Study on supply chain highlights potential risks to election security

Introduction

The supply chain is the collection of critical connections that bind businesses and organizations together to deliver value to customers. With the globalization and interconnectedness of technology these relationships have grown more complex, increasing the dependency on 3rd, 4th, 5th and even 6th party suppliers to deliver quality end products. The ease with which organizations can form productive supplier relationships is unprecedented, but so is the potential risk those partnerships bring. This is particularly true with sub-tier suppliers, the often-hidden entities on which you and your direct suppliers rely.

In 2015, Apple and several other technology giants discovered a supplier had been providing motherboards with installed surveillance microchips[1]. Earlier this year, Amazon had to investigate if a vendor manufacturing the Alexa used child labor[2]. And, the CEO of Mars was recently quoted, stating that the global supply chain is "broken" and pledging $1 billion to develop supply chain sustainability efforts[3].

Supply chain risks affect every organization, from small, local businesses to the largest government agencies. And, even the best-intentioned aren't sure how to fully tackle the challenge. A recent Deloitte survey found that 70% of organizations report a moderate to high level of dependence on third parties[4], while a Microsoft survey found that only 15% of companies have any confidence in their supply chain risk mitigation[5].

Improving the level of supply chain risk mitigation to match the level of third-party dependence is a challenge everyone is trying to solve, whether it's the safety and reliability of military and commercial aircraft, the health and resiliency of our food supply or some of our most sensitive infrastructure: U.S. election technology.

Of course, the challenges related to voting security aren't strictly a supply chain story, but there are similarities in the following analysis that apply to nearly every product and service critical to the success of any business or government organization.

Election Security in Brief

The looming 2020 U.S. Presidential election has drawn more focus to election security than supply chains ever could. The interconnected nature of the global economy means that almost every country has a vested interest in the outcome of U.S. elections. China and Russia have been accused of launching numerous cyber incursions across the globe to impact election outcomes[6]. The purported scope of China and Russia's election tampering is vast. Both nations have allegedly launched numerous cyber-attacks across the globe, performing actions such as tampering with voter registration records, shutting down polling systems, and spear-phishing election officials[7]. Many are asking what is being done to ensure the security of the democratic process in the U.S.

Russia infamously launched a barrage of cyberattacks against several election systems during the 2016 presidential election[6]. Their attempts to sway elections in democratic nations date even further back to 2007 in Estonia where Russia leveraged very similar tactics to spread disinformation, foment public conflict, and divide a democracy[8]. During the 2014 Ukrainian presidential election, Pro-Russian hackers also undertook a series of cyber-attacks designed to tamper with and delay the election[9].

China has also made similar, if marginally less brazen efforts to interfere with democratic nations deemed threatening to the Chinese state. China has long been executing sophisticated cyber-attacks to disrupt and threaten democracies in nations like Indonesia, Taiwan and Hong Kong which, according to experts, have served as possible training grounds for influencing the 2020 US presidential election. In 2018, a pro-Beijing Taiwanese candidate by the name of Han Juo-yu an upset victory in the city of Kaohsiung, positioning himself to run for the state's president. His rise from virtual unknown to major political force was, in large part, due to backing from Beijing which included support from Chinese hackers who manipulated social media surrounding the election[10].

China also has a documented record of compromising the manufacturing of electronics, enabling backdoors and modifying hardware to conduct surveillance. For example, in 2015, Elemental, a U.S. Government contractor, was discovered to have had unauthorized microchips embedded in their products by a supplier from China. The microchips allowed hackers to create an undetectable doorway into any network the machine was installed on. Elemental's products were used by agencies ranging from the DoD to the CIA[1]. This is simply one instance of a broader campaign to compromise the American government through supply chain attacks. In 2009 the intelligence community stated, in a leaked report, that "an increasing number of actors are seeking the capability to target … supply chains and other components of the U.S. information infrastructure. Intelligence reporting provides only limited information on efforts to compromise supply chains, in large part because we do not have the access or technology in place necessary for reliable detection of such operations."[11]

According to Dan Coats, the former Director of National Intelligence "China and Russia are more aligned than at any point since the mid-1950s, and the relationship is likely to strengthen in the coming year as some of their interests and threat perceptions converge, particularly regarding perceived U.S. unilateralism and interventionism and Western promotion of democratic values and human rights."[6]

While states have spent hundreds of millions of dollars to shore up election security, leading cyber experts have warned that these changes have done little to fix the major vulnerabilities exploited during the last election [12].

