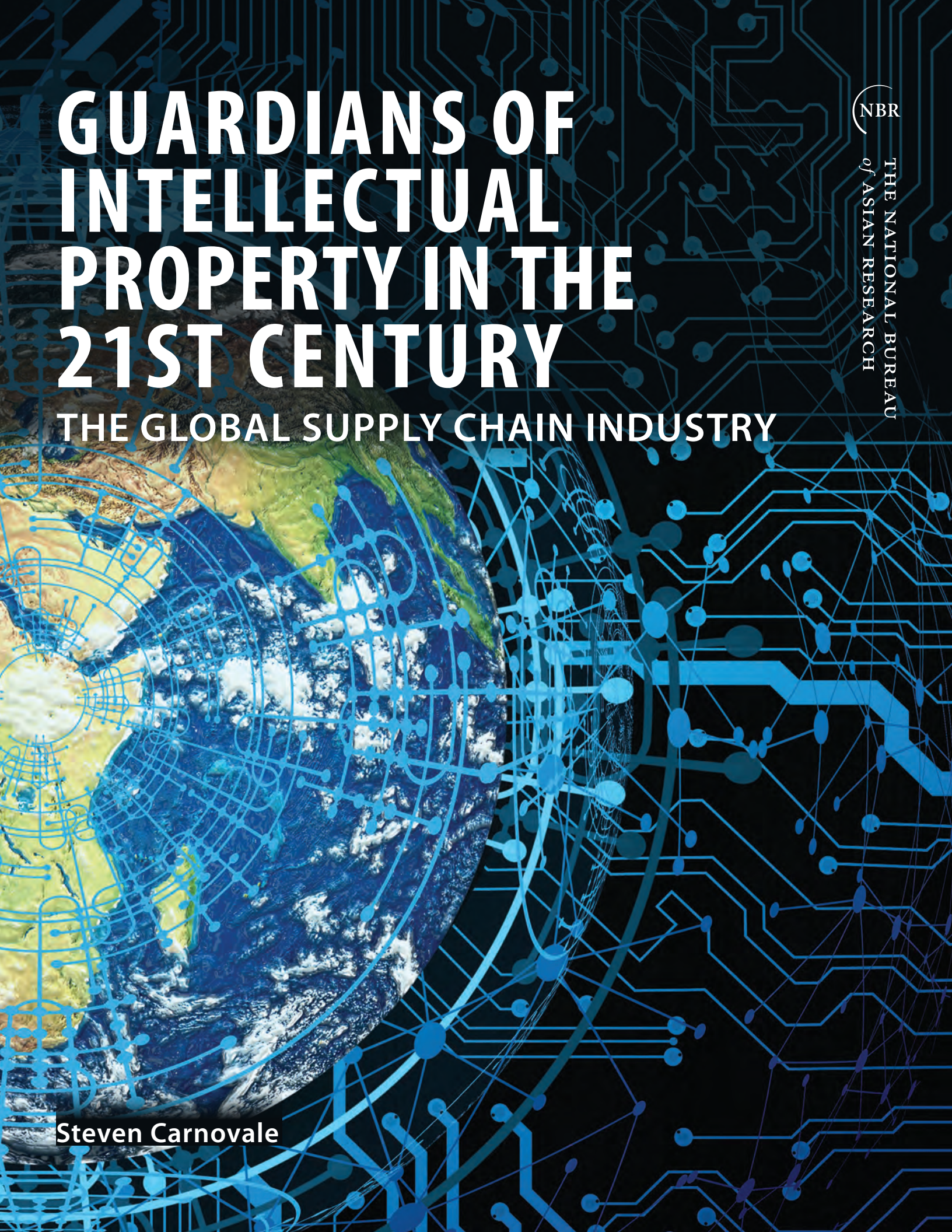
GUARDIANS OF INTELLECTUAL PROPERTY IN THE 21ST CENTURY

THE GLOBAL SUPPLY CHAIN INDUSTRY



Steven Carnovale

NBR
THE NATIONAL BUREAU of ASIAN RESEARCH

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #95 | DECEMBER 2021

GUARDIANS OF INTELLECTUAL PROPERTY IN THE 21ST CENTURY

The Global Supply Chain Industry

Steven Carnovale

THE NATIONAL BUREAU *of* ASIAN RESEARCH

The NBR Special Report provides access to current research on special topics conducted by the world's leading experts in Asian affairs. The views expressed in these reports are those of the authors and do not necessarily reflect the views of other NBR research associates or institutions that support NBR.

The National Bureau of Asian Research helps decision-makers better understand Asia and craft concrete, actionable policy. NBR is an independent research institution based in Seattle and Washington, D.C. We bring world-class scholarship to bear on the evolving strategic environment in Asia through original, policy-relevant research, and we invest in our future by training the next generation of Asia specialists.

Our research is conducted by a global network of specialists and tackles critical issues identified by stakeholders in anticipation of future challenges. The findings are a result of independent scholarship and do not reflect institutional perspectives. Our rigorous standards facilitate informed decision-making based on knowledge rather than ideology.

Established in 1989, NBR is a legacy organization of Senator Henry M. Jackson, who foresaw the national need for an institution to study and inform public policy on Asia in both the public and private sectors. Building on Senator Jackson's bipartisan approach, NBR engages policymakers looking for reliable Asia expertise through sustained interaction in high-trust, nonpartisan settings. Our experts and research have shaped congressional legislation and administration policies, brought issues to the top of the U.S. foreign policy agenda, and attracted worldwide media attention. We mobilize expertise on Asia for a more effective foreign policy.

NBR receives support from foundations, corporations, government (including foreign governments of allies and liberal democracies), and public agencies, and philanthropic individuals. NBR reserves the right to publish findings. We do not undertake classified or proprietary research work, and we observe policies to avoid conflicts of interest.

To download issues of the NBR Special Report, please visit the NBR website http://www.nbr.org.

This is the ninety-fifth NBR Special Report.

NBR is a tax-exempt, nonprofit corporation under I.R.C. Sec. 501(c)(3), qualified to receive tax-exempt contributions.

For further information about NBR, contact:

The National Bureau of Asian Research
1414 NE 42nd Street, Suite 300
Seattle, Washington 98105

206-632-7370 Phone
nbr@nbr.org E-mail
http://www.nbr.org

GUARDIANS OF INTELLECTUAL PROPERTY IN THE 21ST CENTURY

The Global Supply Chain Industry

TABLE OF CONTENTS

PREFACE

The following report was commissioned on behalf of the Center for Innovation, Trade, and Strategy at the National Bureau of Asian Research (NBR) to study the risks to intellectual property (IP) in modern supply chains, and to understand what can be done to protect them. To holistically assess this broad field, the following guiding research questions were advanced:

- What is the current state of the technological arsenal to fight IP theft, and are there gaps?
- Which parts of the supply chain (e.g., sourcing, production, outbound logistics) are the most vulnerable, and what can be done to secure them?
- What will the future of IP theft look like?
- How can companies prepare and hedge this risk appropriately?

In order to address these questions, the primary research methodology was modeled after a semi-structured interview approach, such that issues could emerge naturally. Thereafter, the findings were synthesized into a series of concrete insights and recommendations. Nine experts participated in three roundtable interview sessions between October 2020 and January 2021 in order to solicit expertise and insight. In each case, all interviews were held virtually. The interview protocol was set ahead of time and was standardized to match and align with the stated project objective and outcomes. Each session was recorded with the participants' permission, and ahead of time the participants were made aware that the meeting was being governed by the Chatham House Rule. All quotes in the report that follows are presented anonymously and have been edited for clarity and concision of message. In all cases, the interviews lasted approximately 90 minutes.

In addition, the principal investigator, Steven Carnovale, solicited three supporting briefs, which appear in the appendices. The first appendix details the legal challenges associated with IP infringement in several countries with high-dollar volumes of foreign direct investment. The purpose of this brief is to provide background legal research to investigate current legislation and legal thought on IP theft and strategies to address it. The second and third appendices examine how blockchain and artificial intelligence are modernizing and reshaping supply chains, as well as how these technologies can be leveraged to improve supply chain security and assist in better protecting IP throughout supply chains. In all cases, sources, data, and other methodologies have been disclosed.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #95 | DECEMBER 2021

Guardians of Intellectual Property in the 21st Century

The Global Supply Chain Industry

Steven Carnovale

STEVEN CARNOVALE is Assistant Professor of Supply Chain Management and Program Director at the Saunders College of Business at the Rochester Institute of Technology. He can be reached at <scarnovale@saunders.rit.edu>.

EXECUTIVE SUMMARY

This report examines how increasing complexity in modern supply chains has introduced new vulnerabilities for companies' intellectual property (IP) and explores ways to better protect IP throughout supply chains, with an emphasis on the use of emerging technology to achieve this goal.

MAIN ARGUMENT

The length and complexity, the number of geographically distributed firms, and the number of products that modern supply chains are tasked with delivering to consumers have grown exponentially over the past several decades. Regional supply chains have transformed into global ones with IP and related proprietary information being dispersed across firms' extended enterprises. Couple these trends with the increase in digitization and the larger presence of internet-enabled technologies, and the number of attack vectors for malevolent actors has outpaced potential protections and safeguards. Succinctly stated, supply chains are vulnerable to IP theft. But questions remain, such as which parts of supply chains are the most vulnerable? What technologies exist to help protect IP? What is missing, and what can be done? The following measures are needed to better protect IP throughout supply chains: (1) the implementation of training for supply chain personnel to match the scale and scope of the increasingly pervasive vulnerabilities of IP in supply chains, (2) the implementation of protocols for traceability and tracking of raw materials at the beginning of the supply chain, and across entities of the supply chain, ideally through an established set of standards for IP protections in the onboarding process, and (3) the establishment of a detection, mitigation, and recovery strategy such that firms have a balanced approach to handling IP theft.

POLICY IMPLICATIONS

This report finds that companies seeking to better protect their IP in supply chains should both take steps to mitigate personnel-related risks and develop a detection, mitigation, and recovery strategy. Key elements to these approaches include the following:

- Train personnel to better understand and identify potential IP vulnerabilities and breaches.
- Improve monitoring and detection capabilities throughout supply chains, including by implementing more stringent traceability protocols, utilizing supplier scorecards, leveraging AI and blockchain technologies, and improving information sharing.
- Strengthen mitigation efforts, with a focus on cybersecurity, by limiting and monitoring access to data and utilizing practices such as encryption and two-step authentication.
- Establish recovery protocols that ensure a quick return to a pre-disruption state by using redundant suppliers to allow for shifts away from bad actors and by having legal strategies in place to respond to potential malpractice.

