, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

20. "Notice of the State Council on Printing and Distributing 'Made in China 2025'", The State Council, 8 May 2015, acesso em 14 maio 2020, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

21. White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies*

and Intellectual Property of the United States and the World (Washington, DC: The White House, June 2018), p. 16, acesso em 14 maio 2020, https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

22. Meia Nouwens and Helena Legarda, "China's Pursuit of Advanced Dual-Use Technologies", International Institute for Strategic Studies, 18 December 2018, acesso em 10 mar. 2020, https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance; Mike Yeo, "China's Military Capabilities are Booming, but Does Its Defense Industry Mirror That Trend?", Defense News, 14 August 2018, acesso em 10 mar. 2020, https://www.defensenews.com/top-100/2018/08/14/chinas-military-capabilities-are-booming-but-does-its-defense-industry-mirror-that-trend/.

23. Stefan H. Verstappen, *The Thirty-Six Strategies of Ancient China* (San Francisco: China Books and Periodicals, 1999), p. 91-95.

24. Shou Xiaoson, ed., *The Science of Military Strategy*, trans. Chinese Academy of Military Science (Beijing: Military Science Press, 2013), p. 17.

25. Ibid., p. 3.

26. Ibid., p. 247-48.

27. The White House, *National Security Strategy*, p. 21.

28. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, p. 25.

29. Ibid., p. 23-28.

30. Ibid., p. 24.

31. Ibid.

32. Defang He, "As for Indigenous Innovation, Information Should Go Ahead of Rest", *China Information Review* 10 (2006): p. 12-13, quoted in Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, p. 38.

33. "Contracts", DOD, acesso em 15 maio 2020, https://DOD.defense.gov/News/Contracts/.

34. Chunlin Zhang, *How Much do State-Owned Enterprises Contribute to China's GDP and Employment* (Washington, DC: World Bank, 15 July 2019), p. 10, acesso em 15 maio 2020, http://documents.worldbank.org/curated/en/449701565248091726/pdf/How-Much-Do-State-Owned-Enterprises-Contribute-to-China-s-GDP-and-Employment.pdf.

35. Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, p. 17-19.

36. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, p. 93-94, p. 111.

37. Ibid., p. 79-80, p. 95.

38. "National High-tech R&D Program (863 Program)", Ministry of Science and Technology of the People's Republic of China, acesso em 15 maio 2020, http://en.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm; "Chinese Scientist Huang Kexue Jailed for Trade Theft", BBC News, 22 December 2011, acesso em 15 maio 2020, https://www.bbc.com/news/business-16297237.

39. "Made in China 2025", The State Council, 8 May 2015, acesso em 15 maio 2020, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

40. Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, p. 16.

41. Ibid., p. 17-20.

42. "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018", U.S. Department of Justice, acesso em 15 jun. 2020, https://www.justice.gov/opa/page/file/1223496/download.

43. Senate Comm. on Armed Services, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, S. Rep. No. 112-167, at vi–viii (2012), acesso em 15 maio 2020 https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf.

44. Ibid., p. ii–iv.

45. Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", Bloomberg Businessweek, 4 October 2018, acesso em 15 maio 2020, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

46. Jacob Kastrenakes, "Trump Signs Bill Banning Government Use of Huawei and ZTE Tech", The Verge, 13 August 2018, acesso em 15 maio 2020, https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

47. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, p. 12.

48. Ibid., p. 136-37.

49. Alexander Bowe, *China's Overseas United Front Work: Background and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, 2018), p. 12, acesso em 10 jun. 2020, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.

50. Ibid, p. 10, p. 12.

51. Ibid., p. 10.

52. Michael Barr, *Who's Afraid of China?: The Challenge of Chinese Soft Power* (London: Zed Books, 2011), p. 67.

53. *China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses, Before the Senate Judicary Committee*, 115th Cong. (2018) (statement of E. W. "Bill" Priestap, Assistant Director of Counterintelligence Division, Federal Bureau of Investigation), acesso em 18 maio 2020, https://www.fbi.gov/news/testimony/chinas-non-traditional-espionage-against-the-united-states.

54. U.S. Department of Justice, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases", news release no. 20-99, 28 January 2020, acesso em 15 jun. 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

55. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, p. 156-57.

56. Ibid., p. 157.

57. Ibid., p. 188.

58. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: DOD, 2019), p. 65, acesso em 18 maio 2020, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

59. Ibid.

60. Verizon RISK Team, *2013 Data Breach Investigations Report* (New York: Verizon, 2013), p. 21, acesso em 18 maio 2020, https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigations-report-2013.pdf.

61. National Bureau of Asian Research, *Update to the IP Commission Report*, p. 11.

62. "Gen. Alexander: Greatest Transfer of Wealth in History", YouTube video, posted by "American Enterprise Institute", 9 July 2012, 1:27, acesso em 18 maio 2020, https://www.youtube.com/watch?v=JOFk44yy6IQ.

63. U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", news release no. 14-528, 19 May 2014, acesso em 18 maio 2020, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

64. Ibid.

65. FireEye iSight Intelligence, *Red Line Drawn: China Recalculates its Use of Cyber Espionage* (Milpitas, CA: FireEye, June 2016), p. 3 e p. 15, acesso em 18 maio 2020, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

66. Elsa Kania and John Costello, "The Strategic Support Force and the Future of Chinese Information Operations", *The Cyber Defense Review* 3, no. 1 (Spring 2018): p. 106-7.

67. U.S.-China Economic and Security Review Commission, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: U.S. Government Publishing Office, 2016), p. 57, acesso em 10 jun. 2020, https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf.

68. Edward Wong, "How China Uses LinkedIn to Recruit Spies Abroad", *New York Times* (site), 27 August 2019, acesso em 18 maio 2020, https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.

69. DOD 5220.22-M, *National Industrial Security Program Operating Manual* (Washington, DC: DOD, 2006, incorporating change 2, 18 May 2016), acesso em 18 maio 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODm/522022M.pdf.

70. Ibid.; "FAR [Federal Acquisition Regulation]", Acquisition.gov, last updated 15 May 2020, acesso em 18 maio 2020, https://www.acquisition.gov/browse/index/far; "Defense Federal Acquisition Regulation Supplement [DFARS]", Acquisition.gov, last updated 18 May 2020, acesso em 18 maio 2020, https://www.acquisition.gov/dfars.

71. Ron Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, rev. 2 (Gaithersburg, MD: National Institute of Standards and Technology, February 2020), acesso em 18 maio 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

72. "DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)", Office of the Under Secretary of Defense for Acquisition, 31 December 2019, 252.204-7012(m)(2), acesso em 10 mar. 2020, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

73. "DFARS 252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (Dec 2019)", Office of the Under Secretary of Defense for Acquisition, 31 December 2019, 252.204-7018, acesso em 18 maio 2020, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7018.