ARTIGO DOI 10.52781/cmm.a082

Ameaças ao Ciberespaço, Logística e Segurança Nacional Não Necessariamente nessa Ordem

Cyberspace, Logistics and National Security Threats, not Necessarily in that Order

Resumo: Qual a relação entre as vulnerabilidades cibernéticas, a logística e a segurança nacional? Preocupações com a potencial exploração das vulnerabilidades do ciberespaço para causar ineficiência logística em questões de segurança nacional perduram há quase um quarto de século. Este artigo atualiza o cenário desse debate e estende a análise às ameaças recíprocas representadas por essas três áreas. Uma metodologia descritiva, baseada em estudo de casos a partir de fontes governamentais, artigos acadêmicos e artigos de notícias, é usada para correlacionar ciberespaço, cadeias logísticas e segurança nacional. Demonstra-se que, para além do senso comum de que ciberataques podem explorar vulnerabilidades existentes em diferentes níveis da crescente automação presente nos sistemas logísticos, apresentando novas ameaças que podem incapacitar sistemas militares ou infraestruturas civis relevantes à segurança nacional, existe uma crescente ameaça posta pela complexidade logística aos produtos cibernéticos e à segurança nacional, bem como uma 'armamentização' (*weaponisation*) de decisões de segurança nacional de alguns países que põem em risco as cadeias de suprimento, cibernéticas ou não, de outras nações com reflexos no desenvolvimento de suas capacidades de defesa.

Palabras clave: ciberespaço; gestão de cadeias de suprimento; gestão estratégica.

Abstract: What is the relationship between cyber vulnerabilities, logistics and national security? Concerns about the potential exploitation of cyberspace vulnerabilities to cause logistical inefficiency in national security matters have lingered for nearly a quarter of a century. This article updates the landscape of this debate and extends the analysis to the reciprocal threats posed by these three areas. A descriptive methodology, based on case studies obtained from government sources, academic articles and news articles, is used to correlate cyberspace, logistics chains and national security threats. It is demonstrated that, in addition to common sense that the exploitation of existing cyber vulnerabilities at different levels of the increasing automation present in logistical systems presenting new threats that can disable military systems or civil infrastructures relevant to national security, there is a growing threat posed by the logistical complexity to cybernetic products and national security, as well as a 'weaponisation' of national security decisions of some countries that jeopardize supply chains, cybernetic or not, of other nations, with reflexes in the development of their defence capabilities.

Keywords: cyberspace; supply-chain management; strategic management.

Marcelo Malagutti
Instituto Vegetius.
Brasília, DF, Brasil.
marcelo.malagutti@vegetius.org.br

Recebido: 22 out. 2021
Aprovado: 25 jul. 2022

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introdução

Já é senso comum que a exploração de vulnerabilidades cibernéticas pode desativar ou danificar gravemente sistemas logísticos críticos e, assim, comprometer a segurança nacional. No entanto, esta seria a única ordem de causalidade entre essas variáveis? Este artigo argumenta que não. Como será demonstrado, evidências empíricas confirmam que as cadeias de suprimentos podem ser utilizadas para comprometer capacidades cibernéticas e impactar a segurança nacional. Da mesma forma, mostra-se que as decisões de segurança nacional de um país afetam as cadeias logísticas que criam vulnerabilidades cibernéticas para outros. Por conseguinte, sob certas condições, os três fatores podem estar causalmente relacionados em qualquer ordem.

Para isso, utiliza-se um método de pesquisa descritiva do tipo *associations* (GERRING, 2012). O método é aplicado usando as lentes do pensamento de Estudos Estratégicos, procurando padrões recorrentes de força efetiva (não necessariamente militar) para superar vontades opostas em situações de conflito. Esta abordagem permeia as obras de Clausewitz (1976), Liddell Hart (1930, 1931), Aron (2002), Beaufre (1965), Howard (1979), Freedman (1998, 2015), Gray (2008) e Stone (2007), para citar apenas alguns. A seleção de casos e documentos de referência abrangeu os últimos 10 anos, com a notável exceção do exercício Destinatário Elegível (Eligible Receiver), utilizado como balizador do problema idealizado.

O artigo está estruturado da seguinte forma. Após esta introdução, uma segunda seção apresenta uma breve introdução à logística, enquanto uma terceira descreve brevemente o seu encontro com o ciberespaço. Uma quarta seção apresenta dois exemplos clássicos de ciberataques que comprometeram sistemas de defesa, mostrando a ordem tradicional de relação de causalidade entre as três variáveis analisadas. Uma quinta seção exemplifica os riscos de incapacitação logística das forças militares no teatro de operações, tanto do ponto de vista de suprimentos quanto de comunicação e controle, exemplificando o caso de ciberataques que ameaçam a logística e a segurança nacional. Uma sexta seção apresenta as ameaças representadas pelos processos de fabricação de software e hardware, com uma cadeia de suprimentos composta por vários pontos de contato exploráveis para implementação de vulnerabilidades. Essa situação aponta para uma logística que ameaça a cibersegurança e a segurança nacional, com uma subseção discutindo os esforços dos governos para lidar com elas. Uma sétima seção discute o "armamentização" da cadeia de suprimentos cibernética, onde decisões de segurança nacional ameaçam a logística dos produtos cibernéticos. Finalmente, são feitas breves considerações sobre as conclusões deste trabalho.

2 Uma (Muito) Breve Introdução à Logística

Uma definição bem aceita de logística empresarial a apresenta como "o processo de planejamento, implementação e controle do fluxo e armazenamento eficiente e eficaz de bens, serviços e informações relacionadas desde o ponto de origem até o ponto de consumo em conformidade com os requisitos do cliente" (WOOD, 1998).

O estudo da Logística como ciência teve origem militar. Vegécio, no século IV ou V, já dedicava parte significativa de sua obra aos fundamentos do fornecimento de suprimentos militares (VEGETIUS, 1767). Além disso, o próprio termo deriva do *Major-General de Logis,* militar cuja função "antigamente era alojar e acampar as tropas, dar direção às marchas das colunas e localizá-las no solo" (JOMINI, 1862, p. 188). Ao longo dos anos, esse conjunto básico de funções foi ampliado com o aumento da complexidade dos exércitos e batalhas. Curiosamente, Clausewitz, muitas vezes considerado o mais influente teórico ocidental da guerra, nem propôs uma definição de logística nem usou um termo específico para descrevê-la. Isso leva acadêmicos a argumentar que ele a considerava "tudo o que é necessário para que a força de combate seja tida como certa" (PROENÇA JÚNIOR, DUARTE, p. 645).

Atualmente, nas ciências militares, Logística refere-se a "todas as atividades das unidades das forças armadas em funções de apoio às unidades de combate, incluindo transporte, abastecimento, comunicação de sinais, assistência médica e similares" (LEIGHTON, 2022). A dificuldade de encontrar um termo específico que possa, sem prejuízo, abranger e definir precisamente essa elaborada lista de atividades ainda permanece nos dias de hoje (LEIGHTON, 2022). A importância da logística para os militares é, de fato, expressa pela citação "amadores falam de tática, mas profissionais falam de logística", "atribuída a todos, de Napoleão Bonaparte a Omar Bradley" (EPSHTEIN; FAINT, 2019).

Cadeias de suprimentos são os fluxos de bens e informações dentro e entre organizações, "ligados por uma série de facilitadores tangíveis e intangíveis, incluindo relacionamentos, processos, atividades e sistemas de informação integrados" (PECK, 2012, p. 196). Elas são "o mecanismo no centro da globalização das últimas décadas pelo qual matérias-primas, peças e componentes são trocados através de múltiplas fronteiras nacionais antes de serem incorporados em produtos acabados" (SUPPLY..., 2019).

A aquisição, armazenamento e distribuição de centenas de milhares de itens de munição, armamento, veículos (com suas peças de reposição e serviços de manutenção correspondentes), combustível, uniformes, alojamento, alimentação, saúde e higiene, com cadeias de suprimentos complexas, que devem operar em terrenos difíceis, com meios de transporte restritos e em condições de combate, é uma tarefa de enorme complexidade.

O combustível e os armamentos devem ser armazenados numa zona de combate com munições suficientes para sua defesa. Caso contrário, o inimigo poderia tomar esses estoques de combustível e armamentos, com um duplo impacto negativo: perdê-los e vê-los usados contra seus proprietários originais. Portanto, é fundamental ter apenas o necessário e suficiente de cada item de suprimento em cada área de atuação. Os mesmos princípios se aplicam à logística civil: as corporações buscam eliminar estoques desnecessários com o mesmo esforço com que tentam evitar a indisponibilidade de itens que possam comprometer suas operações.

Apesar de operarem em cenários diferentes, as cadeias logísticas militares e civis perseguem, assim, os mesmos objetivos primários. O foco não é mais *orientado à massa,* mas *orientado à velocidade*, com apenas estoques necessários e suficientes, distribuição confiável, custos adequados, cadeias de suprimentos confiáveis e entrega *just-in-time* ou sob *demanda* (KRESS, 2002).

