Writing the Private Sector Back into the Defense Equation – Unlearned Lessons

Dr. Andrea Little Limbago

Global supply chains received a one-two punch in 2020. The ongoing US-China trade war and COVID-19 made it clear that the increasingly complex, fragile, and opaque global supply chains were no longer sustainable. These significant shocks, coupled with the SolarWinds supply chain compromise and growing concerns over data security and digital supply chain risk, have caused many in the private sector to rethink their global footprint. These global transformations also create a rare opportunity to rethink the role of the private sector in national security.

For the most part, the private sector has been omitted from the defense equation despite being on the frontline of adversarial behavior and geopolitical conflict. In a recent testimony, Senator Angus King explained, "many smaller companies, particularly in Silicon Valley and in the technology field generally, have given up on the Pentagon."[1] When US tech giants withdraw from participation in Pentagon programs,[2] while others aid in the massive surveillance and human rights violations in China,[3] the divide between technologists and policymakers may seem too vast to mend. Nevertheless, closing this gap is a national security imperative. Just as the global order is undergoing transformations, so too must the role of the private sector in national defense.

The window of opportunity for bridging this gap is now. However, as Amy Zegart and Kevin Childs explain, fixing this divide requires thinking differently.[4] To be sure, for the last decade, the private sector largely dismissed any role in national security – and vice versa. Even following Russian interference in the 2016 US Presidential election, many tech leaders were slow to comprehend how their technology could be abused by adversaries.[5]

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Andrea Little Limbago is a computational social scientist specializing in the intersection of technology, national security, and information security.

As the Vice President of Research and Analysis at Interos, Andrea leads the company's research and methodology regarding global supply chain risk, with a focus on globalization, cybersecurity, and geopolitics. Andrea is a Co-Program Director for the Emerging Tech and Cybersecurity Program at the National Security Institute at George Mason, an industry advisory board member for the data science program at George Washington University, a non-resident fellow at the Atlantic Council's GeoTech Center, and a board member for the Washington, DC chapter of Women in Security and Privacy (WISP). Andrea previously taught in academia, was a technical lead at the Department of Defense, and Chief Social Scientist at Endgame and Virtru.

Andrea earned a Ph.D. in Political Science from the University of Colorado at Boulder and a BA from Bowdoin College.

Fortunately, times are changing and private sector leaders from across industries are reassessing their global footprint and how geopolitics impacts their bottom line. This article considers the forces driving the private sector's nascent transformation toward resilience in a post-pandemic global order and how the defense community must seize the moment to redefine public-private sector relations and optimize US national security.

Lessons Unlearned: Thinking Differently about the role of the Private Sector in National Security

These high-profile divides have dominated headlines for the last decade and obscured underlying shifts across the private sector when it comes to national security. The notion of private-public partnerships generally receives strong support, but the frameworks for these partnerships have barely evolved since the Cold War. Even when discussing the Silicon Valley/DC divide, it is largely framed with a focus on bridging a gap between technologists and policymakers through joint research and development, misaligned acquisition processes, and workforce solutions.

While addressing the divide between technologists and policymakers is essential, it is a well-known problem with emerging or nascent solutions. Governmental programs such as the Defense Innovation Unit and DefenseWerx were created to facilitate these partnerships and expedite innovation and technological transitions. Conversely, there are a growing number of programs to recruit more technologists into policy, such as the Aspen Tech Policy Hub,[6] TechCongress,[7] and the National Security Institute Technologist Fellowship.[8] Additional bug bounty programs such as Hack the Pentagon and Hack the Capitol further seek to bring these groups together to address an array of national security and technology challenges, while the Biden administration is experimenting with new approaches to hiring tech talent.[9] The emergence of these programs over the last decade is a welcome change and highlights some lessons learned. Although there is still plenty more work to do, there are a growing number of programs working on it.

In contrast, there has been much less attention devoted to the broader private sector and its role in national security. The private sector is increasingly described as the frontline in cybersecurity, but little has changed in policy or in partnerships despite their growing role as defenders. Of course, there are examples of the government and corporations working together – for example to bring down bot networks – but these are few and far between when looking at the scale and scope of the threat.[10]

For instance, the financial sector is a well-known target of state and non-state adversaries and is among the sixteen critical infrastructure sectors designated by the U.S. Department of Homeland Security.[11] A BBC report highlights a financial 'fraud epidemic' as a national security problem due to both its destabilizing impact on society as well as being a source of funds for terrorist and criminal networks, not to mention the growing number of state and non-state actors that target the financial industry.[12] The fifteen other critical infrastructure sectors similarly are on the front lines of cyber warfare, but rarely get the attention or the resources needed to defend against nation-state attacks.