Supply chains are the primary value-creating engines of the modern economy, working in the background to provide the world with the goods it needs to survive. Generally speaking, supply chains handle the identification and acquisition of raw materials and services; the production, manufacturing, and distribution of finished and work-in-process goods and services to manufacturing locations; and the movement and storage of finished products from the source of production to the end consumer.

In the early years after the industrial revolution, supply chains were, at most, national, though predominantly subnational. Over the past few decades, however, they have grown considerably longer, more complex, and much more global in nature. No longer are firms constrained by geography when they look to source a part or service. Now, advances in telecommunications and freight technologies have opened up access to every corner of the world. Couple this access with increased levels of regional economic integration through reductions in trade barriers, including through preferential trade agreements, and companies can now access markets that previously would have been impossible. For both consumers and manufacturers alike, this is a boon. Consumers gain access to a more diverse set of goods at a lower price, and manufacturers can take advantage of the lower cost of labor and greater access to raw materials.

Despite these major economic benefits, the globalization of supply chains has also introduced new risks. Among the myriad vulnerabilities that such technological shifts engender, one lurking threat stands out: the real, and growing, risk of intellectual property (IP) theft. IP is defined by the World Intellectual Property Organization (WIPO) as creations, both tangible and intangible, resulting from human intellect.[1] Such creations are generally protected by patents, copyrights, trademarks, and other legal protections to safeguard against infringement on or the exploitation of someone else's property (for more information on the legal protections of six key Asian countries, see **Appendix 1**). As supply chains have lengthened and become more global, firms' IP has been exposed to threats unimaginable several years prior. For example, a report from the Commission on the Theft of American Intellectual Property at the National Bureau of Asian Research (NBR) echoed this point regarding lengthening supply chains:

> [S]tolen IP represents a subsidy to foreign suppliers that do not have to bear the costs of developing or licensing it. In China, where many overseas supply chains extend, even ethical multinational companies frequently procure counterfeit items or items whose manufacture benefits from stolen IP, including proprietary business processes, counterfeited machine tools, pirated software, etc.[2]

The risk that firms operating in or along global supply chains face with respect to IP is extremely pervasive. In a survey by the American Chamber of Commerce in Shanghai, 54% of companies (all of which are foreign companies operating in China) believed that "lack of IP protection and enforcement" is a hindrance to their business.[3] This belief was most common in the pharmaceutical, medical devices, and life sciences industry, at 71.4%, followed closely by industrial manufacturing, at 68.4%. Indeed, this threat is not imaginary. The Commission on the Theft of American Intellectual Property calculated that "the annual losses are likely to be comparable to

---

[1] *Understanding Intellectual Property*, 2nd ed. (Geneva: WIPO, 2016), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_895_2016.pdf.

[2] Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle: NBR, 2013), https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf.

[3] AmCham Shanghai, "2020 China Business Report," September 2020, https://www.amcham-shanghai.org/en/taxonomy/term/1163.

the current annual level of U.S. exports to Asia—over $300 billion."[4] The problem is so vast that public-private partnerships have cropped up to protect the most vulnerable industries (i.e., those connected to the defense industrial base or critical technologies). One recent example features the intelligence community and the U.S. Defense Advanced Research Projects Agency partnering to create systems to protect IP along the semiconductor supply chain.[5] However, this risk is not limited solely to the most cutting-edge industries, such as semiconductors. An automotive supplier, for example, working with a major original equipment manufacturer that may digitally receive highly confidential schematics for a new part it is manufacturing introduces cybertheft risks to the IP. Another significant risk is the degree to which the Internet of Things (IoT) connects devices via cloud computing but also exposes serious security threats and vulnerabilities. This is not anecdotal. A recent Deloitte report finds that cybertheft and related incidents are vastly up, particularly during the Covid-19 pandemic.[6]

Furthermore, all functions across the supply chain are vulnerable to IP infringement. Manufacturing, either internally or through contracted third parties, often involves unique and proprietary production processes, rich with IP all too vulnerable to theft via corporate espionage. Firms have established manufacturing joint ventures in various parts of the world where leakage of IP renders them vulnerable to exploitation and extremely expensive remediations (e.g., ransomware). The 2018 Section 301 Report estimates that from China alone, "theft of American IP currently costs between $225 billion and $600 billion annually"—a figure that aligns with the findings of NBR's Commission on the Theft of American Intellectual Property.[7]

Cumulatively, anecdotal reports as well as empirical findings continue to point to the supply chain as a unique vulnerability in the war against IP infringement. In order to provide clarity on this issue, this report addresses the following questions:

- Which parts of the supply chain (i.e., sourcing, manufacturing, and outbound logistics) are the most vulnerable, and what can be done to secure them?
- What is the current state of the technological arsenal to fight IP theft, and are there gaps?
- What best practices can companies leverage to mitigate IP risks?

This report outlines potential responses to these questions. First, specific IP concerns around sourcing, manufacturing, and outbound logistics are discussed. Next, the technological solutions that exist are reviewed, followed by an examination of where the gaps are and what needs to be done in order to close them. The central aim is to provide decision-makers with clarity on how to move forward to secure IP along and within the largest value-creation engine of the modern economy—the global supply chain.

---

[4] Commission on the Theft of American Intellectual Property, *The IP Commission Report*.

[5] N.F. Mendoza, "Intel and DARPA Partner to Advance U.S. Semiconductor Supply Chain Security, Domestic Manufacturing," Tech Republic, March 18, 2021, https://www.techrepublic.com/article/intel-and-darpa-partner-to-advance-us-semiconductor-supply-chain-security-domestic-manufacturing.

[6] Cedric Nabe, "Impact of COVID-19 on Cybersecurity," Deloitte, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

[7] Office of the U.S. Trade Representative, "Section 301 Report," March 22, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF; and Commission on the Theft of American Intellectual Property, *The IP Commission Report*.

Where Are the Largest Vulnerabilities?

In February 2021, President Joe Biden signed Executive Order 14017, which seeks to strengthen U.S. supply chains through a comprehensive review of their vulnerabilities. The executive order directs agency heads to focus on "the defense, intelligence, cyber, homeland security…or other contingencies that may disrupt, strain, compromise, or eliminate the supply chain—including *risks posed by supply chains' reliance on digital products that may be vulnerable to failures or exploitation*" (emphasis added).[8] Given the increasing utilization of technology in modern supply chains, cybersecurity threats continue to mount, and the consequences of a breach are massive. In 2020 the average cost of a data breach was $3.86 million, with the average resolution time 280 days, and with healthcare facing the highest average cost.[9] This is a serious issue when considering the degree to which healthcare relies on IP (e.g., drug formulations, vaccine development, and various other R&D initiatives). In fact, the FBI has recently partnered with the National Intellectual Property Rights Coordination Center on several initiatives, one of which explicitly focuses on the inclusion of counterfeit goods into the Department of Defense (and other federal) supply chains.[10] Clearly, the threat that modern supply chains face is gaining greater attention among policymakers.

While the review will provide a critical step forward in mitigating the inevitable risk that supply chains face in today's global landscape, additional nuance is required. Specifically, this includes drilling down into which functions of the supply chain are particularly vulnerable to IP theft. For the purposes of this report, we organize these functions as follows: (1) sourcing (i.e., raw material and vendor acquisition/management), (2) production and manufacturing, and (3) outbound logistics and distribution. Each of these groups performs a key role to effectively provide goods and services to the global economy, and each is faced with key challenges in protecting IP.

A Cross-Functional Supply Chain IP Issue

Regardless of which component or function of the supply chain is being examined, there is one constant: people are ultimately responsible for the planning, execution, and safeguarding of supply chain assets and, consequently, IP. In all the interviews with experts from the field conducted for this report, in one way or another regardless of experience working in supply chain management, one critical vulnerability kept arising: the human factor.

Trade secrets are not always kept in a folder marked "TOP SECRET" in an executive's office. Rather, these secrets—proprietary knowledge or information, often related to the processes of design and production inherent to supply chains—often reside in the skill and talent of the personnel employed at the company. This expertise is multifaceted: (1) the skill/talent for which the employee was hired, (2) the decision-making fiat that the employee has, and (3) the skill and talent accumulated on the job. Bad actors often seek to extract and exploit proprietary information existing in the form of employees' knowledge and skills. At the same time, vulnerabilities arise out of how much decision-making authority is delegated to employees, who might then make choices

[8] White House, "Executive Order on America's Supply Chains," February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains.

[9] John Zorabedian, "What's New in the 2020 Cost of a Data Breach Report," Security Intelligence, July 28, 2020, https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report.

[10] FBI, "Intellectual Property Theft/Piracy," https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft.

that expose IP and other digital assets to the risk of theft. There are two overarching vulnerabilities in this space: the human factor and the subversion of process-based controls.

The human factor. The double-edged sword of talented employees is that they are hard to acquire, and when acquired, they are hard to keep. With respect to IP, the difficulty is related to what occurs when employees depart the firm that owns the IP or has used or otherwise been exposed to IP as part of the supply chain. This poses risks associated with employees taking proprietary processes and ideas with them or being vulnerable to other malevolent actions from outside entities. A typical strategy is to employ legalese and build noncompete, nondisclosure, or other contractual measures to hedge against such breaches. But these measures do not always work.

A recent example of this dynamic highlights how pervasive the problem is. An executive from a Chinese oil and gas company was recently charged with theft of trade secrets for colluding with a local external consultant in order to extract critical process information. The consultant "was to be paid $1,000 each day of a 15-day visit, according to the charges. *This agreement allegedly also included a confidentiality provision*" (emphasis added). Then, the consultant transferred proprietary information to the malevolent firm in an unauthorized manner. The result was that the "corporate entities could be fined up to $5 million or three times the value of the stolen trade secret, whichever is greater," and the perpetrator "faces a possible prison sentence of up to 10 years as well as a $250,000 fine or twice the gross gain or loss."[11] Now consider the amount of interaction that firms have with external entities in increasingly long and complex supply chains. With multiple tiers of suppliers and a global presence, the contractual governance to adhere to or protect the firm's IP can become weaker and thus pose significant risks. Consider the situation where, for example, one supplier has contracts to supply a similar (or even identical) component to multiple customers. In this case, the supplier would be privy to IP for two (or more) distinct competitors, which is inherently risky. In this example, the perpetrator was caught, but what about the countless others who are not? Of course, this is only one example, but there are numerous others that all speak to the risk the human factor can cause with respect to IP leakage.