On September 23rd, Congress voted to allocate $250 million to support state governments' election security measures, enabling states to further secure election technology[13]. However, that funding may not be enough, according to entities like the Brennan Center[14], who estimated the true cost of securing elections for the next 5 years to be over $2.153 billion.

The following analysis provides an overview of the role played by third parties in the U.S. voting infrastructure manufacturing process. We examine the connections between an election hardware manufacturer and countries with historical interest in interfering in foreign and U.S. elections. This paper is not meant to, nor does it, imply that any U.S. election technology company is inherently good or bad at supply chain risk mitigation based solely on the countries to which they are connected. What it does show is that Artificial Intelligence technology exists to support companies in the constant battle of matching the level of supply chain threat mitigation with the level of third-party dependence.

The Voting Industry

The voting technology industry has 3 vendors providing the election infrastructure used by 92% of the voting public[15]. This level of concentration poses challenges to regulators and the inherent security of voting systems. A 2018 report by the Senate Intelligence Committee specifically stated that "the number of vendors selling machines is shrinking, raising concerns about supply chain vulnerability."[16]

Increased Openness

Recently, voting machine companies have raised the possibility of working with ethical hackers, requesting feedback from both researchers and private companies about the best methods for letting outsiders vet their security. Chris Wlaschin, a top cybersecurity official for ES&S (one of the top 3 companies in the voting industry) stated that: "For many years the industry…preferred to work quietly behind scenes. [But] 2016 brought cybersecurity to the front burner and folks in this industry who were uncomfortable talking about vulnerabilities have warmed up to it."[17]

These steps towards increased cybersecurity may not fully address supply chain security. A recently published report by the Brennan Center specifically cites the fact that state and federal officials have limited visibility into "foreign ownership of [election]vendors (whether foreign nationals, or agents of foreign governments, own companies performing critical election functions)" as well as "supply chains (where parts, software patches, and installations come from; how are they transported; and how they are kept secure)."[18]

Terminology

Supplier Tiers: A tier 1 supplier would be the company the election machine vendor directly buys components from. Tier 2 suppliers are the companies the tier 1 suppliers buy from to make the products ultimately used in the studied machine. Tier 3 companies are the businesses who the Tier 2 suppliers buy from.

Component Tiers: A tier 1 component is a component from a tier 1 supplier, tier 2 components are from tier 2 suppliers and are purchased by tier 1 suppliers to make tier 1 components, and so on. The components described in this study are **all part** of the studied machine.

China-based company: For the purposes of this report a "China-based company" is either a company headquartered in China, or a Chinese subsidiary or location of an international business.

Study & Findings

We mapped the supply chain for one of the products of a major voting machine manufacturer: a touchscreen-based electronic voting station, hereafter referred to as "Machine A". Machine A is widely used across the United States and functions as a primary point of interface for voters. This mapping was done using publicly available data and AI to map Machine A's supply chain, discovering connections between suppliers and products. To conduct our research, Interos broke Machine A down into a list of component parts, identifying, in total, 140 digital and physical components that make up Machine A. We began by discovering the 38 components that the manufacturer directly buys from suppliers (their tier 1 suppliers), then identified the 50 known parts that make up those components and identifying the suppliers behind those parts (the tier 2 suppliers). We then went another step further, identifying the 70 sub-components within those components and the associated businesses (the tier 3 suppliers). We then identified if those companies had any additional locations in China or Russia.

While having a location in China or Russia is not unusual for large, international businesses especially in technology, Chinese rules require foreign companies in specific industries to partner with local companies and experts maintain that any company operating in China could not refuse a request to hand over information to the state intelligence apparatus[19]. Similarly, the Russian government has previously forced large western tech companies to turn over access to source code for things like security and encryption software[20]. Given Russia and China's aggressive espionage efforts on and offline, companies relying on suppliers with locations in the two countries could be cause for concern.