In fact, given such policy stagnation in addressing the technological realities of the threat landscape, many US and European corporations are now trying to shape global cyber norms. Microsoft's call for a "Digital Geneva Convention" and the Tech Accord, Siemen's Charter of Trust,[13] and Intel's draft US privacy law[14] illustrate this growing movement by corporations to shape the digital rules of the road. Importantly, the growing number of companies signing these accords or seeking similar initiatives demonstrates the growing overlap between national security initiatives and corporate bottom lines.

Of course, the private sector is extremely heterogenous, with great diversity among those corporations that internalize how national security may impact them and those who prefer to maintain a blind eye to it. While there has been policy inertia on the government's side, there has equally been those in the private sector who continue to discount the impact of national security threats on their bottom line. In discussing China's long-time campaign to tamper with technology products, a former FBI official recommends, "Silicon Valley in particular needs to quit pretending that this isn't happening."[15]

To be sure, many on both sides remain wedded to Cold War analogies and private/public sector models from anachronistic eras. Nevertheless, there is also growing acknowledgement of the ongoing inflection point and transformation in the global order which is prompting many in the private sector to rethink their relationship with national security. The next section explores the driving forces behind these shifting attitudes in the private sector regarding geopolitics and national security. This growing momentum introduces an opportune moment to rethink the role of the private sector in national security.

Global Shocks to the Bottom Line

For the private sector, the bottom line will generally trump national security considerations. This will not change. What has changed is the growing convergence of the bottom line and national security, a convergence that introduces great opportunities for reinventing private sector contributions to the defense equation. This section details those core factors behind these shifting attitudes in the private sector.

COVID-19 and Global Supply Chains (globalization reformed)

Beyond the public health and economic devastation, Covid-19 has exposed significant vulnerabilities in a hyper-globalized system, largely the complexity, opacity, and insecurity of global supply chains. From the well-documented food and vaccine distribution and personal protective equipment disruptions to manufacturing and defense supply chains, modern supply chain fragility has now become a top C-suite and consumer concern alike.

Last year, the Bank of England predicted the pandemic would cause the worst economic contraction since 1706.[16] Global economic activity ground to a halt in March 2020, dropping 30-35% in a few weeks. Global GDP forecasts dropped from 2.4% in February to –4% in March, UNCTAD predicted a 30-40% contraction in foreign direct investment flows,[17] while unemployment numbers quickly surpassed the Great Recession and approached Great Depression levels. The April 2020 jobs report detailed a massive jump in US unemployment to 14.7%,[18] as over 20 million people suddenly lost their jobs. This one-month shift was double that during the entire 2007-2009 Great Recession.

While the economy currently is making greater progress than the dire predictions of Spring 2020, the shock will forever transform the global economy. Those who anticipated a return to 'normal' in the post-pandemic global order will be in for a rude awakening. H.T. Goranson and Beth Cardier best detail this risk, noting, "The fact that our smartest scientists and political leaders are envisioning a return to 'normal' reflects a collective failure of imagination."[19]

For the private sector, the global supply chain disruptions linked to geographic dependencies – mainly geographic concentration in China – was a wake-up call. Many companies did not realize the extent to which their extended supply chain was so fragile, with 98% of executives noting some level of supply chain disruption due to COVID-19.[20] In preparation for the future shocks, 24% of companies plan to relocate supply chains, only 10% said China was stable for long-term sourcing, and 50% plan to identify alternative or backups.[21]

In short, while past private sector priorities focused on market access to the world's largest consumer base, the pandemic exposed the underlying fragility of this approach and prompted many in the private sector to begin transforming their global supply chains toward greater resilience.

Industrial Policy is Back

As the Internet exploded, the notion that borders do not exist in cyberspace became a common refrain. The same was often said of globalization, as goods flowed across borders at unprecedented levels. In both cases, national borders were always there, but were either discounted or completely ignored in favor of the potential promise of new market share and growth. This risk calculus is changing, as ongoing trade policies and data sovereignty laws have brought borders front and center to the business world.