3 Onde a Logística e o Ciberespaço se Encontram

A efetividade, combinação resultante de eficiência (fazer as coisas corretamente) com eficácia (fazer o que precisa ser feito), é um imperativo para a logística. Como tal, a automatização tem sido historicamente associada à gestão da cadeia de suprimentos.

A logística moderna exige informações dinâmicas sobre toda a cadeia de suprimentos, denominada 'In-Transit View' (KRESS, 2002). Tais controles são fortemente apoiados por sistemas informatizados, seja qual for a forma de contratação, controle de custos, estoque ou distribuição adotada. Os dados gerados em pontos dispersos, seja de requerentes, fornecedores ou transportadores, são coletados e processados de forma integrada em tempo real. O usuário informa sua posição e necessidade; o sistema verifica a disponibilidade dos fornecedores e informa o preço e a previsão de chegada (ETA) ao usuário, que pode confirmar ou não o pedido. Se o aceite for estabelecido, o usuário pode acompanhar o movimento do item em direção a ele e a ETA ajustada em tempo real.

Da mesma forma, os sistemas informatizados permitem dimensionar a demanda, determinar a localização e o tamanho dos estoques, demandar fornecedores, às vezes até mesmo sem interação humana, controlar e monitorar a distribuição dos itens, e também determinar a mudança de planos operacionais, proporcionando 'visibilidade total do ativo' (KRESS, 2002).

Veículos autônomos, bem como inteligência artificial, "podem alterar fundamentalmente como as cadeias de suprimentos operam e usam seus dados, sistemas e ativos integrados"; esses novos níveis de automação aumentarão a eficiência e reduzirão os custos operacionais (TURNBULL, 2018, p.45). Como parte fundamental do que hoje é chamado de Indústria 4.0, espera-se que a Manufatura Aditiva (impressão 3D) possibilite a produção local de itens e peças de reposição sob demanda, simplificando assim as necessidades de transporte e armazenamento e riscos associados. Em 2015, o Laboratório de Pesquisa de Engenharia de Construção do Centro de Pesquisa e Desenvolvimento de Engenheiros do Exército dos EUA estabeleceu a Construção Automatizada de Estruturas Expedicionárias (ACES). Tem como objetivo desenvolver tecnologia de impressão 3D confiável e fácil de usar, capaz de gerar estruturas expedicionárias militares personalizadas sob demanda, em campo, usando materiais disponíveis localmente (JAGODA *et al.*, 2020, p. 2). Em janeiro de 2021, o Departamento de Defesa dos EUA divulgou sua Estratégia de Manufatura Aditiva para alinhar a impressão 3D com a missão do DoD (UNITED STATES, 2021a, p. 4). Os militares dos EUA já podem "imprimir" peças de reposição para submarinos, Humvees e até bombardeiros estratégicos B-52, e encomendaram uma unidade de fabricação 3D portátil do tamanho de um contêiner que poderia ser desdobrada em terra e mar (BURTON; MCBIRNEY, 2022; SCHWAAR, 2022).

No entanto, apesar do quão vitais são os prós do aumento da automação, eles também possuem contras relevantes. Com o impulso para a automação, os sistemas logísticos se tornarão cada vez mais conectados e segmentáveis (TURNBULL, 2018). Não surpreendentemente, o relatório do Departamento de Defesa dos EUA emitido em 2022, em atenção à Ordem Executiva sobre Cadeias de Suprimentos da América de 2021, faz 88 referências a termos "cibernéticos", mais de um terço das 251 referências a "cadeia de suprimentos" (BIDEN JR, 2022; UNITED STATES, 2022a).

Os avanços tecnológicos levantam o espectro de uma corrida armamentista na segurança da cadeia de suprimentos, com hackers privados e patrocinados pelo Estado tendo vantagem sobre corporações e governos (SUPPLY..., 2019). Além disso, as cadeias de suprimentos já são um dos "três principais vetores de ataque cibernético" (junto com redes e pessoas internas) (NYE JR, 2017, p. 50). Portanto, ainda há muito esforço a ser feito para proteger as cadeias de suprimentos contra ataques por meio de dispositivos computacionais (LEE; MOLTKE, 2019).

4 Ameaças Cibernéticas aos Sistemas Logísticos de Segurança Nacional

Esta seção apresenta o caso clássico de ameaças cibernéticas que arriscam a logística relevante para a Segurança Nacional.

Quase um quarto de século atrás, em junho de 1997, o Estado-Maior Conjunto dos EUA realizou um exercício denominado *Eligible Receiver* para testar as defesas cibernéticas americanas. O cenário proposto era o de uma crise que obrigaria Washington a enviar rapidamente tropas e aviões para a Coreia do Sul. Trinta e cinco especialistas da Agência de Segurança Nacional (NSA) compuseram a 'equipe vermelha', simulando hackers a serviço da Coreia do Norte com a missão de subverter a operação americana, utilizando apenas equipamentos e informações publicamente disponíveis. Em apenas duas semanas, usando somente computadores comerciais e programas de hackers baixados da Internet, essa equipe vermelha conseguiu "invadir simultaneamente as redes elétricas de nove cidades americanas e quebrar seus sistemas de emergência 911" (ADAMS, 2001, p. 101).

"Tendo assegurado o caos civil e distraído Washington", os hackers atacaram as redes de computadores do Pentágono, conseguindo "circular livremente pelas redes, semeando destruição e desconfiança por onde passassem" (ADAMS, 2001, p. 101). Por exemplo, direcionar suprimentos para destinos errados, potencialmente paralisando aeronaves de combate de última geração devido à falta de combustível, peças sobressalentes e armas (ADAMS, 2001).

Da mesma forma, a exploração de vulnerabilidades cibernéticas na logística militar pode estar por trás da desativação de radares e baterias antiaéreas computadorizadas, como os israelenses provavelmente fizeram na Operação Orchard antes de embarcarem em um ataque aéreo contra as supostas instalações nucleares da Síria em Deir Ez-Zor. (LIFF, 2012).

Atualmente, o Conselho de Ciência da Defesa dos EUA (DSB) considera os impactos de um ataque cibernético contra as cadeias de suprimentos potencialmente espetaculares. Sempre que os EUA estiverem em conflito, devem esperar por ataques cibernéticos com a intenção de corromper suas cadeias de suprimentos, fazer com que seus mísseis e bombas não funcionem ou até mesmo usá-los contra as próprias tropas americanas. Suprimentos, incluindo comida, água, munição e combustível, podem não chegar aonde ou quando necessários. Os comandantes militares perderiam rapidamente a confiança nas informações e na capacidade de controlar seus sistemas e forças. Uma vez perdida, a confiança é difícil de recuperar (UNITED STATES, 2013b).

Em 2013/14, o Comitê de Serviços Armados do Senado dos EUA investigou ataques cibernéticos envolvendo o Comando de Transporte do Departamento de Defesa (DoD) dos EUA (TRANSCOM) e onze de seus fornecedores. O relatório resultante observa que o comitê se con-

centrou no TRANSCOM devido ao seu papel central em "operações de mobilização, implantação e sustentação e os recursos críticos que os contratados do TRANSCOM fornecem para atender aos requisitos militares em operações de contingência" (BRYAN *et al.*, 2014). O relatório afirma que as companhias aéreas privadas fornecem mais de noventa por cento da capacidade de movimentação de passageiros e mais de um terço da capacidade bruta de movimentação de carga do DoD, enquanto 95% de sua carga seca é transportada por navios mercantes. Além disso, mais de 90% das transações de implantação e distribuição do DoD ocorrem em redes não classificadas, muitas das quais pertencem a empresas privadas, de acordo com uma estimativa do comandante do TRANSCOM (BRYAN *et al.*, 2014).

A investigação do TRANSCOM identificou 50 ataques cibernéticos ou intrusões realizadas entre 1 de junho de 2012 e 30 de maio de 2013. Além disso, pelo menos 20 intrusões bem-sucedidas em redes contratadas foram classificadas como Ameaças Persistentes Avançadas (APT). O termo é "usado para distinguir ameaças cibernéticas sofisticadas que são frequentemente associadas a governos estrangeiros"; destes, o comando foi informado de apenas dois, "uma descoberta preocupante, dado o impacto potencial das intrusões cibernéticas nas informações e operações de defesa" (BRYAN *et al.*, 2014, p. i).

Entre os motivos pelos quais o TRANSCOM desconhecia os ataques, constatou-se a existência de lacunas nos requisitos contratuais de comunicação, além da falta de entendimento comum entre a contratada e suas subcontratadas quanto ao alcance do que deve ser relatado em relação aos ciberataques. Além disso, o Departamento Federal de Investigação (FBI) e o DoD muitas vezes desconheciam que as empresas identificadas como vítimas de ataques cibernéticos eram fornecedoras desse comando (BRYAN *et al.*, 2014).