Having a location or being headquartered in the two countries also presents a security challenge by potentially offering human and/or network access. According to a 2018 study by the Ponemon Institute, 59% of organizations have had a breach that was caused by one of their vendors[21]. Having an office or manufacturing in countries with oppositional interests to the US inherently opens the door to risk.

Disclaimer: Interos' research identifies the components that make up Machine A, where the companies that supply those components are based, and the other locations of those companies. We did not study the exact origin of individual parts or manufacturing location. Interos recognizes the extreme sensitivity of election security matters and has contacted the company involved.

For the purposes of this study, Interos exclusively used publicly and commercially available data. Primary data sources include import/export records, company websites, SEC filings, news articles, and the Interos proprietary knowledge graph. Our data does not account for every component in the studied machine or every business or supplier relationship.

Our mapping revealed that several components and technology used in Machine A come from companies with locations in Russia and China. A few of those suppliers were also headquartered in China. Our study has identified that:

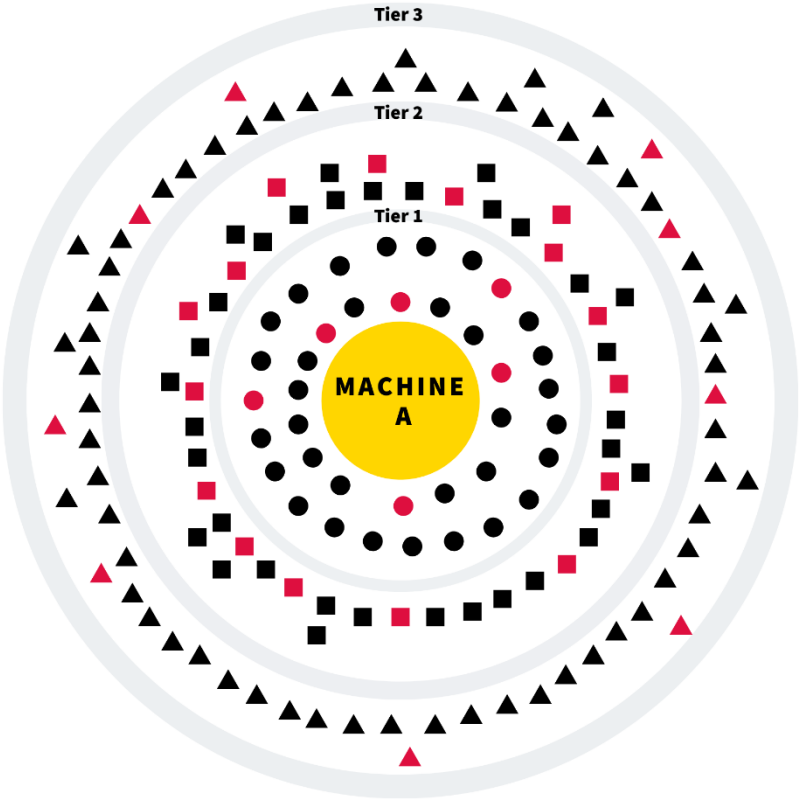
- **19.6% of components mapped for Machine A came from China-based companies**
- **58.6% of suppliers within Machine A's supply chain have locations in either Russia or China**.

Data Visualizations

Interos mapped the supply chain for Machine A down to the third tier, discovering not just who supplies the components directly to the manufacturer, but the suppliers behind those organizations. The visualizations below illustrate the results of our findings.

Visualization A (below) shows the percentage of components within the different tiers that are coming from companies **based in China**. Each shape represents a **component,** with red shapes representing components from China-based companies. **6 of 38 Tier 1** components are from companies based in China. **16 of 50 Tier 2** components are from companies based in China. Lastly, **9 of 70** Tier 3 components are from companies based in China. In total, **19.6% (38) of the components in the first 3 tiers of Machine A's supply chain come from China-based companies**.