While COVID-19 accelerated the push toward greater geographic diversification of global supply chains, the US-China trade war had already prompted a nascent focus on reshoring and onshoring. The 2019 Kearney U.S. Reshoring Index recorded a record high, indicating a growing number of companies shifting their dependencies away from a few core Asian countries toward other regions.[22]

The notion of trade wars is actually too restrictive, as both China and the US are deploying a range of tools in their economic statecraft toolbelt. Industrial policy is back with the business community caught in the crossfire yet again. For instance, the U.S. Department of Commerce has added over 350 Chinese companies to their entity list, which prohibits the export, re-export, or in-country transfer of their products.[23] The Cybersecurity Maturity Model Certification (CMMC) is one of many U.S. Defense Department efforts to secure its supply chain and incorporates security standards into its acquisition process.[24] Through Section 889 of the National Defense Authorization Act (NDAA) of 2019, the Federal Acquisition Council (which includes the Department of Defense, NASA, and the GSA) has restricted federal contractors from using the products from five Chinese companies, and their affiliates and subsidiaries. Separately, from June 2020 to January 2021, the Pentagon issued four different lists – and a total of 43 Chinese companies – with links to the Chinese military pursuant to Section 1237 of the 1999 NDAA.[25] This statutory requirement specifies that the Pentagon must release the names of “Communist Chinese military companies” but there is no compliance requirement. However, a November 2020 Executive Order[26] restricted investments in 31 of the 43 companies listed, and the 2021 NDAA introduced Section 1260H, which supersedes section 1237.[27]

In response, China has sanctioned[28] three US defense companies to signal opposition to US arms sales to Taiwan and the growing trade partnerships between the US and Taiwan – a partnership focused on ties among like-minded democracies with “shared values that will inform how we reinvent the supply chains of the future.”[29] China also has announced new details regarding their ‘unreliable entity list’ — companies deemed to be a danger to China’s national sovereignty, security, or development.[30]

While the US and China continue the tit-for-tat retaliatory economic policies, democracies across the globe are starting to leverage industrial policy to secure their own supply chains. Australia,[31] Italy,[32] Sweden,[33] UK,[34] Germany,[35] and India[36] are among the growing list of countries restricting Huawei from their 5G cellular infrastructure. India has taken additional steps, banning over 100 Chinese apps following military conflict along the Chinese/ Indian border.[39] The EU recently introduced[40] details for a U.S.-EU tech alliance, while the UK has proposed[41] a 10-country 5G pact of democracies (D-10). Members of the UK parliament also introduced the creation of a trusted suppliers list that would ban China and Russia from the defense supply chains.[42] In fact, many former members of the Soviet bloc are especially wary of Chinese influence and are blocking Chinese projects from the Baltic to the Adriatic. A Lithuanian member of Parliament summarized these decisions succinctly in noting, “We are choosing the Western technosphere. We are not choosing the Chinese technosphere.”[43] These regulatory dynamics introduce yet another supply chain risk for global corporations that increasingly shapes their calculus when restructuring their global footprint.

Data at Risk

At the end of 2020, the SolarWinds supply chain attack revealed just how vulnerable the digital software supply chain is across Fortune 500 companies and the public sector alike.[44] Far from being unique, the SolarWinds attack is part of a broader trend where legitimate software and third-party suppliers provide the attack vector for compromise. These kinds of ‘next-gen’ attacks jumped by 430% year over year.[45] A recent survey found that 60% of data breaches were the result of supply chain or third-party exposure, while most do not monitor all their suppliers for cyber risk.[46]

The physical supply chain also introduces cyber risks that have largely been ignored for the last decade but are beginning to enter the risk calculus. The diffusion of digital authoritarianism – the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations – introduces new data risks for global supply chains.

Whether through data sovereignty laws, Internet blackouts, or ‘cybersecurity’ laws that mandate government access to data within their borders, any private sector footprint within these countries faces much greater risk of data exfiltration and service disruption. For instance, Cambodia is moving toward an autarkic Internet inspired by China’s Great Firewall,[47] while Vietnam[48] and Thailand[49] both passed cybersecurity laws that give the government greater control of data within their borders. Ecuador’s all-seeing eye surveillance system[50] is already powered by Chinese technologies, while Kazakhstan’s required digital certification[51] has proven to enable man-in-the-middle attacks numerous times.