O Planejamento Estratégico 2015-2022 da Agência de Logística de Defesa dos EUA (DLA) estabeleceu que a segurança cibernética constitui um risco operacional significativo que impõe desafios severos às cadeias de suprimentos da DLA em todos os momentos. Assim, é necessário criar um ambiente que estimule a denúncia e o combate às ameaças cibernéticas e que a mesma atenção seja estendida à sua base de fornecedores, onde a DLA deve ser 'astuta' na gestão do relacionamento para garantir que os parceiros do setor privado protejam os suprimentos e a integridade de dados para fornecer apoio eficaz aos combatentes (UNITED STATES, 2015). A astúcia pretendida pode ser refletida no uso de PBL para 'estimular' fornecedores.

A investigação do Senado dos EUA descobriu que todos os APTs identificados no TRANSCOM e seus fornecedores foram atribuídos à China. Também indicou que os analistas militares chineses identificaram a logística e a mobilização como potenciais vulnerabilidades dos EUA, "dados os requisitos de precisão nas redes de coordenação, transporte, comunicações e logística" e que a doutrina militar chinesa "advoga visando o comando e controle do adversário e logística redes para impactar sua capacidade de operar durante os estágios iniciais do conflito". Além disso, a investigação descobriu que especialistas americanos em planejamento militar chinês levantaram a possibilidade de a China usar capacidades cibernéticas para impedir o envio de forças dos EUA em caso de contingência (BRYAN *et al.*, 2014). Assim, os chineses poderiam buscar obter, em um eventual conflito com os EUA, as mesmas vantagens obtidas pela equipe vermelha da NSA em Eligible Receiver, há 25 anos.

Possivelmente o efeito mais relevante do Eligible Receiver foi o fato de que os hackers também conseguiram paralisar o sistema de Comando e Controle (C2) humano com um alto nível de desconfiança decorrente de ordens falsas de um general comandante, forjando "notícias falsas sobre a crise e instruções das autoridades civis de comando" (ADAMS, 2001, p. 101).

> "Como resultado, ninguém na cadeia de comando, do presidente em diante, podia acreditar em qualquer coisa. Este grupo de hackers que utilizava recursos disponíveis publicamente foi capaz de impedir que os Estados Unidos travassem uma guerra de forma eficaz" (ADAMS, 2001, p. 101).

C2 é também uma função logística militar. Embora não intrinsecamente uma capacidade militar cibernética como muitas outras, tornou-se tão dependente do ciberespaço que um oponente pode ser tentado a buscar um primeiro ataque cibernético incapacitante contra ela (MORGAN, 2010). Esse processo de degradação ciber-C2, destinado a destruir (ou pelo menos degradar amplamente) a coesão interna do oponente, poderia potencialmente incapacitar as forças militares do inimigo alvo e aumentar a eficácia de um ataque cinético subsequente contra eles.

Além disso, o armamento moderno tem sido cada vez mais dependente de circuitos integrados, e hoje a eletrônica contém código programável de complexidade crescente. Ao mesmo tempo, o DoD tornou-se um comprador muito menos influente numa vasta e globalizada base de fornecedores. Por isso, garantir que os componentes eletrônicos de defesa estejam livres de vulnerabilidades é uma tarefa hercúlea (UNITED STATES, 2017).

Como as definições de configuração desses dispositivos permanecem inalteradas por longos períodos, os componentes comprometidos podem criar vulnerabilidades persistentes, e explorar essas vulnerabilidades em componentes ou em seus softwares incorporados pode causar falhas nos armamentos modernos. Essas explorações são particularmente prejudiciais porque é difícil diferenciá-las de falhas elétricas ou mecânicas.

Além disso, um ciberataque em si não tem que ser letal. Se degradar a eficácia de uma força militar ou reduzir a funcionalidade de armas de precisão e sistemas de mira ou a disponibilidade de combustível e suprimentos médicos, o resultado será mortal para a força dependente de recursos comprometidos (TURNBULL, 2018).

Ainda assim, no âmbito da Segurança Nacional, além das ameaças cibernéticas à logística militar e C2, há também a ameaça cibernética frequentemente mencionada à infraestrutura crítica civil. Até recentemente, os casos mais famosos foram aqueles envolvendo o fornecimento de energia da Ucrânia em 2015, chamado Industroyer, e 2016, chamado CrashOverride, possivelmente lançado por hackers russos (AUCHARD; FINKLE, 2016; ZETTER, 2016). No entanto, em maio de 2021, um ataque de ransomware atribuído a um grupo cibercriminoso russo chamado DarkSide atingiu o Colonial Pipeline, deixando vastas partes dos EUA com suprimentos restritos de derivados de petróleo (SANGER; PERLROTH, 2021).

5 Ameaças Logísticas aos Produtos Cibernéticos

Esta seção discute o caso em que a logística ameaça os produtos cibernéticos e a Segurança Nacional. É senso comum que um parafuso, fusível ou componente químico adulterado em uma cadeia de suprimentos longa e difícil de controlar pode afetar o desempenho ou criar vulnerabilidades físicas em qualquer equipamento militar. Um entendimento menos perceptível, no entanto, é que, da mesma forma, componentes adulterados na cadeia de suprimentos estendida de produtos de hardware ou software podem afetar o desempenho ou criar vulnerabilidades neles e nos sistemas que os utilizam. Para melhor captar esse conceito, é necessário entender a cadeia de suprimentos dos produtos cibernéticos, que o Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) chama de Cadeia de Suprimentos Cibernética (NIST; FIREEYE, 2015).

Já em 2001, oficiais de inteligência americanos acreditavam "que certos equipamentos e softwares importados da Rússia, China, Israel, Índia e França" estavam infectados com "dispositivos" capazes de "ler dados e destruir sistemas", embora essa suspeita fosse difícil de provar (ADAMS, 2001). Recentemente, hardware falsificado foi identificado em sistemas adquiridos pelo DoD (LYNN III, 2010). Como resultado, um relatório da Comissão Permanente de Inteligência da Câmara dos EUA em 2012 restringiu a compra de equipamentos das empresas chinesas Huawei e ZTE (ROGERS; RUPPERSBERGER, 2012).

Os sistemas digitais atuais são altamente complexos, construídos pela sobreposição de componentes de software e hardware integrados em diferentes níveis e fornecidos por vários fornecedores de diversas partes do mundo. A materialidade do hardware o torna facilmente perceptível, e os humanos são mais propensos a entendê-lo e aceitá-lo como arriscado ou inseguro. No entanto, o software é o que 'anima' o hardware.

No nível de software muito básico, os dispositivos eletrônicos geralmente são controlados por *firmware,* software gravado em seus componentes. Ele determina como o equipamento funciona. Um exemplo famoso é o Basic Input Output System (BIOS) de processadores, mas também existe em placas de circuito de rede e vídeo, scanners ou impressoras. Cada vez mais, o hardware oferece a possibilidade de atualizar seu firmware, alterando assim o comportamento operacional do dispositivo sem a necessidade de substituí-lo. O malware pode explorar vulnerabilidades de firmware, por exemplo, inserindo um 'interruptor' que pode desativar o hardware sob ordens dos inimigos. Possivelmente pior, o malware pode fazer com que os dispositivos se comportem de forma irregular.

O firmware usa outra camada de software, o *driver*, para se comunicar com *Sistemas Operacionais* (SO) como Android, iOS, Windows ou Linux. O mesmo par hardware-firmware (uma impressora, por exemplo) tem drivers diferentes para se comunicar com SO diferentes. Um driver adulterado pode modificar o funcionamento de um dispositivo, enganando o SO. Este foi o princípio por trás do Stuxnet, onde os Controladores Lógicos Programáveis (PLCs) que conectam as centrífugas de enriquecimento de urânio iranianas ao seu sistema de Supervisão de Controle e Aquisição de Dados (SCADA) foram substituídos por outros modificados. Assim, enquanto o sistema de controle indicava que as centrífugas estavam operando regularmente, elas estavam realmente girando fora do ritmo previsto e, portanto, sendo fisicamente danificadas (ZETTER, 2015a).

Em um nível mais alto, é possível contaminar o próprio SO. No caso Snowden, foi revelado que a Cisco, maior fabricante mundial de ativos de rede, teve o SO de seus roteadores e servidores (Cisco IOS) manipulado pela NSA (GREENWALD, 2014). Em dezembro de 2015, a Juniper Networks, segunda maior fabricante mundial de ativos de rede, anunciou a descoberta de uma backdoor secreta no JunOS, o sistema operacional de seus firewalls. Verificou-se que ela tinha sido inserida no código antes de 2011 (ZETTER, 2015b). Não ficou claro quem teria implantado essa backdoor.

Em agosto de 2016, a Cisco, novamente, anunciou a descoberta de uma vulnerabilidade de dia-0 (de fábrica) no Cisco IOS, implantada 13 anos antes, que poderia ser explorada para garantir acesso total às redes usando seus equipamentos. Foi encontrada ao se analisar o código-fonte supostamente pertencente ao Equation Group (hackers ligados à NSA) que foi 'vazado' na Internet pelo grupo de hackers Shadow Brokers (GOODIN, 2016). Portanto, a NSA poderia ter explorado essa vulnerabilidade para violar redes de computadores de interesse dos EUA. A Cisco encontrou pelo menos oito outras backdoors semelhantes em seu sistema operacional em 2017 e 2018 (CIMPANU, 2018; CISCO, 2017).