Some comments from the expert panel consulted for this report highlight the importance of this human factor:

- "Access to massive technology, and the way that we protect it today, seems to be crude. Lots of violations exist, and they are human-based violations. Lots of IP resides in the individual, and there is a problem with this….[T]here can be a lot of strategy related to how to protect IP, and some IP lawsuits (i.e., a legal strategy), but the weak link…is when the guards let them [perpetrators] through. The human factor is key."
- "There needs to be proper risk management and risk assessment that are focused on IP protections, and enabling people is critical to preserving this security. The human factor is the critical link that enables a firm to control and maintain propriety over its IP in a competitive landscape."

The subversion of process-based controls. Conventional strategy to protect IP generally deals with protecting patents, copyright protections, and trade secrets. In the United States, such protections are enumerated in the Constitution. Article I, Section 8, provides Congress the power

[11] "Chinese Energy Company, U.S. Oil & Gas Affiliate and Chinese National Indicted for Theft of Trade Secrets," U.S. Department of Justice, October 28, 2020, https://www.justice.gov/usao-sdtx/pr/chinese-energy-company-us-oil-gas-affiliate-and-chinese-national-indicted-theft-trade.

"to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[12] In fact, the first U.S. patent was issued in 1790. While the application and vetting processes have changed, the legal structure of ownership rights has not.

Copyright protections are generally related to creative pursuits (e.g., art and multimedia), whereas patent protections relate to the invention and novelty of an industrial product.[13] Trade secrets are a form of IP that is commercially valuable and contains confidential information on a product or process (e.g., the recipe for a food product).[14] In the case of a patent or a copyright, each mechanism's purpose is to act as a process-based control to protect the owner of the IP, whereas a trade secret represents an internal protection of sorts. Yet, the mere application for a patent, for example, could signal to a malevolent actor that the submitting firm has something worth stealing, thereby exposing the firm to vulnerability. Some experts even suggest not filing a patent at all![15] Further, consider where and how management stores proprietary information. Take, for example, information that explicitly details how a new manufacturing process will be executed, or an R&D document detailing the features of a company's new smartphone. Is the information stored on hard disks internally, or on cloud servers externally? Who has access? What about the transition from one cloud storage provider to another? What if a schematic for a patent submission has been sent to a printer that has random access memory, thereby opening up an access point for a hacker to siphon off IP? In each of these instances, for a supply chain to effectively produce products and maintain its competitiveness, all IP along the supply chain needs to be secured and protected. Unfortunately, the expansiveness of modern supply chains makes this a challenging proposition.

All these anecdotal scenarios illustrate operational realities that management must grapple with. As a result, while process-based controls can be put into place, the old adage rings true: where there is a will, there is a way. A recent Deloitte report sums up the problem rather succinctly: "Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create growing challenges in protecting trade secrets."[16]

Some comments from our expert panel illustrate the scope of the challenges involved in the subversion of process-based controls:

- "There is a certain assumption that when going global there will be theft. So, the locational decisions become critical. Thinking through patented vs. trade secret, how much do I want to patent? Interestingly, this could expose the firm to vulnerability. So, the legal strategy to protect the IP (i.e., the patent) can signal that there are products that are so innovative that they need to be protected. On the product side, these conversations have been ongoing, but it is typically after the production, rather than before, thus opening up the firm to IP-related issues."
- "The technology is there. The processes and the people, these are the key issues for IP protections."

---

12 "The Constitution of the United States: A Transcription," National Archives, https://www.archives.gov/founding-docs/constitution-transcript#toc-section-8.

13 *Understanding Intellectual Property*, 6.

14 WIPO, "Trade Secrets," https://www.wipo.int/tradesecrets/en.

15 "10 Effective Ways to Protect Your Intellectual Property," *Forbes*, July 23, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/07/23/10-effective-ways-to-protect-your-intellectual-property/?sh=2390722732e1.

16 "The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property," Deloitte, https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html.

Subsequent sections will dive into the IP-related nuances and vulnerabilities associated with specific portions or functions of the supply chain. But the human factor, juxtaposed with (and perhaps amplified by) the subversion of process-based controls, rises above other challenges as a truly cross-functional problem. That is, across all of the core supply chain functions (i.e., sourcing, manufacturing, and delivery) the procedural and legalistic attempts to ebb the theft of IP are all rendered moot when the human factor is not taken into account.

IP Issues in Sourcing

Sourcing refers to managing the external resources of a firm. This includes the identification and acquisition of raw materials, work-in-process inventory, maintenance/repair/operating inventory, internet services, and logistics services, among other resources. In most cases, the sourcing function is the "start" of the supply chain; it is also where the risks to IP begin. In interviews conducted for this report, a few relevant themes for IP and sourcing kept arising. Broadly speaking, these issues are related to traceability and counterfeit goods. An important point to note is that these concepts are two sides of the same coin but manifest at different times in the sourcing process. Generally speaking, a lack of traceability with respect to raw materials or other work-in-process inventory causes (or at least facilitates) the inclusion of counterfeit goods into the supply chain. A somewhat recent and rather notable example of the balance between traceability and counterfeiting is the "horsemeat scandal" at various supermarkets in Ireland and the United Kingdom. After the Food Safety Authority of Ireland began inspecting the DNA of various frozen meat products amid suspicion of deceptive practices, it was revealed that over one-third of the "beef" samples contained horsemeat and nearly 85% contained pig DNA.[17] The supermarket Tesco later came under scrutiny when one of the ready-made meal products (spaghetti with "beef" bolognese) was found to contain 60% horsemeat.[18] The meal was sourced from a French factory, whose suppliers were spread out across Europe, extending the geographic and administrative length of the supply chain to a point where fraud and deception become veritably impossible to root out. Thus, the challenge of traceability makes the issues related to the human factor noted above even more pronounced, as IP in the supply chain requires trust between partners, even when there are contractual considerations involved. This issue is only amplified by the complexity associated with protecting trade secrets, industrial design, or other more technologically dependent IP.

Traceability. The challenge of ensuring transparency in the supply chain, particularly as it relates to the inbound source of raw materials, presents issues of quality control. For manufacturers that rely primarily on trust in their suppliers not to incorporate fraudulent products, the inclusion of substandard materials can easily become a problem. As supply chains continue to expand their supply bases globally, this risk only increases. The consequences for quality, resulting from a lack of transparency, can be grave.

The pharmaceutical industry provides a rich context to examine the importance of this issue. Various products rely on temperature-controlled delivery and storage, in addition to strict quality standards throughout the supply chain. In addition, this industry is also subject to the lengthening and globalization of supply chains as "roughly 80% of active pharmaceutical ingredients and

[17] Felicity Lawrence, "Horsemeat Scandal: The Essential Guide," *Guardian*, February 15, 2013, https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide.

[18] "Horsemeat Scandal: Tesco Reveals 60% Content in Dish," BBC, February 11, 2013, https://www.bbc.com/news/uk-21418342.

40% of finished drug product are imported into the U.S. from overseas."[19] In order to enhance traceability and strengthen protections, President Barack Obama in 2013 signed into law the Drug Supply Chain Security Act, which "outlines steps to build an electronic, interoperable system to identify and trace certain prescription drugs as they are distributed in the United States." This law enhances the ability of the Food and Drug Administration (FDA) to protect consumers "from exposure to drugs that may be counterfeit, stolen, contaminated, or otherwise harmful." It also improves "detection and removal of potentially dangerous drugs from the drug supply chain to protect U.S. consumers." Additionally, the law directs the FDA to establish "national licensure standards for wholesale distributors and third-party logistics providers, and requires these entities report licensure and other information to FDA annually."[20] Effectively, the legislation "require[s] drug supply chain stakeholders to trace prescription drugs, in a secure manner, from the manufacturer down to the dispenser of the drug" in order to improve overall traceability and ensure the integrity of the pharmaceutical industry.[21] While the Drug Supply Chain Security Act is quite helpful, it only covers one sector. This law can, however, present a framework for an industry-wide standard (which will be discussed further in subsequent sections).

The following comments from interviews with the expert panel for this report highlight the issue of traceability:

- "Traceability means that the raw material source would have the batch number, which is recorded, and then the quality documentation would be sent down the line for verification throughout the supply chain."[22]
- "Things that are not traced (raw materials) are most vulnerable, as well as anything that has variability (in price and quality of supply). Price is often a determining factor for procurement, and thus counterfeiting can be a concern [when the price is too good to be true]. There is a clear relationship between pricing and counterfeiting."

Counterfeit goods. With respect to inbound materials, there is no coherent standard to verify the authenticity of a raw material (e.g., traceability), and as a result potentially the product itself. This gives rise to significant opportunities for infringement of a product's IP. One assessment by the FBI suggests that "counterfeit goods cost the U.S. economy an estimated $600 billion a year, or 3% of the U.S. gross domestic product."[23] The counterfeit issue arises as a result of a lack of transparency and the opacity of information being shared across supply chain entities and manifests in increased warranty, liability, and service costs to manufacturers.

Comments from the expert panel highlight the issue of counterfeit goods:

- "Lack of visibility and transparency, no data passed on from one to the other. Sharing data does not happen as much as it should, and as a result vulnerabilities arise."
- "Transparency (or lack thereof) is the largest issue, and as a result much of the information is not passed onwards…. Process alignment is an issue. Integration is required to ensure that

---

[19] Ned Pagliarulo and Edwin Lopez, "Top Challenges Facing Drug Supply Chains," BioPharma Dive, April 23, 2018, https://www.biopharmadive.com/news/top-challenges-facing-drug-supply-chains/521876.

[20] "Drug Supply Chain Security Act (DSCSA)," U.S. Food and Drug Administration, https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa.

[21] Christopher Smith, "INSIGHT: The Drug Supply Chain Security Act and Preemption of State Laws," Bloomberg Law, April 2, 2019, https://news.bloomberglaw.com/pharma-and-life-sciences/insight-the-drug-supply-chain-security-act-and-preemption-of-state-laws.

[22] For readers interested in how blockchain technology could be implemented as a traceability protocol, please see Appendix 2.