At the same time, government-induced Internet shutdowns are similarly on the rise. Uganda, Belarus, Russia, and Myanmar are among the growing list of governments deploying this technique for information control within their borders. India has also adopted this technique and holds the record for a democracy with the longest Internet shutdown at over 100 days. There were 213 documented incidents of shutdowns across at least 33 countries in 2019 alone.[52] In 2020, governments cut off the Internet to 268 million people – 93 shutdowns across 21 countries – a 49% increase in total hours from 2019.[53] According to the Business Continuity

Institute's Supply Chain Resilience Report,[54] these kinds of Internet disruptions are the most top-of-mind disruption concern for almost two-thirds of organizations surveyed. Government-led Internet blackouts increased 6000% between 2011-2018,[55] and cost the global economy $8 billion in 2019 alone,[56] and likely increased in 2020.[57]

Taken together, national borders dramatically impact data risk. Increasingly for the private sector, where you stand depends on where your data resides. With the average global brand having tens – if not hundreds –of suppliers across the globe, and a large portion of their data distributed across the supply chain, data abroad is increasingly data at risk. But those risks are not uniform and have instigated a growing emphasis on building trusted networks within the public and private sectors.

New Priorities and Solutions for Post-Pandemic World Order

This confluence of shocks has forced a reckoning with geopolitics and the private sector. To be clear, this is not a uniform reprioritization, but those who restructure their operational resilience around these risks will gain the competitive advantage in the post-pandemic world order.

For instance, Intel's new CEO describes the company as "..., a national asset. This company needs to be healthy for the technology industry, for technology in America."[58] With chip manufacturing front and center in the technology supply chain disputes between the US and China, this framing may become more commonplace for other businesses in the tech and critical industries.

This renewed national corporate pride is not limited to the US. Porsche recently announced[59] it would not expand production with a Chinese factory, opting for a Made in Germany approach despite higher labor costs. This came at the expense of lower growth in China in 2020 compared to competitors, and it is still too early to tell whether market pressures or geopolitics will dominate decisions across the auto industry.

At the same time, there are growing shifts toward crafting trusted supply chain networks – both digital and physical – and especially for a democratic 'tech alliance.'[60] The US is weighing a democratic economic alliance[61] that would retaliate in response to Chinese coercive trading policies, such as those used recently against Australia.[62] In addition, trustworthy networks are foundational to these tech alliances and are a growing priority among democracies.[63] The 'quad allies' – Australia, India, Japan, and the US – are stepping up tech ties to strengthen their security and coordination in critical supply chain and technology areas.[64] Creating these alliances will take time and are in a very nascent, exploratory phase but are essential to supply chain diversification, agility, and security.

The movement toward trusted supply chains also has introduced the potential creation of "trust zones"[65] that would share research and technology, while excluding those entities deemed security risks. There also is growing emphasis on industrial policy to formalize these trusted networks, whether through new prohibitions and restrictions to address the semiconductor chip dependencies,[66] national strategies to identify choke points in emerging technology supply chains, as well as through trusted alliances.[67]

Coordinating these restrictions and prohibitions across countries would have several advantages, including a unified front against adversaries, incentivized and increased information sharing, as well as the consistency necessary for private sector compliance. Governments should also consider financial incentives to facilitate compliance given the enormous difficulty and costs of replacing many of the prohibited technologies or reshoring to trusted locations. According to one assessment, it will cost US small carriers $1.8 billion to 'rip and replace'[68] existing Huawei and ZTE equipment from their networks. A German estimate predicts an even larger cost, closer to $3.5 billion for their largest telecom provider.[69] Non-compliance fines also can be extremely costly. OFAC issued over a billion dollars in violation fines in 2019.[70] In July 2021, the FCC approved a $1.9 billion program to expand its reimbursement plan[71] to assist in the compliance costs of removing prohibited technologies from US telecommunications networks. Japan has designated over $2 billion to their domestic champions to facilitate decoupling from the Chinese market.

Additional incentives and protections for information sharing will be essential across these trusted networks. While the SolarWinds attack has expedited[72] information sharing, it was in fact reactionary. A recent report from BSA, The Software Alliance, to the Biden Administration highlights the essential role of information sharing both domestically and with foreign partners, but laments that the government still lacks an effective means for two-way information sharing six years after the Cybersecurity Information Sharing Act was passed.[73] A core component of information is ensuring the data is protected, and given the growth in supply chain attacks, there is reason for concern. Therefore, data protection and more coherent data protection strategies across the democracies must similarly be foundational in securing the 'trust' in information networks.