O nível de software seguinte é chamado de *middleware,* o "software que fica entre um sistema operacional e os aplicativos executados nele", "funcionando essencialmente como camada de tradução oculta" e permitindo comunicação e gerenciamento de dados para aplicativos (MICROSOFT, 2022). Esta categoria inclui gerenciadores de bancos de dados e servidores web, entre outros. Os aplicativos (Apps) se conectam a eles por meio de bibliotecas de software chamadas Interfaces de Programação de Aplicativos (APIs) ou Kits de Desenvolvimento de Software (SDKs). Essas APIs, que geralmente são desenvolvidas por fornecedores terceirizados em diferentes partes do mundo, podem ser alteradas no processo de integração.

Quase na camada de software superior está o software Commercial-Off-The-Shelf (COTS), como plataformas de automação de escritório, sistemas de e-mail, geradores e leitores de pdf e centenas de outros. Arquivos de documentos portáteis da Adobe (PDFs) e documentos do Microsoft Office 'armamentizados' vêm comprometendo os sistemas há algum tempo (HUTCHINS; AMIN; CLOPPERT, 2010).

Finalmente, a camada de software superior é aquela dos aplicativos especializados, que operam os "negócios principais" das organizações, como sistemas de logística. A complexidade das aplicações modernas transformou o desenvolvimento de software em uma linha de montagem, num contexto de desenvolvimento colaborativo, com componentes muito especializados (APIs) adquiridos de terceiros, criando assim cadeias de suprimento muito longas (SHERMAN, 2019).

Grande parte desses componentes são *caixas pretas,* com seu código-fonte invisível, embora o Open-Source Software (OSS) esteja ganhando espaço na indústria de software e aceitação no meio militar (UNITED STATES, 2021b). A cadeia de suprimentos de software tornou-se uma teia complexa de componentes dentro dos componentes de código confiáveis baixados de uma organização e usados para criar aplicativos (BLESSMAN, 2019). Além disso, o software é "extremamente maleável sob pressão da combinação certa de toques dos dedos, o que pode trazer vantagens e fraquezas estratégicas quando incorporado ao mundo através da dependência de tecnologia conectada" (WOODS; BOCHMAN, 2018).

No geral, essa complexidade torna crucial manter esses vários componentes atualizados, e o gerenciamento contínuo de patches de software é necessário. O gerenciamento de patches de software é complicado pela fragilidade dos ambientes de produção, onde uma infinidade de aplicativos e pacotes de suporte devem interagir sem causar conflitos ou falhas catastróficas (TURNBULL, 2018).

Além disso, uma versão adulterada do software de uma empresa de contabilidade ucraniana contendo uma carga destrutiva, chamada NotPetya, paralisou redes globalmente, custando à FedEx e à Maersk, duas gigantes da logística, mais de US$ 300 milhões cada. (UNITED STATES, 2018). Mecanismos de atualização de software (sistemas de entrega, de fato!) foram abusados para obter acesso aos sistemas de controle de rede (WOODS; BOCHMAN, 2018).

Em outro caso famoso, em 2017, cerca de 2,2 milhões de clientes foram infectados com uma backdoor quando hackers, visando empresas como Samsung, Sony, Asus, Intel, VMWare, O2 e Fujitsu, sequestraram o sistema de atualização automatizada do CCleaner, um antivírus e software de segurança (CORERA, 2018; UNITED STATES, 2018).

Recentemente, investigações revelaram que a SolarWinds, uma empresa dos EUA que produz um software de gerenciamento de rede de TI chamado Orion, havia sido infectada em outubro de 2019. O comprometimento dessa cadeia de suprimentos permitiu o uso da atualização de segurança de software de rotina do Orion para instalar software malicioso nas redes dos clientes da SolarWinds. Esse comprometimento garantiu o acesso dos hackers a pelo menos nove agências federais dos EUA, incluindo o Departamento do Tesouro e o Departamento de Justiça, e a "principais equipamentos de tecnologia digital, como Cisco, Intel, Nvidia e Microsoft, bem como segurança cibernética. empresas como a FireEye" (WILLETT, 2021, p. 8).

A complexidade da cadeia de suprimentos de software desafia a maioria dos programas de segurança corporativa, uma vez que componentes adulterados se tornam difíceis de detectar e "as organizações simplesmente confiam que seus fornecedores estão fornecendo software seguro, oferecendo aos agentes de ameaças uma solução alternativa para derrotar os procedimentos de segurança de uma organização" (BLESSMAN, 2019, p. 10).

Vulnerabilidades na cadeia de suprimentos podem ser inseridas ou descobertas ao longo de todo o ciclo de vida de um produto de software, dando especial atenção ao fato de que a maioria dos sistemas são desenvolvidos, adquiridos e distribuídos sem planos formais de proteção (UNITED STATES, 2017).

5.1 Lidando com a Cadeia de Suprimento Cibernética

A Estratégia do DoD de 2011 para operar no ciberespaço apresentou vulnerabilidades e ameaças da cadeia de suprimentos à capacidade operacional do DoD como um dos "aspectos centrais da ameaça cibernética" (UNITED STATES, 2011). Também afirma que:

> Software e hardware correm o risco de adulteração maliciosa mesmo antes de serem integrados a um sistema operacional. A maioria dos produtos de tecnologia da informação usados nos Estados Unidos são fabricados e montados no exterior. A dependência do DoD na fabricação e desenvolvimento estrangeiros cria desafios no gerenciamento de riscos nos pontos de projeto, fabricação, serviço, distribuição e descarte (UNITED STATES, 2011, p. 3).

Intuitivamente, alguém pode se sentir tentado a propor que o governo aprove hardware e software estrangeiros antes que eles entrem no mercado. Na prática, porém, isso não seria viável. O número de linhas de código-fonte (SLOC) para produtos de software comercial cresceu para aproximadamente cinquenta milhões, e o governo dos EUA acredita que esse crescimento continuará nas próximas décadas (UNITED STATES, 2013b). No lado do hardware, os circuitos integrados complexos hoje têm mais de dois milhões de transistores. É, portanto, impossível testar completamente as falhas e vulnerabilidades de tais produtos de software ou hardware. Tentar verificá-los na íntegra levaria anos.

Estes produtos complexos entram frequentemente no mercado com bugs. Por exemplo, em 1994, logo depois que os novos processadores Pentium entraram no mercado, foi revelado um bug na divisão de números de ponto flutuante, tornando-a bastante imprecisa (HALFHILL, 1995). Em 2020, foi descoberta uma nova falha presente em todos os processadores da empresa produzidos nos últimos cinco anos, que poderia ser explorada para obter acesso à segurança do sistema (BLUMENTHAL, 2020).

Em 2014, o NIST publicou seu Framework for Improving Critical Infrastructure Cybersecurity em uma parceria entre o governo dos EUA e o setor privado, tendo em mente que "semelhante ao risco financeiro e de reputação, o risco de segurança cibernética afeta os resultados de uma empresa" (NIST, 2014). O princípio central é que a cibersegurança na cadeia de suprimentos não diz respeito apenas à tecnologia da informação e comunicação (TIC), mas envolve fornecedores, revendedores, gerenciamento, continuidade e confiabilidade da cadeia de suprimentos, segurança do transporte e outras atividades de segurança.

Com base em seu framework, o NIST passou a pesquisar não apenas empresas de TIC, mas também empresas que utilizam amplamente produtos de TIC em seus processos. Entre as empresas participantes estão Boeing, Cisco, Deere, Dupont, Fire Eye, Fujitsu, Intel, Juniper, Northrop Grumman, P&G e concessionárias de serviços públicos (ou infraestrutura). O objetivo era detectar como as empresas lidam com questões como as abaixo (NIST, 2014):

- Fornecedores terceirizados com acesso físico ou virtual a sistemas de informação, códigos fonte de programas ou equipamentos (desde limpeza até engenharia de software);

- Práticas inadequadas de segurança da informação por parte dos seus fornecedores;

- Produtos de hardware ou software comprometidos adquiridos de fornecedores;

• Vulnerabilidades de segurança de software no gerenciamento da cadeia de suprimentos ou sistemas de fornecedores;

• Hardware falsificado ou malware incorporado;

• Armazenamento ou agregação de dados por terceiros;

• Repetibilidade e rastreabilidade do processo de projeto e desenvolvimento de software ou hardware;

• Capacidades do fornecedor para resolver vulnerabilidades, incluindo 0 dias.

Assim, há uma preocupação crescente do governo dos EUA em relação à garantia do Gerenciamento de Risco da Cadeia de Suprimentos Cibernética (C-SCRM) com seus fornecedores, e estes com os deles, de forma recursiva (NIST; FIREEYE, 2015).