[23] Jennifer Schlessinger and Andrea Day, "Here's How the Trade War Could Lead to a Boom in Counterfeit Goods," CNBC, March 13, 2019, https://www.cnbc.com/2019/03/13/heres-how-the-trade-war-could-lead-to-a-boom-in-counterfeit-goods.html.

the transparency is heightened between members of the supply chain. Information sharing with partners needs to be significantly improved to facilitate trust and reduce the potential for opportunistic behavior."

IP Issues in Manufacturing

The manufacturing portion of supply chains is chiefly tasked with transforming raw materials and work-in-process inventories into finished goods for ultimate distribution to consumers. In the sequencing of a supply chain, this part of the process would be subsequent to the sourcing function, and as a result what happens in the manufacturing processes of firms is largely dependent on what is being acquired externally. Therefore, the issues raised above in the sourcing process implicitly affect the manufacturing process. But there are additional considerations—specifically, issues related to product quality, brand image, and data security.

Product quality. As manufacturing continues to globalize, and as firms engage contract manufacturers more and more frequently, they can leave themselves vulnerable to theft of IP on the process side. There are also risks to theft of IP on the product itself, particularly related to reverse-engineering. The consequences of fraudulent or subpar quality inputs into the production process can have serious consequences to the original equipment manufacturer, often arising out of warranty expenses and other related quality failures. If the parts entering into the final product are of poor quality, this could compromise the end product, resulting in serious financial and reputational loss.

The Takata airbag recall is an excellent example of the potential liability and reputational risk that firms can face if an input to a product is fraudulent. In the early 1990s, Takata, a major airbag supplier to several automakers, switched the chemical composition of the component required to deploy its airbags. This new chemical composition, when exposed to prolonged heat and humidity, can deteriorate and cause the airbag to deploy too soon, or not at all, leading to serious injury or death. In the mid-2000s an internal report indicated that Takata knew that this could and likely would happen, but the company covered up the finding and continued to supply numerous automakers with fraudulent and inferior products. After multiple deaths and injuries and several million recalled airbags, Takata pled guilty to criminal charges. The economic cost to resolve the issue was approximately $24 billion, which was four times greater than Takata's revenue forecasts.[24] This was not just an issue for Takata, as the company's poor-quality products resulted in Toyota, Mazda, Subaru, and BMW also entering into agreements totaling over $550 million for the losses encountered by their customers.[25]

Interviews with the expert panel for this report highlight the supply chain challenges related to product quality:

- "From the original equipment manufacturer side of things in the automotive space, fraudulent products can be an issue, particularly because of the complexity of the product. There can be over 10,000 parts in a new vehicle. There are a lot of theft instances of product (fit and finish)… there are a lot of joint ventures, there is some shared equity, and as a result vulnerabilities for IP leakage arise."

---

[24] "Takata Puts Worst-Case Recall Costs at $24 Billion," Bloomberg, March 29, 2016, https://www.bloomberg.com/news/articles/2016-03-30/takata-said-to-put-worst-case-airbag-recall-costs-at-24-billion.

[25] Charisse Jones and Nathan Bomey, "Timeline: How Takata's Air-Bag Scandal Erupted," *USA Today*, June 25, 2017, https://www.usatoday.com/story/money/2017/06/25/takata-air-bag-scandal-timeline/103184598.

- "With respect to IP in the context of product fraud, quality control can be an issue. There is a large market for knock-off products."

Brand image. The negative impact on brand image that arises from IP infringement and related maladies also can be dire for firms. The rise in platforms such as Amazon, Alibaba, and related online marketplaces has simultaneously increased access to markets and consumers and opened up new pathways for malevolent actors to sell counterfeit goods fraudulently listed as genuine. Increased levels of drop-shipping (a customer fulfillment approach where products go directly from the manufacturer/distributor and bypass a retail or other intermediary with the goal of decreasing lead times to the customer) have obfuscated the clarity of ownership and enabled "passing of the buck" with regard to who is legally at fault.

Take, for example, a fraudulent product sold to an unknowing consumer via Amazon through a third-party reseller. The reseller never physically owns or holds the good but merely processes the order and then facilitates shipping to the end consumer. Is the platform responsible for verifying the authenticity of the product? Is the reseller? Is the shipping company? Is the brand? Ultimately, regardless of who is responsible, the brand image can be jeopardized. This cuts both ways: on the product side and on the platform side. From an IP standpoint, a firm has a vested interest in protecting its brand via the channels through which its products get distributed. On the other hand, unless there is traceability and strict governance between manufacturer and retailer, once the ownership of the product has transferred, this issue becomes challenging to police. Consumers also "punish" the platform that sold the product, and this may well be justified if the platform knowingly allowed counterfeit goods to enter its distribution channels. Yet, the issue becomes even murkier if it was the brand that allowed a counterfeit product into circulation in the first place.

Some comments from the external panel highlight this issue:

- "Incentives and alignment are key. Airlines care about kilos, ocean carriers care about 20-foot containers. A retailer, for example, cares about compliance. So what are the incentives and alignments? In the marketplace, the risk and incentive model is very different. The responsibility is shifted based on the ownership of the product/brand. There is no idea for how to solve this problem, or who/where/what the issues are. The biggest risk and vulnerability is the business model that firms use to commercialize their IP. IP compliance is risk mitigation, and this is a necessary component for the protection of IP."
- "Now, with social media, all IP becomes a brand issue."

Data security. A final issue that arises in the context of IP infringement and manufacturing is data security. This issue largely arises in collaborative manufacturing environments where joint engineering teams work together on a schematic/computer-aided design or other digital medium through which the product is developed. It is conceivable that product design and engineering teams from all corners of the world simultaneously tap into a common server that is hosted in the cloud, which is allegedly secure. On the one hand, it is a marvel of modern technology to be able to codevelop a product leveraging talent across the world. On the other hand, the IP housed on these servers is an increasing cybersecurity vulnerability, the costs of which are enormous and increasing. Malevolent actors seek to gather software code, patented trade secrets, or other potentially valuable information that they can exploit for their gain.

There are effectively two key points of concern about data security with respect to IP. First, as global supply chains continue to lengthen geographically, and the number of agents to whom

a firm grants access continues to grow, more and more confidential and proprietary data must enter a cloud-based environment to allow collaboration between entities. Second, there is seldom appropriate onboarding to govern the handling of proprietary data, as well as other data security concerns, thus exposing firms to a major IP vulnerability. These issues are unrelenting and will likely grow exponentially over the coming decades, as highlighted by the following quotes from the expert panel:

- "Necessarily, the Internet of Things expands the connection points to information and the potential for extraction/infiltration. Data security is critical."
- "Many people are tapping into common databases, design data, engineering data…. [W]hen the number of outside resources is increasing, the risk is higher. More entities, more risk. Cybersecurity protections are key. Electronics parts and materials with…extensive distribution networks can cause vulnerability."

IP Issues in Outbound Logistics and Delivery

The outbound logistics function of the supply chain is responsible for the movement of goods, either from the raw material source to the manufacturing facility or from the manufacturing facility to its next destination (i.e., distribution center, retail establishment, or final consumer), and storage in between. Here, international borders are crossed, government agencies are interacted with, and intermediary connections are made. The storage element occurs in between each phase of the movement, where warehouses act as repositories for products yet to be sold, or yet to be transformed into finished goods. As supply chains have lengthened and globalized, few areas of the supply chain have been stretched and tested as much as the logistics space. As a result, these processes are uniquely vulnerable to malevolent actors. Issues of title, ownership, liability, and information security pervade this space. Third-party logistics providers act as guardians of information but are susceptible to hacking and can be complicit in the inadvertent facilitation of theft and leakage of IP. In the logistics space, two prominent threats arise: data security and product guardianship.

Data security. While data security in the above section referred to specific IP associated with the product itself, here it refers to IP around process and delivery. IP around delivery deals with strategy: the design and deployment of logistics networks, and the processes associated with how a product will arrive at the consumer. Strategy includes plans for developing a new distribution center, any trade secrets associated with product allocations to a free-trade zone, or even the rebalancing of work-in-process inventory to a new intermediary location.

Take, for example, recent innovations around UPS's drone delivery, where there is IP for the technology to optimize scheduling and the design of the drone itself. The issue of safeguarding data and ensuring its security is an immense challenge for logistics professionals, particularly because of the volume and variety of products being moved. The adoption of IoT technology to increase connectivity and access to information via microchip and internet-enabled devices has led to severe new vulnerabilities for IP theft. Necessarily, the IoT increases the connection points and thus the exposure to theft. This increased exposure creates complexity, which tends to be a significant driver of fraudulent activity and can lead to vulnerabilities such as spoofed data about product shipments, sensors on transportation that are hacked, and shipments that are hijacked, facilitating theft of products and their resultant IP (through reverse-engineering).

Interviews with the expert panel highlighted these issues with data security around process and delivery:

- "Spoofing of data and information (product level and shipment level) becomes an issue. Also, in the customs-clearance phase the introduction of false information can cause serious problems."
- "Logistics certainly has the highest number of issues and the largest risks. The movement of material and the opportunities to hold random information and deduce compromising information are inherent in the third-party-logistics space, as is the opportunity to introduce information that can compromise shipments, IP, and other critical and proprietary information."
- "[An important issue is the] interactions between country customs, and whether or not they have embraced digitization. In the freight forwarding industry, there is a gap between what should be and what is done. Current systems are archaic. Application program interfaces to reduce the complexity and friction of the transactions exist, but their adoption is not widespread to the degree that would be helpful. With regard to protecting IP customs and connectivity of information between entities, drop-shipping and other logistics processes around how the information is going to move (and to whom it will be released) become critical."

Product guardianship. In the ever-expanding space of logistics and freight, ownership terms and liability can get messy. While shipment terms (i.e., "free on board"—when ownership and assumption of risk are transferred when the product is placed onboard the vessel of the buyer's choice; or "free alongside"—where the assumption of risk is transferred when the product is placed adjacent to the vessel of the buyer's choice, usually at the port of departure) are pre-negotiated, and International Commercial Terms can help facilitate the transaction, the guardianship of the product is significantly more opaque.

Recall the issue with fraudulent or subpar quality products entering the production process. When products sit in warehouses, if left unmonitored, they are vulnerable to shrinkage. This shrinkage can lead to malevolent actors either reverse-engineering products and flooding the market with discounted, poor-quality products or replacing original products with lower-quality alternatives. If the product being reverse-engineered is a finished good, there are issues associated with brand image, quality, and warranty concerns, as noted above. The essential issue is that there is often ambiguity associated with who will interact with the products, thus exposing firms to IP-related vulnerabilities, despite any contractual governance (or perhaps lack thereof) that may be in place. All told, logistics as a function is highly vulnerable to IP theft.