Finally, the government should craft assurance policies to incentivize companies that pursue best practices for protecting their intellectual property and technology across their supply chains, including qualified bidders and qualified manufacturers lists. This, in turn, should spark a reckoning within US companies as well, especially among tech giants who currently power[74] many of the surveillance capabilities[75] on the US restricted lists, including those with military end-users. To be clear, this does not require a complete decoupling – that is neither practical nor advantageous – but rather incentivizing specific behavior for improved security across supply chains. When that does involve decoupling, government assistance could go a long way. A U.S. Chamber of Commerce report[76] estimates full decoupling would cost hundreds of billions of dollars, lost jobs, lost economies of scale, lost innovation, in addition to completely crippling certain industries. Finding this delicate balance between national security and economic security and welfare requires assurance-based support informed by both the private and public sectors, with each internalizing the practicalities and realities of a post-pandemic world order.

CONCLUSION

When the pandemic hit, numerous private sector companies shifted or expanded production capabilities, for example from athletic gear to masks and gowns,[77] 3-D greeting cards to face shields,[78] and pickup trucks to ventilators.[79] This begs the question: what role would the private sector play during other shocks, such as a large-scale military conflict?

There are many areas of disagreement between Silicon Valley and policymakers, but there is also growing alignment between the private sector writ large and national security concerns. The private sector continues to bear the brunt and costs of global supply chain disruption. From cyber-attacks to shifting data surveillance laws to geo-economics to geographic concentration risks, the private sector is caught in the crosshairs of these global shifts and is reassessing its global footprint for greater operational resiliency.

Geopolitics increasingly play a role regarding where and with whom the private sector purchases technology and which companies are integrated into their supply chain. The push-pull factors of geopolitical and industrial policy shifts are directly impacting their risk calculus and bottom line. The ongoing supply chains disruptions introduced by the COVID-19 pandemic have further prompted renewed thinking within the private sector about geographic and product concentration risks.

The confluence of these revelations provides an opening for democracies to reinvent the role of the private sector in the defense equation. As many global brands are reassessing their global footprint and the range of risks involved, many of these shifts increasingly align with national security objectives. From seeking locations with greater data protection to building operational resilience with trusted partners, there is increased opportunity for collaboration across the private and public sectors. However, this will only be possible by pushing aside the lessons unlearned of the last decade. National security and the corporate bottom line can go hand-in-hand, but it will require renewed focus and forward leaning solutions on par with the geopolitical, geoeconomic, and technological challenges of the post-pandemic world order.

NOTES

1. "Department of Defense Nominee Touts Senator King's Leadership on Cyberspace Solarium Commission." February 2, 2021, https://www.king.senate.gov/newsroom/press-releases/defense-department-nominee-touts-senator-kings-leadership-on-cyberspace-solarium-commission.
2. Billy Mitchell, "Google's Departure from Project Maven was a 'little bit of a canary in a coal mine'," FEDSCOOP, November 5, 2019, https://www.fedscoop.com/google-project-maven-canary-coal-mine/.
3. Liza Lin and Josh Chin, "U.S. Tech Companies Prop Up China's Vast Surveillance Network," *The Wall Street Journal,* November 26, 2019, https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846.
4. Amy Zegart and Kevin Childs, "The Divide Between Silicon Valley and Washington is a National Security Threat," *The Atlantic*. December 13, 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.
5. Casey Newton, Zuckerberg: the idea that fake news on Facebook influenced the election is 'crazy,' *The Verge*, November 10, 2016, https://www.theverge.com/2016/11/10/13594558/mark-zuckerberg-election-fake-news-trump.
6. Aspen Tech Policy Hub, https://www.aspentechpolicyhub.org/.
7. TechCongress, https://www.techcongress.io/.
8. George Mason University National Security Institute, https://nationalsecurity.gmu.edu/technologist-fellowship/.
9. Katie Malone, Hide and Seek: Biden administration gets creative recruiting tech talent. *CIODive*, January 20, 2021, https://www.ciodive.com/news/biden-source-code-usds-white-house/593686/.
10. Microsoft Defender Security Research Team, "Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andormeda), Microsoft Blog, December 4, 2017, https://www.microsoft.com/security/blog/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/.
11. Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors.
12. https://www.bbc.com/news/business-55769991.
13. Charter of Trust, https://www.charteroftrust.com/.
14. "Intel publishes third draft of federal US privacy law recommendations," *IAPP Daily Dashboard*, May 29, 2019, https://iapp.org/news/a/intel-publishes-third-draft-of-federal-u-s-privacy-law-recommendations/.
15. Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," *Bloomberg*, February 12, 2021, https://www.bloomberg.com/features/2021-supermicro/.
16. D'Souza, Deborah. "Bank of England Predicts Worst Contraction since 1706." *Investopedia*. https://www.investopedia.com/bank-of-england-predicts-worst-contraction-since-1706-4844284
17. "Coronavirus could cut global investment by 40%, new estimates show," *UNCTAD,* March 26, 2020, https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2313.
18. Heather Long and Andrew Van Dam, "U.S. unemployment rate soars to 14.7%, the worst since the Depression era," *The Washington Post,* May 8, 2020, https://www.washingtonpost.com/business/2020/05/08/april-2020-jobs-report/.
19. H.T. Goranson and Beth Cardier, "Recovery is Not Enough," *Project Syndicate,* December 11, 2020, https://www.project-syndicate.org/commentary/building-intrinsic-reslience-against-future-shocks-by-h--t--goranson-and-beth-cardier-2020-12.
20. "COVID Resilience Report: The Impact of COVID-19 on Supply Chains and How Businesses are Preparing for the Next Shock," *Interos,* October 1, 2020, https://www.interos.ai/project/interos-2020-survey/.
21. A.B. Brown, "BDO: 24% of companies plan to relocate supply chains" *CFODive*, https://www.cfodive.com/news/cfo-outlook-survey-reshore-supplier-technology/593438/.
22. "Global Pandemic roils 2020 Reshoring Index, shifting focus from reshoring to right-shoring" *Kearney*, https://www.kearney.com/operations-performance-transformation/us-reshoring-index.
23. Bureau of Industry and Security, U.S. Department of Commerce, Entity List, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.
24. Cybersecurity Maturity Model Certification, https://www.acq.osd.mil/cmmc/.
25. "DOD Releases List of Additional Companies, In Accordance with Section 1237 of FY99 NDAA," https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