Quando um governo compra produtos ou serviços com *fabricação* inadequada ou segurança *integrada*, os riscos persistem durante todo o ciclo de vida do item adquirido. Este efeito duradouro faz parte do que torna a mudança nos processos de aquisição tão importante para alcançar a cibersegurança e a resiliência. A compra de produtos e serviços com a segurança de fábrica integrada adequada pode ter custos iniciais mais elevados. Ainda assim, reduz o custo total de propriedade (TCO) devido à mitigação de riscos e à redução da necessidade de correção de vulnerabilidades em produtos distribuídos ou implantados em campo (UNITED STATES, 2013a).

Em processos de aquisição tipicamente longos do DoD, cerca de 70% dos eletrônicos em sistemas de armas estão obsoletos ou fora de produção antes que esses produtos sejam implantados (UNITED STATES, 2017). Isso faz com que novos componentes sejam inseridos durante o processo de produção, o que dificulta ainda mais a validação da integridade desses componentes.

Como resultado, o malware pode ser implantado em sistemas informatizados (hardware + software) à medida que são desenvolvidos ou construídos e potencialmente usados para criar 'interruptores' e backdoors operados remotamente, permitindo que invasores manipulem os sistemas em execução em situações de conflito. Para conter este risco, as empresas privadas de software e hardware nos Estados Unidos tornaram-se parceiras governamentais na criação de mecanismos de segurança. Por exemplo, a Microsoft e outras empresas de computadores desenvolvem estratégias sofisticadas para detectar códigos maliciosos (como as backdoors da Juniper Networks e Cisco) e impedir sua implantação em suas cadeias de suprimentos globais (LYNN, 2010). Apesar de, em março de 2021, uma falha no produto servidor de e-mail Microsoft Exchange ter sido usada por hackers chineses para obter acesso aos dados e e-mails dos usuários, afetando "até 30.000 entidades públicas e privadas, principalmente pequenas empresas e governos locais" (WILLETT, 2021).

6 Armamentização de Segurança Nacional da Cadeia de Suprimento Cibernética

Por fim, esta seção descreve como as decisões de Segurança Nacional em relação às restrições de exportação e importação armamentizam as cadeias de suprimento cibernéticas, apresentando ameaças à cadeia de logística cibernética de outros países. Isso exemplifica o terceiro caso estudado, em que as decisões de Segurança Nacional afetam o ciberespaço e as cadeias logísticas em países estrangeiros.

Desde 2015, o governo dos EUA impede a Intel de revender seus processadores mais modernos para a China, supostamente porque seriam usados para testes nucleares (CLARK, 2015). Em 2018, o país recuperou as duas primeiras posições na lista de supercomputadores, anteriormente ocupadas pela China (TOP500.ORG, 2020). A diferença entre os processadores reflete-se nos números apresentados. Enquanto o U.S. Sierra, em primeiro lugar, chega a 200 PFLOPS com 2,4 milhões de núcleos e consome 10 MW de energia, o chinês TaihuLight, terceiro da lista, usando processadores chineses, chega a 125 PFLOPS com 10,6 milhões de núcleos e consome 15 MW (TOP500.ORG, 2020).

A solução chinesa preferida, típica de qualquer país em desenvolvimento, é substituir soluções estrangeiras por nativas, uma solução que requer uma forte capacidade de inovação e, contraintuitivamente, conexões globais (LEWIS, 2018). A China usa "campeões nacionais, protege-os no mercado doméstico e os ajuda a competir" globalmente (LEWIS, 2018, p. 5-6). "[Se] a China não tivesse bloqueado o Google, não haveria Baidu" (LEWIS, 2018, p. 5-6). No entanto, "esta promoção de campeões nacionais por qualquer meio é a fonte de grande parte das atuais tensões comerciais, e os governos ocidentais estão lentamente desenvolvendo respostas que restringirão o crescimento da China, a menos que suas políticas mudem" (LEWIS, 2018, p. 5-6).

Mais de 25 séculos atrás, Sun Tzu escreveu:

> Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se conheces a ti mesmo, mas não ao inimigo, por cada vitória conquistada sofrerás também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, sucumbirá em todas as batalhas (TZU, 2009, p. 13).

Ter informações de inteligência faz parte do senso comum da política. Além disso, as agências de inteligência estão sempre procurando oportunidades de coletar informações confidenciais por meio de redes e dispositivos de TIC, mesmo em tempos de paz, e relacionadas a parceiros e aliados tradicionais. Nem mesmo equipamentos fornecidos por empresas de países tradicionalmente neutros podem ser considerados insuspeitos e inalcançáveis por seus tentáculos. Por exemplo, a empresa suíça Crypto AG, fabricante de criptógrafos usados em mais de 120 países, fez parte, entre 1970 e 2018, de uma parceria altamente sigilosa entre a CIA e o serviço de inteligência alemão BND. O equipamento da Crypto AG foi sabotado para que essas agências pudessem acessar as informações que esses dispositivos encriptaram (MILLER, 2020). Em outro caso famoso, Snowden deixou claro que a NSA estava espionando dezenas de aliados dos EUA, incluindo Alemanha, Brasil, Japão e México (GREENWALD, 2014).

Agora, o governo dos EUA acusa a Huawei, líder mundial em telefonia 5G, de ter ligações obscuras com a inteligência chinesa. Além disso, os EUA argumentam que preferem o uso de equipamentos da sueca Ericsson ou da finlandesa Nokia, ainda que mais caros, e personalidades do governo norte-americano chegaram a sugerir a aquisição de ações para controlar essas empresas (KHARPAL, 2020).

Os Estados Unidos também estão pressionando seus aliados a vetar o uso da tecnologia chinesa 5G. Em maio de 2020, o Reino Unido anunciou a proibição de atuação da empresa. A alemã Deutsche Telekom (32% estatal) respondeu que excluir a Huawei de suas redes 5G seria o 'Armagedom' e, embora não restringindo sua participação, anunciou recentemente que a Ericsson foi escolhida (ALLEVEN, 2020; ERICSSON, 2020; PETZINGER, 2020). Sob enorme pressão dos EUA quanto à participação da Huawei nas redes brasileiras, com o embaixador dos EUA ameaçando 'consequências', os militares brasileiros teriam dito ao seu governo que "a mesma eventual exposição que o Brasil pode sofrer da tecnologia chinesa com a Huawei também ocorrerá com qualquer outra empresa" (AMADO *et al.*, 2020; ROSA; ANTUNES, 2020). Na verdade, uma posição muito pragmática, considerando os casos Crypto AG, Cisco e Juniper, entre outros.

Do lado chinês, em 2017, uma nova lei de cibersegurança restringiu a venda de tecnologias de informação e comunicação estrangeiras. Além disso, a China exigiu que as empresas estrangeiras submetessem esses produtos a análises de Segurança Nacional administradas pelo governo e que as empresas que operam na China armazenassem seus dados na China, exigindo aprovação oficial antes de serem transferidos para outros países. (UNITED STATES, 2018). Como está claro que as revisões de segurança serão longas e imperfeitas, essa parece ser uma forma de criar barreiras para a tecnologia estrangeira, um contra-ataque devido às restrições ocidentais à Huawei.

Excluída do mercado dos EUA em 2019, a Huawei respondeu proibindo o uso de componentes norte-americanos. A gigante chinesa começou a trabalhar para substituir esses componentes por versões chinesas (STRUMPF, 2020). No entanto, mesmo essa estratégia foi ameaçada quando o Departamento de Comércio dos EUA intensificou as restrições em maio de 2020, proibindo os fabricantes de componentes que usam a tecnologia dos EUA em todo o mundo de vender produtos para a Huawei (UNITED STATES, 2020). Essa nova dificuldade pode até tirar a empresa de sua posição dominante na corrida 5G e colocar em risco a manutenção das redes telefônicas de outras gerações fornecidas pela empresa e já em uso em diversos países (STRUMPF, 2020). Além disso, os EUA agora estão considerando bloquear o fornecimento de tecnologia dos EUA para cinco empresas chinesas de vigilância por vídeo (SHIDONG, 2019).

As restrições à utilização não se referem apenas ao hardware, mas também ao software. A proibição do governo dos EUA à Huawei impede o Google de licenciar o uso do sistema operacional Android em telefones da empresa (MOON, 2019). Embora o núcleo do Android seja de código aberto, podendo continuar a ser utilizado pela empresa chinesa, vários serviços associados são fornecidos pelo Google e deixariam de estar disponíveis, limitando a utilidade dos smartphones da Huawei (MOON, 2019).

Em meio ao embargo dos EUA ao fornecimento de tecnologia à China, Pequim ordenou que todos os escritórios do governo e instituições públicas removessem equipamentos e software estrangeiros até 2022 (YANG; LIU, 2019). A medida faz parte de uma campanha para reduzir a dependência Chinesa de tecnologias estrangeiras, sendo provável que dissocie as cadeias de suprimento entre os EUA e a China e podendo significar um golpe significativo para as empresas dos EUA (YANG; LIU, 2019). As novas sanções impostas acrescentaram urgência ao projeto. Ao contrário dos esforços anteriores para a autossuficiência em tecnologia, o objetivo é que as empresas e o governo em breve estejam livres de ameaças (YANG; LIU, 2019).