The expert panel highlighted the following issues with product guardianship:

- "All points of the supply chain are vulnerable to IP theft, but mostly it is the warehousing piece…. [M]any products spend the most time at the warehouse, and as a result, this is an area of opportunity. Currently, this space is significantly lacking technology and tracking capabilities. Many firms know that this is an issue, and this is the opportunity for a technological improvement or innovation to help solve this problem of transparency."
- "Global security events (e.g., September 11) have transitioned the focus of customs to security rather than other pursuits (e.g., IP theft). The scale has gone from millions to tens of millions."

The State of Technology for IP-Related Supply Chain Issues

Today, most IP resides in a digital medium (i.e., servers and onsite computers). As such, a breach of a firm's IP often implies that there has been a breach of a firm's cyberdefenses and cybersecurity practices. Coupled with the increased complexity of supply chains and IP residing in distributed systems across multiple firms, this is a recipe for theft and malevolence. What options currently exist to deal with IP theft from a technology perspective? Broadly speaking, the existing technology seeks to protect a firm's security footing in order to mitigate cybertheft by potential malevolent actors (e.g., ransomware attacks), safeguard proprietary information, and identify when a breach has occurred. These three areas are discussed in this section.

Cybersecurity Protections

According to a report from Deloitte, "compared with more familiar cybercrimes such as the theft of credit card, consumer health, and other personally identifiable information…. IP cyber theft has largely remained in the shadows."[26] A concerning thought, but a practical reality, is that IP is the largest asset for most companies, and it may be the most vulnerable. The distributed nature of work and recent trends in the work-from-home landscape have exacerbated the challenges associated with cybertheft of IP. Thus, in order for any digital asset to be secured across a firm's extended enterprise (including its IP), a comprehensive cybersecurity protocol must be implemented. Currently, the following is recommended:

- *Enable encryption, where possible, such that in the event of a cyberattack the IP is harder to access*. This would add a layer of friction that can reduce the likelihood of IP theft and leakage.
- *Establish a dual-factor authentication system to access proprietary information*. This would serve a dual-faceted purpose by adding a layer of access protection and increasing governance (i.e., access protocol) around who can view potentially confidential information.
- *Perform stress tests and employee training around cybersecurity*. As the human factor was seen as one of the most critical vulnerabilities in IP, such investments in training should help mitigate IP theft.
- *Assess the scope and location of all IP throughout the extended enterprise and develop a counterintelligence footing, anticipating the threat and preparing the response*.[27] Coupled with the training noted above, this measure provides transparency around what IP exists (and where it exists) and also establishes an organizational culture around protecting IP.
- *Practice cyber hygiene by applying the National Institute of Standards and Technology framework to identify vulnerable digital assets; protect, where possible, against vulnerabilities; and detect and respond to incidents quickly and comprehensively*.[28] Such measures would establish a sound mitigation protocol that can reduce the potential damages associated with a breach.

Blockchain Technology

As of late, supply chains and blockchain have made quite the alliance, with recent reports predicting the "post-COVID-19 blockchain supply chain market to grow from USD 253 million in

[26] "The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property."

[27] Alyson Behr and Derek Slater, "Intellectual Property Protection: 10 Tips to Keep IP Safe," CSO, August 24, 2021, https://www.csoonline.com/article/2138380/intellectual-property-protection-10-tips-to-keep-ip-safe.html.

[28] The National Institute of Standards and Technology framework is available at https://www.nist.gov/cyberframework.

2020 to USD 3,272 million by 2026, at a Compound Annual Growth Rate (CAGR) of 53.2% during 2020–2026."[29] While not specific to IP per se, blockchain technology can be useful to IP in many ways. Effectively, the value of blockchain technology is in its design: it is a distributed ledger that records entries and transactions in such a way that they are resistant to fraud, as the preceding transactions are immutable, and all subsequent transactions are recorded in the ledger.[30] This technology allows for a certain degree of anonymity through the use of hashing and cryptography so as to anonymize the entry, theoretically facilitating a heightened degree of information sharing by hiding identifying information. Blockchain technology also allows for the use of so-called smart contracts, which are self-governing, and recording contracts that record all relevant legal information in an immutable way.

These ideas have recently made their way into Covid-19 vaccine development. Vaccines are becoming a desirable target for IP theft, and IBM and Moderna have partnered to explore the efficacy of blockchain and related tools to secure the vaccine supply chain and increase visibility and traceability. Currently, the "goal of the partnership is to identify ways technology can be used to boost secure information sharing between government agencies, healthcare providers, life science organizations, and individuals."[31] Initially, the project sought to track and trace the supply chain to identify potential supply shortages, but it has evolved to provide transparency around vaccine administration and related health information. If implemented properly, the technology can engender a crowdsourced verifiability of authenticity.

Of course, the popular press is replete with examples of blockchain technology being applied to cryptocurrencies and in other related contexts, but the real potential is in its traceability. Consider an example of verifying the authenticity of a copyrighted or patented product whose IP is vital to its owner. Let's assume that the product is sold on a popular platform where third parties can join and sell products. Blockchain technology can be used as a mechanism where the owner logs the ownership and relevant details of the product on the blockchain, then the platform (or consumer) can subsequently check the current product against the information on the blockchain so as to verify its authenticity. Recent hype has been placed on using non-fungible tokens,[32] which "are 'one-of-a-kind' assets in the digital world that can be bought and sold like any other piece of property, but which have no tangible form of their own."[33] Generally, the "non-fungibility" refers to their inability to be exchanged for one another (in contrast to, for example, exchanging one $10 bill for ten $1 bills). This lack of fungibility is driven by an individual and unique digital signature that is housed/powered by the Ethereum blockchain.[34] In this scenario, the blockchain serves as a potential tool to authenticate the product and theoretically protect the IP of the owner. Recent patents have been issued, in fact, that allow for name authentication and

---

[29] Research and Markets, "Global Blockchain Supply Chain Market by Offering (Platform, Services), Type (Public, Private, Hybrid & Consortium), Provider, Application (Asset Tracking, Smart Contracts), Enterprise Size, Vertical (FMGC, Healthcare), and Region—Forecast to 2026," March 2021, https://www.researchandmarkets.com/reports/5304951/global-blockchain-supply-chain-market-by-offering.

[30] Tarun Kumar Agrawal et al., "Blockchain-Based Framework for Supply Chain Traceability: A Case Example of Textile and Clothing Industry," *Computers and Industrial Engineering* 154, no. 6 (2021).

[31] Samantha McGrail, "IBM, Moderna Explore AI, Blockchain for COVID-19 Vaccine Management," HITInfrastructure, March 9, 2021, https://hitinfrastructure.com/news/ibm-moderna-explore-ai-blockchain-for-covid-19-vaccine-management.

[32] Nikhilesh De, "State of Crypto: It's Time to Talk about NFTs and Intellectual Property Law," CoinDesk, March 9, 2021, https://www.coindesk.com/nfts-legal-questions.

[33] "What Are NFTs and Why Are Some Worth Millions?" BBC, September 23, 2021, https://www.bbc.com/news/technology-56371912.

[34] Robyn Conti and John Schmidt, "What You Need to Know about Non-Fungible Tokens (NFTs)," *Forbes*, May 14, 2021, https://www.forbes.com/advisor/investing/nft-non-fungible-token.

legal responsibility mechanisms through blockchain.[35] But not all jurisdictions allow blockchain as proof of ownership.

Other potential uses of blockchain in IP enforcement include smart contracts to govern ownership and precedence of discovery, authentication of IP, ownership transfer and record keeping, and evidentiary claims of ownership and use authorization. For more detail on blockchain and its current utilization in modern supply chains, see **Appendix 2**.

Artificial Intelligence

Artificial intelligence (AI) refers to computerized attempts to model, emulate, and perform human (or biological) intelligence. WIPO defines AI as "a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention."[36] Applications are vast. AI has been used to detect illicit behavior ranging from fraudulent purchases to national security threats, as well as for facial recognition and even in logistics to monitor and track delivery driver behavior.

In the context of IP, significant attention has been paid to AI recently. Legal questions over ownership of AI-generated inventions, the way in which AI should be protected, and so on have stimulated a passionate and ongoing debate. The core of the arguments rests on the antecedent of the "creation," given that the AI that is driving the innovation is being programmed by humans. As a tool for IP protection, however, AI can be useful. Recently, it has been utilized in compliance management, providing more accurate real-time information so that decision-makers are operating more efficiently. AI has also been used to provide proof of origin, product tracking, and authentication by augmenting the hashing and cryptography algorithms so that they can be applied more broadly to other IP such as video, images, and audio. Generally speaking, leveraging the power of modern computing to automate compliance tasks can significantly increase throughput and improve overall fraud detection. This, coupled with the power and traceability of blockchain, is likely to be a game changer with respect to IP protections. For more detail on AI and its integration into modern supply chains, see **Appendix 3**.

From the Current to the Future State

What Are the Current Gaps, and What Should Be Done?

Recent data from the Organisation for Economic Co-operation and Development (OECD) suggests that trade in counterfeit goods represents approximately 3.3% of world trade, with the United States being the country most affected.[37] This is a particularly concerning issue amid the escalating frequency and cost of cyber breaches targeting firms' IP. The current state is precarious.

The questions of where the gaps are and what should be done can be answered in one word: cohesion. There are piecemeal solutions to every problem addressed in this report. For example, consider the traceability problem with raw materials in the sourcing of coffee beans. Blockchain

---

35 "Future FinTech Granted Blockchain Technology-Related Software Copyrights from the China National Copyright Administration," PR Newswire, March 4, 2021, https://www.prnewswire.com/news-releases/future-fintech-granted-blockchain-technology-related-software-copyrights-from-the-china-national-copyright-administration-301240690.html.

36 WIPO, "WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI)," May 21, 2020, https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf.

37 "Trade in Fake Goods Is Now 3.3% of World Trade and Rising," OECD, March 18, 2019, https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm.

is a possible solution to ensure traceability of the coffee bean from farm to cup and everywhere in between. Yet, who will bear the cost? The family farmer located in a developing country? The logistics firm tasked with moving the raw coffee beans from farm to market? The brand that ultimately will sell the roasted, ground, or brewed coffee beans? What about the question of responsibility for counterfeit goods being sold on an e-commerce platform? Of course, if resources were not an issue the platform could deploy AI-driven technology to weed out such products before they are sold, ban the seller from the platform, and remediate the concerns of the consumer. Clearly, this is not the case.