NOTES

26. "Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China," June 3, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.
27. "DOD Releases List of Chinese Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," June 3, 2021, https://www.defense.gov/News/Releases/Release/Article/2645126/dod-releases-list-of-chinese-military-companies-in-accordance-with-section-1260/.
28. Joe McDonald, "China to Sanction Boeing, Lockheed and Raytheon over Taiwan Arms Sales," *DefenseNews,* October 26, 2020, https://www.defensenews.com/global/asia-pacific/2020/10/26/china-to-sanction-boeing-lockheed-and-raytheon-over-taiwan-arms-sales/.
29. Reuters Staff, "US, Taiwan seek 'like-minded' democracies in supply chain shift from China," *Reuters,* September 4, 2020, https://www.reuters.com/article/us-taiwan-usa-trade-idUSKBN25V1DC.
30. Evelyn Cheng, "China releases details on its own blacklist, raising uncertainty for foreign businesses, *CNBC,* September 21, 2020, https://www.cnbc.com/2020/09/21/china-releases-details-on-unreliable-entity-list-raising-uncertainty-for-foreign-businesses.html.
31. "Huawei and ZTE handed 5G network ban in Australia" *BBC,* August 23, 2018, https://www.bbc.com/news/technology-45281495.
32. Giuseppe Fonte and Elvira Pollina, "Italy vetoes 5G deal between Fastweb and China's Huawei: sources." *Reuters,* October 23, 2020, https://www.reuters.com/article/us-huawei-italy-5g-idUSKBN2782A5.
33. Supantha Mukherjee and Helena Soderpalm, "Sweden bans Huawei, ZTE from upcoming 5G networks," *Reuters*, October 20, 2020, https://www.reuters.com/article/sweden-huawei-int/sweden-bans-huawei-zte-from-upcoming-5g-networks-idUSKBN2750WA.
34. Leo Kelion, "Huawei 5G kit must be removed from UK by 2027," *BBC News*, July 14, 2020, https://www.bbc.com/news/technology-53403793.
35. Uwe Parpart and David Goldman, "Germany battles over Huawei's 5G role," *Asia Times*, October 7, 2020, https://asiatimes.com/2020/10/germany-battles-over-huaweis-5g-role/.
36. Amy Kazmin and Stephanie Findlay, "India moves to cut Huawei gear from telecoms network," *Financial Review*, August 25, 2020, https://www.afr.com/world/asia/india-moves-to-cut-huawei-gear-from-telecoms-network-20200825-p55p6g#.
37. Sameer Yasir and Hari Kumar, "India bans 118 apps as Indian soldier is killed on disputed border," *The New York Times*, September 2, 2020, https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html.
38. "EU-US: A new transatlantic agenda for global change," https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279.
39. Srijan Shukla, "UK wants 5G alliance of 10 countries, including India, to avoid reliance on Chinese Huawei," *ThePrint*, May 29, 2020, https://theprint.in/world/uk-wants-5g-alliance-of-10-countries-including-india-to-avoid-reliance-on-chinese-huawei/431735/.
40. Alan Tovey, "MPs want China, Russia barred from defence chain," *The Telegraph*, February 1, 2021, https://www.telegraph.co.uk/business/2021/02/14/mps-want-china-russia-barred-defence-chain/.
41. Daniel Michaels and Valentina Pop, "China Faces European Obstacles as Some Countries Heed U.S. Pressure," *The Wall Street Journal*, February 23, 2021, https://www.wsj.com/articles/china-faces-european-obstacles-as-some-countries-heed-u-s-pressure-11614088843?mod=djem10point.
42. "Joint Statement by the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), January 5, 2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.
43. Ericka Chickowski, "Next-Gen Supply Chain Attacks Surge 430%," *DarkReading*, August 21, 2020, https://www.darkreading.com/application-security/next-gen-supply-chain-attacks-surge-430-/d/d-id/1338717.