No entanto, a substituição de hardware e software dos EUA por equivalentes chineses também apresenta problemas. A chinesa Lenovo utiliza processadores fabricados pela Intel e discos rígidos fabricados pela sul-coreana Samsung (YANG; LIU, 2019). A China fica atrás dos EUA em algumas das tecnologias mais avançadas, incluindo design e fabricação de chips. A Intel e a Qualcomm fabricam os principais componentes de algumas das maiores empresas de tecnologia do país. O sistema operacional mais usado em dispositivos produzidos na China é o Google Android, em smartphones e tablets, ou o Microsoft Windows, em computadores (SHIDONG, 2019).

Em 2019, os EUA elevaram o tom com a Ordem Executiva sobre a Segurança da Cadeia de Suprimento de Tecnologia e Serviços de Informação e Comunicação, que afirma:

> A aquisição ou uso irrestrito nos Estados Unidos de tecnologia de informação e comunicação ou serviços projetados, desenvolvidos, fabricados ou fornecidos por pessoas pertencentes, controladas ou sujeitas à jurisdição ou direção de adversários estrangeiros aumenta a capacidade de adversários estrangeiros de criar e explorar vulnerabilidades em tecnologia ou serviços de informação e comunicação, com efeitos potencialmente catastróficos e, portanto, constituir uma ameaça incomum e extraordinária à segurança nacional, política externa e economia dos Estados Unidos (TRUMP, 2019, n.p.).

Então, em 2020, o confronto EUA-China ganhou um novo capítulo, envolvendo o aplicativo TikTok, usado para postar vídeos curtos, controlado pela empresa chinesa ByteDance, supostamente representando ameaças à Segurança Nacional dos EUA. Ainda não está claro quais seriam essas ameaças, mas é importante observar que informações relevantes para a Segurança Nacional podem ser obtidas de fontes insuspeitadas. Em 2018, dados de um aplicativo inofensivo de rastreamento de condicionamento físico chamado Strava revelaram a localização de bases secretas do Exército dos EUA em todo o mundo. A empresa divulgou mapas que identificam "rotas de corrida populares nas principais cidades ou identificam indivíduos em áreas mais remotas que têm padrões de exercício incomuns". No entanto, "analistas militares notaram que o mapa também é detalhado o suficiente para fornecer informações extremamente sensíveis sobre um subconjunto de usuários do Strava: militares em serviço ativo" (HERN, 2020).

Seja qual for a razão, no caso TikTok, o governo dos EUA pretendia forçar a sua operação local a ser vendida a uma empresa norte-americana. O apoio jurídico é fornecido pelo Comitê de Investimento Estrangeiro nos Estados Unidos (CFIUS) sob a Lei de Produção de Defesa de 1950 (UNITED STATES, [2022b]). O CFIUS pode bloquear a aquisição de empresas americanas por investidores estrangeiros. Em 2018, o TikTok, então denominado Music.ly, também uma empresa chinesa, foi comprado pela ByteDance. Mas a Music.ly, apesar de ser chinesa, de acordo com os regulamentos do CFIUS, é considerada "negócio dos EUA", como uma entidade que se dedica ao comércio interestadual nos Estados Unidos. Assim, a CFIUS pode forçar a operação dos EUA a uma empresa de propriedade americana, uma vez que a ByteDance não solicitou a aprovação da CFIUS no momento da aquisição (CHESNEY, 2020).

7 Conclusão

Este artigo procurou demonstrar como o Ciberespaço, a Logística e a Segurança Nacional representam sérias ameaças entre si. Não necessariamente na ordem usual de causalidade perceptível, mas em qualquer ordem escolhida. Um conjunto prolífico de dezenas de casos, envolvendo principalmente potências cibernéticas, como Estados Unidos e China, bem como Reino Unido, Alemanha e governos e empresas privadas de outras nações, forneceu evidências empíricas robustas para sustentar esse argumento.

Em primeiro lugar, mostrou-se como a procura de uma logística melhor conduz a um aumento da automatização e, por conseguinte, a um maior apoio logístico informatizado. Essa crescente automação, juntamente com o uso de crescentes comunicações digitais, veículos autônomos, inteligência artificial e fabricação aditiva (impressão 3D), entre outras novas tecnologias, representa riscos crescentes de explorar vulnerabilidades cibernéticas e permitir a incapacitação logística de forças e sociedades militares. Apresentando, assim, muitas oportunidades para comprometer a Segurança Nacional. Desde 2018, houve um aumento no ritmo das medidas tomadas (ou iniciadas) pelos governos das potências cibernéticas com o objetivo de reduzir esse risco. No entanto, como argumentado por esta peça, esta era a percepção clássica e mais de senso comum.

Em segundo lugar, bem menos evidente que o primeiro, o artigo mostrou como a logística cada vez mais complexa traz riscos à confiabilidade e ao desempenho dos produtos de hardware e software. Como mostrado, da mesma forma que um componente eletromecânico ajustado infiltrado em qualquer lugar na extensa cadeia de suprimentos de um equipamento militar, software ou componentes de hardware alterados maliciosamente podem comprometer sua confiabilidade ou desempenho. Por conseguinte, afeta também a Segurança Nacional. Para isso, apresentou-se o conceito de cadeias de suprimentos cibernéticas, e como sua complexidade transcende as fronteiras nacionais, demandando muita pesquisa e investimentos para criar e manter controles que aumentem a segurança desses produtos, ao mesmo tempo que fluidos o suficiente para não tornar seu desenvolvimento muito rígido e demorado. Um elemento concreto que dificulta esse controle é que a cadeia produtiva de hardware e software é altamente complexa, com

muitos pontos de contato distribuídos em diferentes partes do mundo. Exemplificando, computadores fabricados no Brasil podem ter simultaneamente circuitos e chips projetados nos EUA, Alemanha e Japão, e produzidos na China, Taiwan, Cingapura, Vietnã e Índia, cujo firmware foi produzido em muitos outros países. Da mesma forma, os grandes e complexos sistemas de software modernos também são construídos em centros de desenvolvimento espalhados por vários países por técnicos de outros países.

Em terceiro lugar, também foi demonstrado como decisões baseadas em Segurança Nacional, como a restrição de exportação (ou importação) de componentes de TI para ou de países estrangeiros, podem comprometer cadeias de suprimentos de hardware e software (logística) e o ritmo de desenvolvimento do ciberespaço. Não só nas nações que são os seus principais alvos, mas também naquelas que implementam essas medidas. Como explicado, a substituição de componentes fornecidos por estrangeiros por componentes nacionais (ou de terceiros "neutros"), se não uma tarefa hercúlea como o controle da cadeia de suprimentos cibernética, também é um esforço caro e demorado.

No geral, o artigo mostra que a percepção evoluiu de uma ameaça estática, fechada dentro do perímetro da nação, governo ou produção de defesa, para um perigo dinâmico presente em toda a cadeia de suprimentos, notadamente fornecedores privados.

A má notícia é que proteger as três áreas é uma tarefa muito complexa. Além disso, sua viabilidade ainda requer muita pesquisa, principalmente no que diz respeito aos ativos de alta tecnologia da Base Industrial de Defesa, as empresas que fornecem aos governos produtos e serviços relacionados à Segurança Nacional.

A boa notícia é que grandes esforços já foram feitos sobre o tema em nível internacional, com abundante material disponível, o que nos permite economizar tempo e recursos para implementar diversas práticas adotadas pela indústria de classe mundial. Mais importante, há uma percepção crescente de que o assunto precisa ser tratado de acordo com sua relevância.

Por enquanto, a única certeza é que as cadeias de suprimentos globais relacionadas ao ciberespaço e à Segurança Nacional estarão sob muito mais escrutínio do que estão hoje. Além disso, pode-se esperar uma abordagem nacionalista consideravelmente maior, possivelmente (ou provavelmente) mudando profundamente o que tem sido considerado o núcleo da tendência recente de globalização.

Agradecimentos

O autor agradece aos pareceristas que contribuíram para a melhoria deste trabalho.

Referencias

ADAMS, James. Virtual defense. **Foreign Affairs**, [New York], v. 80, n. 3, p. 98, May/June 2001.

ALLEVEN, Monica. Deutsche Telekom selects Ericsson for 5G RAN in Germany. **FierceWireless**, [*s. l.*], July 22, 2020. Disponível em: https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany. Acesso em: Jul. 28, 2022.

AMADO, Guilherme *et al.* O recado das Forças Armadas ao Ministério da Defesa sobre o 5G. *Época*, 7 ago. 2020. Disponível em: https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588. Acesso em: Jul. 28, 2022.

ARON, Raymond. **Paz e guerra entre as nações**. São Paulo: Imprensa Oficial do Estado, 2002.

AUCHARD, Eric; FINKLE, Jim. Ukraine utility cyber attack wider than reported. **Reuters**, [Eagan], Jan. 3, 2016. Disponível em: http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104. Acesso em: Jul. 28, 2022.