Visualization A



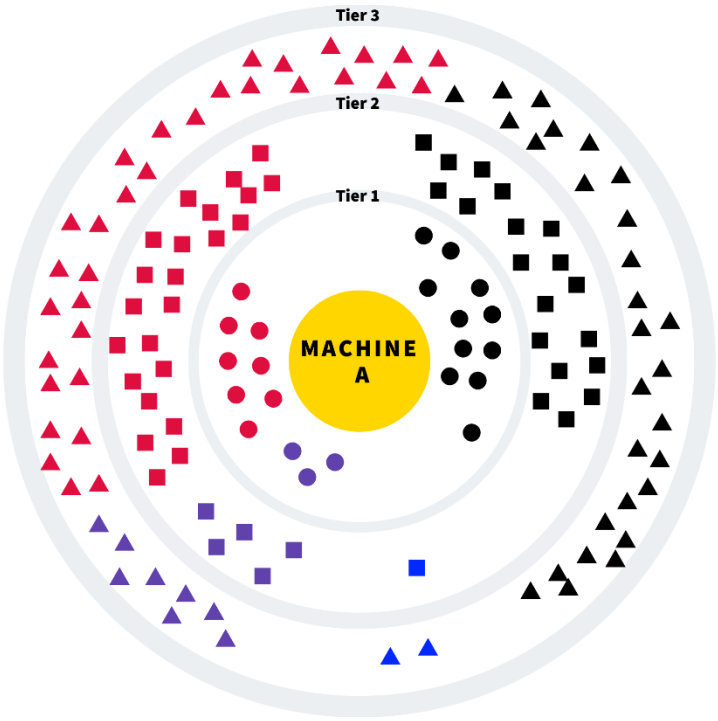
Visualization A Key: *Each shape represents a component of Machine A.* ***Black shapes*** *come from companies not based in China.* ***Red Shapes*** *come from companies based in China.*

Connections to China and Russia

We discovered that **13.57% of suppliers within the first 3 tiers had at least one location in Russia, and 56.43% had a location in China**.

Visualization B (right) shows the companies supplying components used in Machine A. each shape represents a company. Black shapes represent companies with no locations in China or Russia. Blue shapes represent companies with locations in Russia, red shapes represent companies with locations in China. Purple shapes represent companies with locations in Russia and China.

Visualization B



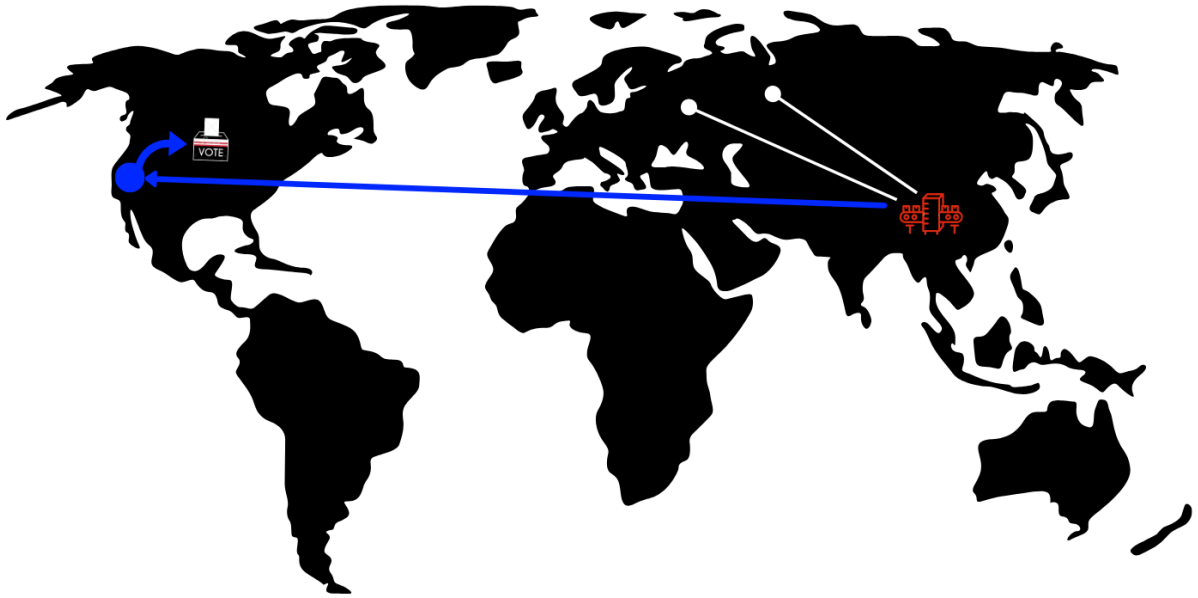
***Visualization B Key**: Companies with locations in China and Russia. **Black shapes** have no locations in Russia or China. **Blue shapes** have locations in Russia. **Red Shapes** have locations in China. **Purple shapes** have locations in Russia and china.*