NOTES

44. Matt Solomon, “Lessons Learned from the Global Year in Breach: Supply Chain Cybersecurity Risk is Swamping Businesses,” *Security Boulevard,* April 24, 2021, https://securityboulevard.com/2021/04/lessons-learned-from-the-global-year-in-breach-supply-chain-cybersecurity-risk-is-swamping-businesses/.
45. Prak Chan Thul, “Cambodia adopts China-style internet gateway amid opposition crackdown,” *Reuters*, February 17, 2021, https://www.reuters.com/article/amp/idUSKBN2AH1CZ.
46. Ashley Westerman, “To the dismay of free speech advocates, Vietnam rolls out controversial cyber law,” *NPR*. January 1, 2019, https://www.npr.org/2019/01/01/681373274/to-the-dismay-of-free-speech-advocates-vietnam-rolls-out-controversial-cyber-law.
47. Patpicha Tanakasempipat, “Thailand passes internet security law decried as ‘cyber martial law’,” *Reuters.* February 28, 2019, https://www.reuters.com/article/us-thailand-cyber/thailand-passes-internet-security-law-decried-as-cyber-martial-law-idUSKCN1QH1OB.
48. Charles Rollet, “Ecuador’s All-Seeing Eye is Made in China,” *Foreign Policy*, August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.
49. Catalin Cimpanu, “Kazakhstan government is intercepting HTTPS traffic in its capital,” ZDNet.” December 6, 2020, https://www.zdnet.com/article/kazakhstan-government-is-intercepting-https-traffic-in-its-capital/.
50. “Targeted, Cut Off, and Left in the Dark,” AccessNow, 2019 Report, https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.
51. Isobel Asher Hamilton, “268 million people had their internet shut off by government-imposed blackouts in 2020, up 49% from 2019,” Business Insider, https://www.businessinsider.com/government-internet-blackouts-human-rights-india-kashmir-coronavirus-2021-1.
52. Editorial Staff, “BCI Supply Chain Resilience Report 2019,” *Continuity Insights*, November 7, 2019, https://continuityinsights.com/bci-supply-chain-resilience-report-2019/.
53. Adam Jacobson, “The Economic Costs of Government Internet Interruptions,” *Risk Management Monitor*, May 7, 2019, https://www.riskmanagementmonitor.com/the-economic-costs-of-internet-interruptions/.
54. Chloe Taylor, “Government-led internet shutdowns cost the global economy $8 billion in 2019, research says,” CNBC, January 8, 2020, https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html.
55. Isobel Asher Hamilton, Government-imposed internet blackouts cost the global economy $8 billion in 2019, and 2020 could be even worse,” *Business Insider*, January 18, 2020, https://www.businessinsider.com/internet-shutdowns-cost-the-global-economy-8-billion-in-2019-2020-1.
56. Ian King, “Intel CEO’s New Crusade Pits Investors Against U.S. Interests,” *Bloomberg*, January 22, 2021, https://www.bloomberg.com/news/articles/2021-01-22/intel-ceo-s-new-crusade-pits-investors-against-u-s-interests.
57. Joe Miller, “Porsche rules out Chinese factory as it hails cachet of ‘Made in Germany’,” Financial Times, February 14, 2021, https://www.ft.com/content/d71660bf-ae2b-41b3-af99-1485b805c812.
58. “Democracies must team up to take on China in technosphere,” *The Economist,* November 21, 2020, https://www.econom ist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere.
59. Bob Davis, “White House Weighs New Action Against Beijing,” *The Wall Street Journal,* November 23, 2020, https://www.wsj.com/articles/white-house-weighs-new-action-against-beijing-11606138925.
60. “Australia demands China explain why it has been singled out on trade restrictions” *The Guardian*, November 22, 2020, https://www.theguardian.com/australia-news/2020/nov/22/australia-demands-china-explain-why-it-has-been-singled-out-on-trade-restrictions.
61. Rajiv Shah, “Ensuring a trusted 5G ecosystem of vendors and technology,” *Australian Strategic Policy Institute*, September 17, 2020, https://www.aspi.org.au/report/ensuring-trusted-5g-ecosystem-vendors-and-technology,
62. “Australia spends $500,000 to strengthen tech ties with Quad allies amid China tension,” *The Guardian*, November 23, 2020, https://www.theguardian.com/australia-news/2020/nov/23/australia-spends-500000-to-strengthen-tech-ties-with-quad-allies-amid-china-tension.
63. David Ignatius, “Biden’s ambitious plan to push back against techno-autocracies,” *The Washington Post*, February 11, 2021, https://www.washingtonpost.com/opinions/bidens-ambitious-plan-to-push-back-against-techno-autocracies/2021/02/11/2f2a358e-6cb6-11eb-9ead-673168d5b874_story.html.