The anecdotal examples above illustrate the reason that cohesion—the development of a cohesive strategy for tackling IP theft—is such a challenge. It is not that there is a lack of possible protections. The real challenge is how to tie them together, when to use which approach, and who will bear the cost. Our experts identified this problem of agency as well. Their recommendations are distilled in the following subsection.

Key Recommendations for How to Protect IP in Supply Chains

The findings of the report and the interviews with industry experts provided for a broad swath of recommendations across all areas of the supply chain, from sourcing to outbound logistics. The common theme that was mentioned, regardless of a person's location or position in the supply chain, was the critical role that the human factor plays in IP infringement in supply chains. This led to one overarching and critical recommendation.

Training. One of the experts with whom we spoke said it best: "Training personnel for what to look out for in the supply chain is essential. The soft skills become critical." Increased interconnectedness and dependence between firms upstream and downstream in the supply chain means that vulnerabilities around IP leakages are increasingly heightened. Thus, training employees to correctly handle and protect IP is no longer optional; it is necessary. Supply chain personnel need to understand what IP is, where the vulnerabilities are, where IP resides, how to protect it, and what the cost of a breach is. Currently, supply chain personnel are largely unaware stakeholders in the governance of IP protections. This passive inattention to IP likely arises from the fact that its protection is normally entrusted to a legal department. Yet, as has been outlined in this report, multiple parties (many of whom function squarely within traditional supply chain domains) should have responsibility over its protection. This needs to change to a more proactive, awareness-focused approach. In the technologically focused world in which supply chains are entrenched, malevolent actors have more touch points, more unique attack vectors, and more opportunities than ever before. The entities operating in the supply chain are the first lines of defense for securing the intellectual capital and property of organizations.

A "detection, mitigation, and recovery" approach. Experts from various industries identified two crucial gaps that cause IP vulnerabilities in the sourcing space: the first is the lack of traceability, and the second is the influx of counterfeit goods entering the supply chain. One of the experts commented about traceability: "There is certainly no standardization. A uniform system that everyone can jump on is the largest gap…. An International Standardization Organization (ISO) of some version is necessary. Presently, the fragmentation in what is available to protect IP causes vulnerabilities." Thus, the largest opportunity to increase security in the supply chain with respect to IP is to establish a cross-functional regulatory body that governs and maintains standards for IP protections between companies similar to the way that International Commercial Terms function

as a tool through which trade terms are negotiated. Currently there are some initiatives that seek to enhance the traceability of various components, as well as agencies that seek to verify or certify the authenticity of inputs and raw materials, but the lack of an industry-wide standard has in many ways constrained the ability of procurement personnel to ensure that the products being acquired are authentic. This causes potential problems related to liability, warranty expenses, brand harm, and so on.

Creating a common standard or certifying organization could be achieved in multiple ways. First, a protocol around what constitutes IP protections in the supply chain needs to be established, possibly modeled on the National Institute of Standards and Technology's cybersecurity protocol. Industry organizations such as the Association for Supply Chain Management (ASCM) or the Council of Supply Chain Management Professionals (CSCMP) could define, adopt, and subsequently champion these standards, which would explicitly detail the process for onboarding suppliers and vetting them through the lens of IP protections, data handling, and cybersecurity, among other criteria. Firms then could communicate to prospective suppliers that this is the minimum standard for doing business with them. Alongside these standards, an incentive structure with a recognized award for excellence in IP protections at multiple tiers in the supply chain (i.e., suppliers, suppliers of suppliers, and so on), such as the Malcolm Baldridge Award in the total quality management space, is one tool to motivate firms to comply with and champion such standards. This would effectively function as a response to the suggestion of an "IP-driven ISO organization" from the respondent quoted above.

The issues associated with IP theft and infringement in manufacturing largely concern liability. From a sourcing standpoint, the key issues center on traceability and counterfeit goods. That is, a lack of visibility into the beginning of the supply chain can lead to several issues downstream in the supply chain. Additionally, the three issues associated with IP infringement and manufacturing relate to brand image, product quality, and data security. The brand image concerns relate to the liability of product failures or consumer harm or to the loss of business associated with inadvertently selling a counterfeit product. Alternatively, on the manufacturing/product side of the supply chain, the risk to the brand name arises as a result of quality issues. Finally, in the logistics space the key mechanism to hedge against the threat of IP infringement is to ensure data security. Logistics networks are guardians of product security, but they are under constant threat of malicious attack.

In all cases and functions of the supply chain, protecting IP boils down to risk management. One of the experts who provided feedback responded that "IP compliance is risk mitigation, and this is a necessary component," while another suggested that "there needs to be proper risk management and risk assessment that is focused on IP protection." Generally speaking, there are three categories into which such strategy falls: (1) detection, (2) mitigation, and (3) recovery.[38] Across all functions of the supply chain, the following recommendations are advanced.

Detection starts at the source, and as such the sourcing function acts as the gatekeeper for preventing fraudulent/subpar products from entering the production process. The following measures are needed to strengthen detection:

- *Make IP a priority during the supplier selection process by including key metrics and stage gates around potential traceability protocols, fraud detection, or other IP protections in the selection*

[38] Scott DuHadway, Steven Carnovale, and Benjamin Hazen, "Understanding Risk Management for Intentional Supply Chain Disruptions: Risk Detection, Risk Mitigation, and Risk Recovery," *Annals of Operations Research* 283, no. 1 (2019): 179–98.

of suppliers. These protocols need to be explicitly laid out in the evaluation criteria in the request for proposals and adopted as firm policy.

- *Implement supplier scorecards that include a measure of "IP defense" to secure IP in future transactions*. This would ideally be a multidimensional measurement of data-handling practices (e.g., cyber hygiene, multi-factor authentication and access protocols, and password requirements) and training about what IP is and who is responsible for its protection, among other factors. This would also signal to the potential supplier that IP protections are front and center, and not an ancillary issue.
- *Leverage and implement AI and other computerized technology to detect fraudulent products and materials where possible*. This is particularly important if electronic procurement on platform sites or digital reverse auctions are being used to acquire materials. From the standpoint of protecting a brand image, detecting and removing fraudulent products is key, particularly as it relates to platform sales.
- *Increase information sharing as a formal requirement of partnering with a firm*. Just as collaborative planning, forecasting, and replenishment is implemented between supply chain partners to increase information sharing between entities for the purposes of production planning and sales forecasting, so too can information sharing around IP handling and governance increase between entities collaborating in the supply chain. This could be facilitated in numerous ways. An industry organization (e.g., CSCMP or ASCM) could champion processes for IP protection and the requisite information and transparency that is needed for a firm to be "IP certified." One of our experts noted that a huge problem in detecting IP infringement is the "lack of visibility and transparency, with no data being passed on from one entity to the other. Sharing data does not happen as much as it should, and as a result vulnerabilities arise."
- *Integrate systems to help improve information sharing*. The current patchwork of systems, technologies, and processes that are operating disparately renders supply chains vulnerable to IP infringement and theft. There are several ways to hedge against the potential downside of inconsistent and disjointed systems. Aligning with the previous recommendation of establishing standards, one of the critical standards should be compatibility between entities' information systems. Take, for example, the way in which a program written in the programming language Python can be utilized on both Windows and macOS operating systems. In a similar manner, information shared regarding IP or the systems tasked with protecting IP between entities should also be compatible. This would reduce the friction between entities and thereby reduce the risk to IP protections.

Mitigation activities assume (rightfully so) that IP infringement will likely occur and plan for the best ways to manage the fallout. First, enhanced enterprise-wide data security is critical for reducing IP leakage. This was a common and strongly held view in all the interviews conducted with experts, and several problems were identified. Schematics on the production and sourcing side are vulnerable. Product routing and shipping details are accessible via IoT devices in freight, and therefore susceptible to outside attacks. For example, employees' email accounts that are accessible via their phones or tablets open up entirely new attack vectors. This is not anecdotal, as recent reports indicate that over 50% of IP breaches are achieved through email.[39] Thus, recommendations for achieving data security are (fortunately) largely congruent with several known cybersecurity recommendations:

[39] Egress, "Data Privacy in 2019 Research Report," 2019, https://pages.egress.com/2019-Data-Privacy-research.html.

- *Catalog what data is being stored and who has access to it and establish a mechanism for tracking when such data has been accessed*. Such policies typically have multiple layers of access, ranging from "read-only" all the way to "full" access where the user can edit, copy, and otherwise manipulate data.
- *Maintain a register for data*. While it might seem obvious, this is a crucial first step in protecting data. A nondigital analogue would be a vault at a bank that maintains strict standards with respect to access and a detailed inventory of its contents.
- *Maintain redundant cloud and physical backups of key data*. This could be a 2 to 1 ratio of physical to digital (i.e., cloud) backups, ideally where the physical backups are not geographically co-located.
- *Leverage encryption wherever possible*. This enables a layer of security such that should data be inappropriately accessed, it is extremely difficult, if not impossible, to read.

Another important set of recommendations focus on augmenting the supplier onboarding process to include specific cybersecurity requirements to safeguard data and other proprietary information. This will hedge against (though, of course, not eliminate) malevolent actors being able to easily acquire IP via a firm's supply base. Specifically, firms should implement the following measures:

- *Take the internal data security recommendations noted above and evaluate the degree to which suppliers are adhering to them, or the degree to which they maintain their own standards that are congruent with internal data security standards*.
- *Include specific IP considerations, such as IP information governance policies (i.e., data security), access and use policies (particularly when IP is not being accessed at the focal firm's facilities but rather at an offsite location), security protocols around background checks to gain access to IP, and storage*. Penalties for violating IP handling requirements should be explicitly stated and documented, in addition to processes for handling fraudulent, nongenuine, or otherwise subpar products received at a firm.
- *Evaluate and enumerate the potential damages of IP theft, both financially and reputationally, and prepare a disaster-response plan on how to approach it*. This disaster-response plan should be structured in such a way that all possible scenarios are listed out and a prescriptive response is provided. It should also be organized in a tiered fashion. That is, tier 1 incidents could be considered low risk, tier 5 incidents could be considered high risk, and tier 2, 3, and 4 incidents would correspond to escalating levels of risk. Then, to the degree possible, all incidents should be enumerated and subsequently classified.[40]
- *Establish a coherent legal strategy for remediation that includes a cross-functional team*.
- *Acquire cybersecurity policies*. In the procurement phase of such policies, firms should ensure that contingencies for IP are included or that other liability/insurance policies have exposure to IP in some way.