BEAUFRE, André. **Introduction to strategy**. London: Faber and Faber Limited, 1965.

BIDEN JR, Joseph R. Executive Order on America's Supply Chains. *In*: THE WHITE HOUSE. Washington, DC: The White House, Feb. 24, 2022. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/. Acesso em: Ago. 1, 2022.

BLESSMAN, Danika. Protecting your software supply chain. **Risk Management**, [*s. l.*], n. 1, p. 10-11, 2019.

BLUMENTHAL, Eli. 'Unfixable' hole in Intel ROM exposes all but latest chips to attack, researchers say. **CNet**, [*s. l.*], Mar. 6, 2020. Disponível em: https://www.cnet.com/news/unfixable-hole-in-intel-rom-exposes-all-but-latest-chips-to-attack/. Acesso em: Ago. 3, 2022.

BRYAN, Joseph M. *et al.* **Inquiry into cyber intrusions affecting U.S. Transportation Command contractors**. Washington: U.S. Senate, 2014. Disponível em: https://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf. Acesso em: Ago. 3, 2022.

BURTON, Phillip; MCBIRNEY, Samantha. Military yet to fully leverage additive manufacturing. **National Defense**, Arlington, VA, Feb. 16, 2022. Disponível em: https://www.nationaldefensemagazine.org/articles/2022/2/16/military-yet-to-fully-leverage-additive-manufacturing. Acesso em: Ago. 3, 2022.

CHESNEY, Robert. TikTok and the law: a primer (in case you need to explain things to your teenager). **Lawfare**, [*s. l.*], Ago. 2, 2020. Disponível em: https://www.lawfareblog.com/tiktok-and-law-primer-case-you-need-explain-things-your-teenager. Acesso em: Ago. 3, 2022.

CIMPANU, Catalin. Cisco removed its seventh backdoor account this year, and that's a good thing. **ZDNet**, [*s. l.*], Nov. 7, 2018. Disponível em: https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing/. Acesso em: Ago. 3, 2022.

CISCO. **Cisco prime home authentication bypass vulnerability**. San Jose, CA: Cisco, Feb. 2017. Disponível em: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20170201-prime-home.html. Acesso em: Ago. 3, 2022.

CLARK, Don. U.S. Agencies block technology exports for supercomputer in China. **The Wall Street Journal**, New York, Apr. 9, 2015. Disponível em: https://www.wsj.com/articles/u-s-agencies-block-technology-exports-for-supercomputer-in-china-1428561987. Acesso em: Ago. 3, 2022.

CLAUSEWITZ, Carl Von. **On war**. Princeton: Princeton University Press, 1976.

CORERA, Gordon. US warns of supply chain cyber-attacks. **BBC**, London, Jul. 26, 2018. Disponível em: http://bbc.co.uk/news/technology-44941875. Acesso em: Ago. 3, 2022.

EPSHTEIN, Uriel; FAINT, Charles. That's logistics: the autonomous future of the Army's Battlefield. *In*: MODERN WAR INSTITUTE. West Point, NY: Modern War Institute, Jan. 2019. Disponível em: https://mwi.usma.edu/thats-logistics-autonomous-future-armys-battlefield-supply-chain/. Acesso em: Ago. 3, 2022.

ERICSSON. Press Releases. **Deutsche Telekom and Ericsson strengthen partnership with 5G deal**. Stockholm: Ericsson, 2020. Disponível em: https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal. Acesso em: Ago. 3, 2022.

FREEDMAN, Lawrence. **Strategic coercion**: concepts and cases. Oxford: Oxford University Press, 1998.

FREEDMAN, Lawrence. **Strategy**: a history. Oxford: Oxford University Press, 2015.

GERRING, John. Mere description. **British Journal of Political Science**, [London], v. 42, p. 721-746, 2012. Disponível em: https://cupdf.com/document/gerring-j-mere-description.html?page=1. Acesso em: Ago. 3, 2022.

GOODIN, Dan. Cisco confirms NSA-linked zeroday targeted its firewalls for years. **Ars Tchnica**, [California], Ago. 17, 2016. Disponível em: https://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/. Acesso em: Ago. 3, 2022.

GRAY, Colin. Why strategy is dificult? *In*: MAHNKEN, T. G.; MAIOLO, J. A. (org.). **Strategic studies**. Oxon: Routledge, 2008. p. 40-47.

GREENWALD, Glenn. **No place to hide**: Edward Snowden, the NSA and the surveillance state. [london]: Penguin Books, 2014.

HALFHILL, Tom R. The truth behind the Pentium Bug. **Byte**, California, Mar. 1995. Disponível em: https://web.archive.org/web/20060209005434/http://www.byte.com/art/9503/sec13/art1.htm. Acesso em: Ago. 3, 2022.

HERN, Alex. Oracle in talks with TikTok that could hijack Microsoft bid. **The Guardian**, London, Ago. 2020. Disponível em: https://www.theguardian.com/technology/2020/aug/18/software-firm-oracle-in-talks-to-buy-tiktok-and-challenge-microsoft-bid. Acesso em: Ago. 3, 2022.

HOWARD, Michael. The forgotten dimensions of strategy. **Foreign Affairs**, [New York], v. 57, n. 5, p. 975, 1979.

HUTCHINS, Eric M.; AMIN, Rohan M; CLOPPERT, Michael J. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains**. [*S. l.*: *s. n.*], 2010. Disponível em: https://community.mis.temple.edu/mis5208sp2016/files/2015/01/iciw2011.pdf. Acesso em: Ago. 3, 2022.

JAGODA, Jeneé *et al.* The viability and simplicity of 3D-Printed construction: a military case study. **Infrastructures**, [*s. l.*], v. 5, n. 4, p. 1-10, 2020.

JOMINI, Antoine. **The art of war**. 3. ed. Rockville: Arc Manor, 1862.

KHARPAL, Arjun. US should take stake in Nokia, Ericsson to counter Huawei in 5G: Barr. **CNBC**, [Englewood Cliffs, NJ], 2020.

KRESS, Moshe. **Operational logistics**: the art and science of sustaining military operations. New York: Springer Science+Business Media, 2002.

LEE, Micah; MOLTKE, Henrik. Everybody does it: the messy truth about infiltrating computer supply chains. **The Intercept**, [New York], Jan. 24, 2019. Disponível em: https://theintercept.com/2019/01/24/computer-supply-chain-attacks/. Acesso em: Ago. 3, 2022.

LEWIS, James. **Technological competition and China**. Washington, DC: Center for Strategic & International Studies, Nov. 2018. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181130_Technological_Competition_and_China.pdf. Acesso em: Ago. 3, 2022.

LIDDELL HART, Basil. Economic pressure or continental victories. **Royal United Services Institution Journal**, [London], v. 76, n. 503, p. 486-510, 1931.

LIDDELL HART, Basil. The essence of war. **Royal United Services Institution Journal**, [London], v. 75, n. 499, p. 490-491, 1930.

LIFF, Adam. Cyberwar: a new "Absolute Weapon"? The proliferation of cyberwarfare capabilities and interstate war. **Journal of Strategic Studies**, London, v. 35, n. 3, p. 401-428, 2012. Disponível em: https://indianstrategicknowledgeonline.com/web/Proliferation%20of%20Cyberwarfare%20Capabilities%20and%20Interstate%20War.pdf. Acesso em: Ago. 3, 2022.

LEIGHTON, Richard. Logistics: military. *In*: ENCYCLOPAEDIA BRITANNICA. [London]: Encyclopaedia Britannica, 2022. Disponível em: https://www.britannica.com/topic/logistics-military. Acesso em: Ago. 3, 2022.

LYNN III, William. Defending a New Domain: the Pentagon's cyberstrategy. **Foreign Affairs**, [New York], v. 89, n. 5, 2010. Disponível em: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. Acesso em: Ago. 3, 2022.

MICROSOFT. Azure. Resources. **What is Middleware?** [Washington, DC]: Microsoft, 2022. Disponível em: https://azure.microsoft.com/en-us/overview/what-is-middleware/. Acesso em: Ago. 3, 2022.

MILLER, Greg. How the CIA used Crypto AG encryption devices to spy on countries for decades. **The Washington Post**, Washington, DC, 2020.

MOON, Angela. Exclusive: Google suspends some business with Huawei after Trump blacklist - source. **Reuters**, [Eagan], May 19, 2019. Disponível em: https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUKKCN1SP0NB. Acesso em: Ago. 3, 2022.

MORGAN, Patrick. Applicability of traditional deterrence concepts and theory to the cyber realm. *In*: NATIONAL RESEARCH COUNCIL (U.S.). **Proceedings of a workshop on deterring cyberattacks**: informin strategies and developing options for U.S. policy. Washington, DC: National Academies Press, 2010. p. 55-76.

NIST. **Framework for improving critical infrastructure cybersecurity**. [*S. l.*: *s. n.*], 2014. Disponível em: papers2://publication/uuid/DD40979D-D391-4678-9601-F14CF1CB8BF5. Acesso em: Ago. 3, 2022.