NOTES

64. Joint Statement from Quad Leaders," September 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders/.
65. David Stilwell and Dan Negrea, "Wanted: Alliance Networks for a New Cold War." National Interest, March 28, 2021, https://nationalinterest.org/feature/wanted-alliance-networks-new-cold-war-181177.
66. Chaim Gartenberg, "The Biden administration is working to help address global semiconductor chip shortage," *The Verge*, February 11, 2021, https://www.theverge.com/2021/2/11/22278431/biden-administration-global-semiconductor-chip-shortage-executive-order..
67. "Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities," June 8, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/.
68. Russell Brandon, "It will cost $1.8 billion to pull Huawei and ZTE out of US networks, FCC says," The Verge, September 4, 2020, https://www.theverge.com/2020/9/4/21422939/huawei-zte-us-phone-networks-fcc-congress-reimbursement-cost.
69. Uwe Parpart and David Goldman, "Germany battles over Huawei's 5G role," *Asia Times*, October 7, 2020, https://asiatimes.com/2020/10/germany-battles-over-huaweis-5g-role/.
70. U.S. Department of Treasury, 2019, Enforcement Information, https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information. .
71. Statement of Commissioner Geoffrey Starks," February 17, 2021, https://docs.fcc.gov/public/attachments/DOC-370055A4.pdf.
72. Samantha Schwartz, "Technology's greatest supply chain challenge? Establishing trust, *Cybersecurity Dive*, January 21, 2021, https://www.cybersecuritydive.com/news/solarwinds-response-nation-state-threat/593239/. .
73. "US: Building a More Effective Strategy for ICt Supply Chain Security," *BSA Position Paper*, February 16, 2021, https://www.bsa.org/policy-filings/us-building-a-more-effective-strategy-for-ict-supply-chain-security.
74. Samuel Woodhams and Simon Migliano, "Big Tech Supporting Blacklisted Surveillance Companies," *TOP10VPN*, May 21, 2020, https://www.top10vpn.com/research/investigations/big-tech-supporting-blacklisted-surveillance-companies/.
75. Mara Hvistendahl, "How Oracle Sells Repression in China," The Intercept, February 18, 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.
76. "U.S. Chamber Releases In-Depth Analysis of U.S.-China Economic Relationship," February 17, 2021, https://www.uschamber.com/press-release/us-chamber-releases-depth-analysis-of-us-china-economic-relationship.
77. Jon Chesto, "Manufacturers provide lifelines during the pandemic, for their employees as well as front-line workers," *Boston Globe*, June 9, 2020, https://www.bostonglobe.com/2020/06/08/business/manufacturers-provide-lifelines-during-pandemic-their-employees-well-front-line-workers/.
78. Wombi Rose, "Two weeks of sleepless nights turn 3D card maker into PPE provider," *Lovepop*, May 13, 2020, https://www.lovepopcards.com/blogs/pop-up-cards/two-weeks-of-sleepless-nights-to-turn-3d-card-maker-into-ppe-provider. .
79. Sean O'Kane, "How GM and Ford Switched Out Pickup Trucks for Breathing Machines," *The Verge*, April 15, 2020, https://www.theverge.com/2020/4/15/21222219/general-motors-ventec-ventilators-ford-tesla-coronavirus-covid-19.