[40] For example, let's assume that a supplier has access to a firm's systems and their access has been governed by its information security policy. Then, as result of a routine audit of the IP data access and use policy, the firm notices that this particular supplier has accessed a section of its system that contains proprietary data and to which it did not have access. The impact is unknown, as the firm only reveals that the data was accessed. If the incident falls into a tier-3 incident, relevant protocols should immediately be enacted. These may include revoking access, sending formal notice, and identifying and contacting redundant suppliers (if applicable, and of course available). The specific protocols for responding and into which tier a particular incident falls are entirely dependent on the firm. Having an explicit disaster-response plan, however, signals to those with whom the firm does business that IP is a top strategic priority.

Finally, the goal of a recovery plan is to return to a pre-disruption state. As such, recovery strategies are needed to chart a path forward after an attack. The following measures would help facilitate recovery:

- *Use redundant suppliers and diverse sourcing strategies*. This measure allows firms to shift suppliers if one has allowed fraudulent or subpar products into the supply chain.
- *Establish backup systems and other contingency plans to move forward*.
- *Execute the legal strategy outlined above and develop plans to communicate with the affected parties (e.g., suppliers and customers)*.
- *Commit to continuous improvement*. After an attack, firms must learn from what happened and close the gap to prevent the issue from occurring again.

Conclusion

As this report has shown, supply chains are highly vulnerable to IP theft. The length and complexity, the number of firms, the number of countries, and the number of products that modern supply chains are tasked with sourcing, manufacturing, and ultimately delivering to consumers have grown exponentially over the past several decades. Regional supply chains have transformed into global ones with IP and related proprietary information being dispersed across firms' extended enterprises. Couple this with the increase in digitization and the greater presence of internet-enabled technologies, and the number of attack vectors for malevolent actors has outpaced potential protections and safeguards.

Unfortunately, there is no part of the supply chain that is unaffected by these threats. Sourcing must focus on quality by training personnel on what to look for and how important traceability is to ensure compliance with quality standards and authenticity. Manufacturing must act as a backstop on sourcing to ensure that subpar or inauthentic materials do not enter into the production process, potentially causing quality failures at later stages of the supply chain. Outbound logistics should buttress data security in a meaningful way to protect against external interference in the IP contained in shipments. In sum, a cohesive, coordinated approach is essential to ensure that IP is protected to the highest degree possible.

APPENDIX 1: THE GLOBAL LANDSCAPE FOR U.S. INTELLECTUAL PROPERTY

Jessica Carnovale

This appendix focuses on the intellectual property (IP) protection issues that U.S. companies face when conducting business in six Asian countries: China, India, Indonesia, Malaysia, Thailand, and Vietnam. These countries were chosen due to their prominence in the global supply chain. The laws surrounding a company's ability to obtain, maintain, and enforce legal protections vary widely between countries. Organizations like the World Trade Organization (WTO) help promote trade by setting minimum standards for member countries and settling disputes between them. Take, for example, the WTO-created Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which is a legal agreement accepted by all WTO members. All six countries discussed in this appendix are WTO members.

Given the importance of IP rules to the global economy and the wide variance in countries' IP protections, a number of institutions, organizations, and reports exist to monitor the state of IP protections in all member countries and help identify their strengths and weaknesses.

- *World Intellectual Property Organization (WIPO)*. WIPO was created to work with its member countries to develop treaties to create an international standard of regulations and oversee IP protection globally to promote innovation and creativity.
- *Agreement on Trade-Related Aspects of Intellectual Property Rights*. The TRIPS Agreement is a multilateral international legal agreement that sets minimum standards of IP protection.
- *Special 301 Report*. This congressionally mandated report under the Trade Act of 1974 investigates and monitors countries that do not enforce adequate IP protection within their acts, policies, or practices to protect U.S. products or services.[1] Problem countries are placed either on the Priority Watch List, which comprises countries that are found to have severe issues within their IP practices and need to be closely monitored, or the Watch List, which comprises countries whose IP issues are not so serious that the United States needs to closely monitor them. The report also outlines an action plan for countries that have been on the Priority Watch List for at least a year. If the foreign country does not implement corrective action to rectify the issue, the U.S. Trade Representative (USTR) can file a dispute with the WTO for further action.
- *International Property Rights Index (IPRI)*. The IPRI is compiled by the Property Rights Alliance, which scores the physical and IP rights of 129 countries on a scale of 0 to 10, with 10 being the best.[2] To score each country, this report looks at three main components: legal and political environment, physical property rights, and IP rights. Each of these components is then broken into a total of ten subcomponents. The data is collected from tenured international organizations that publicly share their findings (e.g., the World Bank). A country's overall score is the average of subcomponents for each of the main three components. The final IPRI score is the average of the main components.

[1] The most recent Special 301 Report is available from the U.S. Trade Representative at https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf.

[2] The 2020 and 2019 International Property Rights Index reports are available from the Property Rights Alliance at https://www.internationalpropertyrightsindex.org.

China, India, Indonesia, Thailand, and Vietnam are on watch lists created and monitored by the USTR. According to the annual Special 301 Report, a particularly vulnerable area for IP in these countries is adequate enforcement at the border (i.e., concerns related to sourcing and logistics). In particular, customs officials lack authority to seize and destroy counterfeit goods. China and India were also found to be among the top countries of origin for counterfeit goods according to a report published in 2019 by the Organisation for Economic Co-operation and Development (OECD).[3] However, this report is based on figures from 2016.

IPRI Averages and Comparisons

This appendix compares the 2019 and 2020 IPRI averages for China, India, Indonesia, Malaysia, Thailand, and Vietnam. These averages are based on a four-year moving average. The data for the 2019 report averages from 2015 to 2019 and the 2020 report from 2016 to 2020.[4] For reference, **Figure 1** provides the global averages of the scores for all 129 countries studied in both the 2019 and 2020 reports.

FIGURE 1 Global IPRI average, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	5.729	5.160	6.474	5.553
2020	5.728	5.140	5.500	5.545

China's IP landscape. China's overall IPRI ratings are above the global averages for both 2019 and 2020 (see **Figure 2**). Although this indicates that China's IP protections exceed average global levels of protection, it should be noted that the country's overall score is far below other major economies, such as Germany (7.741), Japan (8.362), and the group of OECD countries (7.2428).

FIGURE 2 China's IPRI rankings, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	6.033	4.930	7.148	6.021
2020	6.045	4.965	7.149	6.022

[3] "Trade in Fake Goods Is Now 3.3% of World Trade and Rising," OECD, March 18, 2019, https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm.

[4] As noted above, the 2020 and 2019 IPRI reports are available at https://www.internationalpropertyrightsindex.org.

Indeed, China's score ranks only slightly above the average score of Association of Southeast Asian Nations (ASEAN) countries (5.8944)—a group that is still working to develop more meaningful IP laws and institutions.[5] Specifically, the U.S.-China Business Council notes that while strides in the right direction have been made, "challenges remain, including lingering issues with China's IP legal framework in areas such as trade secrets, uneven enforcement, and significant procedural barriers that frustrate company efforts to protect IP in China." It further observes that "counterfeiters and infringers in China are increasingly sophisticated" and "often exploit procedural loopholes, proactively seek to invalidate legitimate patents and trademarks, deploy advanced techniques such as reverse engineering, and find new ways to infiltrate legitimate distribution networks and build their own parallel networks."[6] The USTR has also initiated dispute-settlement proceedings at the WTO to address discriminatory licensing practices. According to the Special 301 Report, China's largest vulnerabilities are trade secrets, counterfeiting, forced technology transfers, and lack of transparency in litigation.

The USTR's Priority Watch List observes the following about China's IP landscape:

- "USTR continues to place China on the Priority Watch List and Section 306 monitoring remains in effect… [This] reflects U.S. concerns with China's system of pressuring and coercing technology transfer, and the continued need for fundamental structural changes to strengthen IP protection and enforcement, including as to trade secret theft, obstacles to protecting trademarks, online piracy and counterfeiting, the high-volume manufacturing and export of counterfeit goods, and impediments to pharmaceutical innovation…. USTR has taken action to address a range of unfair and harmful Chinese acts, policies, and practices related to technology transfer, IP, and innovation."
- "Structural impediments to administrative, civil, and criminal enforcement continue to undermine IP protections, as do certain information communications technology (ICT), IP-ownership, and research and development localization requirements."
- "Over the past year, the United States' engagement of China began to demonstrate key progress with the signing of the U.S.-China Economic and Trade Agreement in January 2020. The agreement requires changes in China's acts, policies, and practices, including structural reforms and other changes to China's legal and regulatory regime to address numerous longstanding concerns of a wide range of U.S. industries."

India's IP landscape. India's overall IPRI ratings in 2019 are above the global average, though it scores lower in the legal and political environment. However, its overall rating dropped below the global average in 2020 due to lower scores across all three categories (see **Figure 3**). According to the Special 301 Report, India's largest vulnerabilities are difficulty receiving, maintaining, and enforcing patents (particularly for pharmaceuticals); weak and outdated laws to protect trade secrets; and high levels of trademark counterfeiting. India does not have a centralized IP enforcement agency to help protect against infringement. Patents are hard to acquire and keep because they are costly, time-consuming, and require excessive reporting, and the legal enforcement to protect trade secrets is weak. Copyrights suffer from high levels of piracy, unauthorized file sharing on video games, commercial scale photocopying, and reprints of academic books.

The USTR's Priority Watch List observes the following about India's IP landscape:

---

[5] Peter N. Fowler, "Intellectual Property Challenges in the ASEAN Region," National Bureau of Asian Research, NBR Commentary, July 1, 2021.

[6] U.S.-China Business Council, "Best Practices: Intellectual Property Protection in China," 2015, https://www.uschina.org/reports/best-practices-intellectual-property-protection-china.