In **Tier 1** of Machine A's supply chain there are 22 companies. 11 have no locations in either Russia or China, 8 have a location in China, and 3 have a location in both countries. In **Tier 2** of Machine A's supply chain there are 48 companies. 19 have no locations in either Russia or China, 23 have a location in China, 1 has a location in Russia, and 5 have a location in both countries. In **Tier 3** of Machine A's supply chain there are 70 companies. 28 have no locations in either Russia or China, 32 have a location in China, 2 have locations in Russia, and 8 have a location in both countries. In total, **58.6% of companies within the first 3 tiers of Machine A's supply chain have locations in China, Russia, or China and Russia**.

Within the Supply Chain

Our findings included the following sample Chinese companies providing components or software that are used Machine A. They are typical examples of Chinese companies found within Machine A's supply chain, indicating the prevalence of this issue. They include:

Company A: A Tier 2 supplier to the voting machine manufacturer, Company A is China-based corporation with locations in Russia supplying hardware for touchscreens used by a Tier 1 supplier, that are ultimately packaged as part of Machine A. Company A's products have received multiple awards from Chinese state-run entities like the National Radio and Television Administration (NRTA), the organization responsible for (among other things) censoring Chinese media. Additionally, the National Institute of Standards and Technology's National Vulnerability Database (NVD) lists 131 vulnerabilities associated with Company A products, although none are associated with components used in Machine A.



The image above illustrates Company A's locations in China and Russia, as well as the journey to the Tier 1 supplier in America, and ultimately to the manufacturer of Machine A.

Company B: A Shanghai-based company with locations in Russia, Company B provided machinery used by a major processor manufacturer to build processors that are incorporated into Voting Machine A.

These companies represent a sampling of the businesses found at the tier 2 and 3 levels of the voting machine's supply chain. Additionally, at the Tier 1 level, the voting technology company behind Voting Machine A is directly buying many products from China-based companies that are used outside the systems core hardware and software including: power supply adaptors, tablets, machine paneling, and machine covers.

Conclusion

The voting industry takes security seriously and none of our findings indicate that the studied machines are compromised in any way. Voting machines on the market today are certified by the U.S. Election Assistance Commission and are not connected to the internet. The company behind Machine A has their machines tested by independent, accredited laboratories and employs security measures that meet applicable federal standards.

However, the complex and opaque nature of supply chains means most companies, regardless of industry, may not even be aware of their product's connections to countries with a significant interest in influencing or disrupting their business.

The intention of this analysis is to show the impact of global interconnectedness on our daily lives. This level of interconnectedness is simply a fact of doing business, particularly in a technology-based industry and world. And it is not going to reverse anytime soon. It is imperative that we understand all the levels of our supply chains and the suppliers we do business with, in order to avoid potentially catastrophic outcomes and optimize our business relationships.

The minimum requirements of a process to accomplish this should include:

- **Discovery** of the origin of physical and digital components, as well as where their journey through the supply chain touches potentially hostile actors or other risks.
- **Assessment** of multiple risk factors to help regulatory and security officials understand where potential threats lie, and the health of the greater industry
- **Triage** – a method of ranking detected risks to ensure compromise is detected in time to prevent interference.
- **Response** – context about the risk to enable regulatory and security officials to isolate and remediate that threat immediately without disruption of the everyday business.
- **Continuous monitoring** – because technology infrastructure inevitably changes as organizations try to improve access, simplify process, and reduce cost and time, each potentially introducing new risk, the business ecosystem must be continuously monitored for change.

The extent to which this process can be made truly continuous (event-driven, not schedule-driven) will enable rapid identification of, and response to, 3rd party multi-tier risk. However, it is not possible today for analysts and risk managers to achieve a level of risk mitigation necessary to face the dynamic challenge of complex supply chains in critical infrastructure using legacy approaches consisting of intermittent monitoring and annual due diligence deep dives. The volume, velocity, and variety of data necessary for continuous monitoring requires a new approach leveraging artificial intelligence, machine learning and other emerging techniques to be successful and protect business and government interests.