NIST; FIREEYE. **Best Practices in Cyber Supply Chain Risk Management**. [California]: National Institute of Standards and Technology, 2015. Disponível em: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-best-practices-in-cyber-supply-chain-risk-management.pdf. Acesso em: Ago. 3, 2022.

NYE JR, Joseph. Deterrence and dissuasion in cyberspace. **International Security**, [*s. l.*], v. 41, n. 3, p. 44-71, 2017.

PECK, Helen. Supply chain vulnerability, risk and resilience. *In*: WATERS, D. (org.). **Global logistics**: new directions in supply chain management. 6th ed. [*S. l.*]: Kogan Page, 2012. p. 192-207.

PETZINGER, Jill. Deutsche Telekom describes potential Huawei ban as "Armageddon" scenario. **MSN**, June 17, 2020. Disponível em: https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM. Acesso em: Ago. 8, 2020.

PROENÇA JÚNIOR, Domício; DUARTE, E. E. The concept of logistics derived from clausewitz: all that is required so that the fighting force can be taken as a given. **Journal of Strategic Studies**, [London], v. 28, n. 4, p. 645-677, 2005. Disponível em: https://www.icesi.edu.co/blogs/estrategialogistica122/files/2012/08/the-concept-of-logistic-derived-from-clausewitz.pdf. Acesso em: Ago. 3, 2022.

ROGERS, Chairman Mike Rogers; RUPPERSBERGER, Dutch. **Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE**. Washington, DC: U.S. House of Representatives, Oct. 2012. Disponível em: https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. Acesso em: Ago. 3, 2022.

ROSA, Bruno; ANTUNES, Cláudia. Embaixador dos EUA alerta que se Brasil permitir chinesa Huawei no 5G enfrentará "consequências". **O Globo**, Rio de Janeiro, jul. 29, 2020. Disponível em: https://oglobo.globo.com/economia/embaixador-dos-eua-alerta-que-se-brasil-permitir-chinesa-huawei-no-5g-enfrentara-consequencias-24555785. Acesso em: Ago. 3, 2022.

SANGER, David; PERLROTH, Nicole. FBI Confirms DarkSide as Colonial Pipeline Hacker. **The New York Times**, New York, May 10, 2021. Disponível em: https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html. Acesso em: Ago. 3, 2022.

SCHWAAR, Carolyn. U.S. Military To 3D print its way out of supply chain woes. Forbes, Feb. 27, 2022. Disponível em: https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster https://www.forbes.com/sites/carolynschwaar/2022/02/27/us-military-to-3d-print-its-way-out-of-supply-chain-woes/?sh=316b8598275d. Acesso em: Ago. 4, 2022.

SHERMAN, Mark. **Growing risks in the software supply chain**: Platform Security Summit 2019. [*S. l.*]: Software Engineering Institute; Carnegie Mellon Univerty, Oct. 2019. Disponível em: https://www.platformsecuritysummit.com/2019/speaker/sherman/PSEC2019-Risks-Software-Supply-Chain-Mark-Sherman.pdf. Acesso em: Ago. 4, 2022.

SHIDONG, Zhang. China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech. **South China Morning Post**, Shanghai, May 22, 2019. Disponível em: https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster. Acesso em: Ago. 2, 2022.

STONE, John. Technology and war: a trinitarian analysis. **Defense & Security Analysis**, [London], v. 23, n. 1, p. 27-40, 2007.

STRUMPF, Dan. Huawei's 5G dominance threatened by U.S. Policy on Chips. **The Wall Street Journal**, New York, 2020. Disponível em: https://www.wsj.com/articles/huawei-struggles-to-escape-u-s-grasp-on-chips-11592740800. Acesso em: Ago. 2, 2022.

SUPPLY chains are undergoing a dramatic transformation. **The Economist**, New York, p. 1-7, July 11, 2019. Disponível em: https://www.economist.com/special-report/2019/07/11/supply-chains-are-undergoing-a-dramatic-transformation. Acesso em: Ago. 2, 2022.

TOP500.ORG. Lists. **Top500 June 2020**. Sinsheim: Top500.org, 2020. Disponível em: https://www.top500.org/lists/top500/2020/06/. Acesso em: Ago. 2, 2022.

TRUMP, Donald J. Executive Order on securing the information and communications technology and services supply chain (EO15873). *In*: THE WHITE HOUSE. Washington, DC: The white House, May 15, 2019. Disponível em: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/. Acesso em: Ago. 2, 2022.

TURNBULL, Benjamin. Cyber-resilient Supply chains: mission assurance in the future operating environment. **Australian Army Journal**, [Canberra], v. 14, n. 3, p. 41-56, 2018. Disponível em: https://search.informit.org/doi/pdf/10.3316/informit.344417545553155. Acesso em: Ago. 1, 2022.

TZU, Sun. **The Art of War (Restored Translation)**. [*S. l.*]: Pax Librorum, 2009.

UNITED STATES. Defense Logistics Agency. **Defense Logistics Agency strategic plan 2015-2022**. [Virginia]: Defense Logistics Agency, 2015. Disponível em: https://www.dla.mil/Portals/104/Documents/Headquarters/History/StrategicPlans/2015%20-%202022%20Strategic%20Plan.pdf. Acesso em: July 28, 2022.

UNITED STATES. Department of Commerce. **Announces the addition of Huawei Technologies Co. Ltd. to the entity list**. Washington, DC: U.S. Department of Commerce, 2019. Disponível em: https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd. Acesso em: Ago. 4, 2022.

UNITED STATES. Department of Defense. **Department of Defense Additive Manufacturing Strategy**. Washington, DC: Department of Defense, Jan. 2021a. Disponível em: https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf. Acesso em: Ago. 4, 2022.

UNITE STATES. Department of Defense and General Services Admnistration. **Improving cybersecurity and resilience through acquisition**: final report of the Department of Defense and General Services Admnistration. [Washington, DC: Department of Defense and General Services Admnistration], Nov. 2013a. Disponível em: https://www.gsa.gov/cdnstatic/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.pdf. Acesso em: Ago. 3, 2022.

UNITED STATES. Department of Defense. Defense Science Board. **Cyber supply chain**. Washington, DC: Defense Science Board, 2017.

UNITED STATES. Department of Defense. Defense Science Board. **Resilient Military systems and the advanced cyber threat**. Washington, DC: Defense Science Bord, 2013b. (Task force report). Disponível em: https://apps.dtic.mil/sti/pdfs/ADA569975.pdf. Acesso em: Ago. 4, 2022.

UNITED STATES. Department of Defense. **Department of Defense Strategy for Operating in cyberspace**. Washington, DC: Department of Defense, July 2011. Disponível em: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Acesso em: Ago. 4, 2022.

UNITED STATES. Department of Defense. **DoD Open Source Software (OSS) FAQ**. Washington, DC: Department of Defense, Out. 28, 2021b. Disponível em: https://dodcio.defense.gov/open-source-software-faq/. Acesso em: Ago. 4, 2022.

UNITED STATES. Department of Defense. Securing Defense-Critical Supply Chains: an action plan developed in response to President Biden's Executive Order 14017. Washington, USA: Department of Defense, Feb. 2022a. Disponível em: https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF. Acesso em: Ago. 4, 2022.

UNITED STATES. Department of Treasury Policy issues. International. **The Committee on Foreign Investment in the United States (CFIUS)**. Washington, DC: US Department of the Treasury, [2022b]. Disponível em: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius. Acesso em: Ago. 2, 2022.

UNITED STATES. **Foreign economic espionage in cyberspace**. [*S. l.*: *s. n.*], 2018.

VEGETIUS, Flavius Renatus. **De Re Militari**. [*S. l.*: *s. n.*], 1767.

WILLETT, Marcus. Lessons of the SolarWinds Hack. **Survival**, [London], v. 63, n. 2, p. 7-26, 2021.

WOOD, Donald F. Logistics: business. *In*: ENCYCLOPAEDIA BRITANNICA. [London]: Encyclopaedia Britannica, 1998. Disponível em: https://www.britannica.com/topic/logistics-business. Acesso em: Ago. 3, 2022.

WOODS, Beau; BOCHMAN, Andy. **Supply chain in the software era**. Washington, DC: Atlantic Council, May 2018. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/. Acesso em: Ago. 1, 2022.

YANG, Yuan; LIU, Nian. Beijing orders state offices to replace foreign PCs and software. **Financial Times**, [London], Dec. 8, 2019. Disponível em: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406. Acesso em: Ago. 1, 2022.

ZETTER, Kim. **Countdown to Zero Day**: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2015a.

ZETTER, Kim. Everything we know about Ukraine's Power Plant Hack. **Wired**, Boone, IA, Jan. 28, 2016. Disponível em: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/. Acesso em: Ago. 1, 2022.

ZETTER, Kim. Suite of sophisticated NationState attack tools found with connection to Stuxnet. **Wired**, boone, IA, Feb 16, 2015b. Disponível em: https://www.wired.com/2015/02/kapersky-discovers-equation-group/. Acesso em: Ago. 1, 2022.


ECEME