Works Cited

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

2. Taylor, Chloe. “Amazon Investigating Claims Its Chinese Supplier Used Illegal Child Labor to Make Alexa Devices.” CNBC. CNBC, August 12, 2019. https://www.cnbc.com/2019/08/09/amazon-investigating-claims-foxconn-used-child-labor-for-alexa-devices.html.

3. Taylor, Kate. “Mars CEO Says the Global Supply Chain Is 'Broken.' Now, the $35 Billion Food Industry Giant Is Investing $1 Billion to Fix It.” Business Insider. Business Insider, November 17, 2019. https://www.businessinsider.com/mars-plan-to-fix-broken-global-supply-chain-2019-11.

4. Ruggeri, Chris, Chris, Deloitte Risk and Financial Advisory, Deloitte Risk and Financial Advisory, and Deloitte Transactions and Business Analytics LLP. “Extended Enterprise Risk Management Survey 2019.” Deloitte, August 27, 2019. https://www2.deloitte.com/us/en/pages/risk/articles/third-party-risk.html.

5. Schwartz, Samantha Ann. “HackerOne's Breach Highlights Security Business Partner Risk.” CIO Dive, December 5, 2019. https://www.ciodive.com/news/hackerone-data-breach-bug-bounty/568518/.

6. Daniel R. Coats, Director of National Intelligence. 2019. "U.S. Senate Select Comittee on Intelligence." January 29. https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf.

7. Fessler, Pam, and Michel Martin. “Russians Believed To Have Used Spear-Phishing In Election Hacking.” NPR. NPR, June 18, 2017. https://www.npr.org/2017/06/18/533438850/russians-believed-to-have-used-spear-phishing-in-election-hacking.

8. Healy, Jason. 2013. A Fierce Domain: Conflict in Cyberspace. Cyber Conflict Studies Association.

9. United States. Congress. Senate. Select Committee on Intelligence. Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia’s Use of Social Media with Additional Views. Washington: U.S., 2019.

10. Huang, Paul. “Chinese Cyber-Operatives Boosted Taiwan’s Insurgent Candidate.” Foreign Policy, June 26, 2019. https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

11. The Intercept. “Everybody Does It: The Messy Truth About Infiltrating Computer Supply Chains.” The Intercept, January 24, 2019. https://theintercept.com/2019/01/24/computer-supply-chain-attacks/.

12. Parks, Miles. “Cyber Experts Warn Of Vulnerabilities Facing 2020 Election Machines.” NPR. NPR, September 4, 2019. https://www.npr.org/2019/09/04/755066523/cyber-experts-warn-of-vulnerabilities-facing-2020-election-machines.

13. Clark, Douglas. “Federal Funding Earmarked for Election Security.” Homeland Preparedness News, September 23, 2019. https://homelandprepnews.com/stories/36881-federal-funding-earmarked-for-election-security/.

14. 212, and 7871. “What Does Election Security Cost?” Brennan Center for Justice. Accessed November 14, 2019. https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.

15.“The Business of Voting.” Wharton Public Policy Initiative. Accessed November 14, 2019. https://publicpolicy.wharton.upenn.edu/business-of-voting/.

16. U.S. Senate Select Committee on Intelligence, Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations, May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry.

17. Marks, Joseph. “The Cybersecurity 202: Voting Machine Companies May Throw Their Doors Open to Ethical Hackers.” The Washington Post. WP Company, September 24, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/09/24/the-cybersecurity-202-voting-machine-companies-may-throw-their-doors-open-to-ethical-hackers/5d891218602ff1737aef738e/.

18. Norden, Lawrence, Gowri Ramachandran, and Christopher Deluzio. “A Framework for Election Vendor Oversight.” Brennan Center for Justice, November 12, 2019. https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight#footnote9_zyz0tzq.

19. ArjunKharpal. “Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice.” CNBC. CNBC, March 5, 2019. https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

20. Schectman, Joel. “Under Pressure, Western Tech Firms Bow to Russian Demands to Share Cyber Secrets.” Reuters. Thomson Reuters, June 23, 2017. https://www.reuters.com/article/us-usa-russia-tech-insight/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB.

21. “Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks.” Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks | Business Wire, November 15, 2018. https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party.