FIGURE 3 India's IPRI rankings, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	5.820	4.876	6.608	5.974
2020	5.708	4.718	6.520	5.886

- "IP challenges facing U.S. businesses in India include those which make it difficult for innovators to receive, maintain, and enforce patents in India, particularly for pharmaceuticals; ineffectual enforcement activities, copyright policies that fail to incentivize the creation and commercialization of content, and an outdated and insufficient trade secrets legal framework."
- "India also further restricted the transparency of information provided on state-issued pharmaceutical manufacturing licenses, continues to apply restrictive patentability criteria to reject pharmaceutical patents, and still has not established an effective system for protecting against the unfair commercial use, as well as the unauthorized disclosure, of undisclosed test or other data generated to obtain marketing approval for pharmaceuticals and certain agricultural chemical products."

Indonesia's IP landscape. Indonesia's IPRI rankings are below the global average in all categories except physical property rights (see **Figure 4**). Its lack of enforcement with counterfeiters leaves IP owners vulnerable to infringement. The United States also has concerns about Indonesia's patent law with regard to patentability for incremental innovations and procedures for using compulsory licenses along with market access barriers. The United States further takes issue with the absence of an effective system to safeguard IP against unfair commercial use. According to the Special 301 Report, Indonesia's largest vulnerabilities are patentability criteria and compulsory licensing, weak IP enforcement, and market access restrictions for IP-intensive industries.

The USTR's Priority Watch List observes the following about Indonesia's IP landscape:

- "U.S. right holders continue to face challenges in Indonesia with respect to adequate and effective intellectual property protection and enforcement, as well as fair and equitable market access. Concerns include widespread piracy and counterfeiting and, in particular, the lack of enforcement against dangerous counterfeit products."

FIGURE 4 Indonesia's IPRI rankings, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	5.405	4.737	7.065	4.414
2020	5.341	4.644	6.990	4.389

Malaysia's IP landscape. Malaysia's IPRI rankings are above the global average (see **Figure 5**), and the country is not currently on either USTR watch list. This shows that Malaysia has strong IP laws and enforcement compared to the global average. According to the Special 301 Report, its largest vulnerabilities are market access barriers and trade secret theft due to procurement regulations that require companies to disclose source code. Malaysia is a member of numerous international agreements and has many domestic laws to protect and govern IP. The Intellectual Property Corporation of Malaysia (MyIPO) oversees and administers the country's IP system. As a member of both the WTO and WIPO, Malaysia follows the IP standards established by the TRIPS Agreement. Malaysia is also a part of both the Patent Cooperation Treaty and the Madrid Protocol. Companies seeking to obtain a patent or trademark can apply through MyIPO. Trademarks are valid for ten years from the date of application and can be renewed every ten years. Copyrights can be registered by filing a copyright voluntary notification with MyIPO but are protected without registration. Patents are governed by the Patents Act of 1983 and the Patents Regulations of 1986 and last fifteen years after the date they are granted.

FIGURE 5 Malaysia's IPRI rankings, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	6.623	5.817	7.814	6.239
2020	6.717	6.157	7.771	6.223

Thailand's IP landscape. Thailand's IPRI rankings are below the global average (see **Figure 6**). However, the country is working toward joining both the WIPO Internet Treaties and the Hague Agreement, which has forced its government to make strong efforts toward improving enforcement of IP rights. According to the Special 301 Report, Thailand's largest vulnerabilities are order enforcement, online piracy, counterfeiting, and unfair commercial use. Thailand does not practice strict border enforcement when it comes to counterfeit and pirated goods. The United States recommends that U.S. IP owners obtain IP protections in Thailand before introducing their products into the Thai market. This protection is useful as it gives the IP proof of ownership in the event of a legal dispute.

FIGURE 6 Thailand's IPRI rankings, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	5.455	4.618	6.981	4.766
2020	5.474	4.585	7.045	4.793

Thailand is currently on the USTR's Watch List. However, this is an improvement, given that in 2016 it was on the Priority Watch List. The USTR's Watch List observes the following about Thailand's IP landscape:

- "Counterfeit and pirated goods continue to be readily available, both in physical markets and online, and the United States urges Thailand to continue to improve on its provision of effective and deterrent enforcement measures. In addition, the United States remains concerned about a range of copyright-related issues."
- "The United States urges Thailand to amend its Copyright Act to address concerns expressed by the United States and other foreign governments and stakeholders, including regarding overly broad technological protection measure exceptions, procedural obstacles to enforcement against unauthorized camcording, and unauthorized collective management organizations."

Vietnam's IP landscape. Vietnam is ranked lower than the IPRI global average in both 2019 and 2020 (see **Figure 7**). Vietnam is currently working toward strengthening its IP protection, but the USTR finds a lack of coordination in enforcing existing laws, which is partly due to lack of resources and training. According to the Special 301 Report, Vietnam's largest vulnerabilities are counterfeiting, border enforcement, and online and broadcast piracy, which remain challenging due to weak enforcement.

FIGURE 7 Vietnam's IPRI rankings, 2019 and 2020

	Overall	Legal and political environment	Physical property rights	Intellectual property rights
2019	5.084	4.742	5.956	4.555
2020	5.132	4.736	6.030	4.631

The USTR's Watch List observes the following about Vietnam's IP landscape:

- "IP enforcement continues to be a challenge and the online sale of pirated and counterfeit goods remains a serious problem. Lack of coordination among ministries and agencies responsible for enforcement remains concerning, and capacity constraints related to enforcement persist, in part due to a lack of resources and IP expertise."
- "Counterfeit goods remain widely available in physical markets…online piracy, including the use of piracy devices and applications to access unauthorized audiovisual content, book piracy, and cable and satellite signal theft persist, while both private and public sector software piracy remains a concern."

Jessica Carnovale is an Adjunct Professor of Supply Chain Management in the Saunders College of Business at the Rochester Institute of Technology. She can be reached at <jcarnovale@saunders.rit.edu>.

APPENDIX 2: BLOCKCHAINS IN SUPPLY CHAINS

Samir Dani

Blockchain technology has gathered tremendous interest within industry sectors in recent times. The proliferation of startups and the pilot projects initiated by several large companies for their operational processes has fueled increased interest in academic and professional circles, too. Although the initial technology and concept were primarily focused on cryptocurrency, blockchain is rapidly moving to become a transaction platform for operational environments.

One domain in which this technology found early recognition is supply chains. The current focus is on supply chain provenance, but the industry is also moving toward tokenization and financing throughout the supply chain. Tokens have been defined as "digital representations of an asset or utility that are typically built on top of existing blockchains."[1] Tokens are cryptocurrency or cryptoassets and are sometimes referred to as any cryptocurrency except Bitcoin and Ethereum. Some examples of tokens are DeFi tokens (cryptocurrency-based protocols that work similar to traditional finance processes such as lending, saving, insurance, and trading), governance tokens (specialized DeFi tokens that provide the holder control over the future of a protocol or app), non-fungible tokens (tokens that provide ownership rights to a unique digital or real-world asset), and security tokens (cryptoassets that represent traditional securities like stocks and bonds).[2]

What Is a Blockchain?

A blockchain is defined as a "secure distributed ledger which can store and exchange value without the need for traditional intermediaries."[3] A distributed ledger is defined as a "technological architecture designed for the clearing and settlement of digital asset trading and distributed computing without having the need for central intermediaries."[4] Satoshi Nakamoto developed the cryptocurrency platform that became Bitcoin in 2008, and the distributed ledger was the tool within this platform that recorded the transactions. One of the tenets of the distributed ledger within this environment is the decentralized approach to recording transactions using the public space. The decentralization and distributed nature, along with the permanent nature of the record, provide trust among the platform members. The platform provides immutable, transparent, and permanent transaction records. The blockchain differs from a relational database on account of its decentralized character and how data is viewed and stored. Trust is built into the system on account of the transactions being verified by the members of the blockchain.

The following specific steps are involved in conducting transactions in the blockchain:

- The transaction is initiated in the blockchain.
- The transaction is represented as a block for delivery to the blockchain members.

---

[1] David Uzsoki and Patrick Guerdat, "Impact Tokens: A Blockchain-Based Solution for Impact Investing," International Institute for Sustainable Development, April 2019, https://www.iisd.org/system/files/publications/impact-tokens.pdf.

[2] Ibid., 2.

[3] Chang Yanling, Iakovou Eleftherios, and Shi Weidong, "Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities," *International Journal of Production Research* 58, no. 7 (2020): 2082–99.

[4] Peter Yeoh, "Regulatory Issues in Blockchain Technology," *Journal of Financial Regulation and Compliance* 25, no. 2 (2017): 196–208.

- The transaction block is transmitted to all parties in the blockchain network, which functions as a peer-to-peer network with each member acting as a node.
- The transactions in a block are verified by the nodes using a computer algorithm providing a unique identification string known as a hash, which ensures the integrity of the block.
- The verified block is added to the blockchain. Each new block added to the blockchain has the hash of the previous block and the new verification hash for the block. Blocks connected to each other through the hashes form the immutable chain.

The immutability of the blockchain is derived through the unique hash. If someone tampers with the data in the block, it will create a new hash for the block. However, this will not coincide with the hash in the adjoining block, thus identifying the breach.

Characteristics of Blockchain Environments

Blockchain environments typically fall into two categories: public blockchain and private blockchain. The major differences between the two are related to who participates and whether they require permission to transact in the blockchain. A public blockchain is "permissionless," which means that anyone can join the network and participate in the transactions (which includes mining and verifying). This provides complete decentralization and anonymity. The private blockchain is a "permissioned" network, which means that only those entities who have the permission to participate in the transactions can join the network. Some blockchains, such as the Ethereum platform, provide both public (Ethereum) and private (Ethereum Alliance) blockchains. In networks where it is essential to know who is participating before any intellectual property (IP), confidential information, or other assets are shared, a private blockchain environment is used.

Both public and private blockchains use consensus mechanisms and instill trust in the network, but the incentives for both systems are different. Within the private blockchain, the network entities will verify the transactions through consensus and hashing. However, the public blockchain entities who are anonymous need to be incentivized (for instance, by providing them with cryptocurrency) to fulfill the mining and hashing mechanisms through consensus for verifying the transaction and creating blocks. Incentivization builds trust in the permissionless public blockchain.

Another important differentiation within blockchain environments is the consensus mechanisms for validating the transactions and creating the blocks. The proof of work is the mechanism normally used by permissionless public blockchains. In this mechanism, network nodes (also called miners) will solve complex algorithms to validate the blocks and in turn will receive cryptocurrency units as a reward. However, this process consumes a vast amount of energy and is responsible for high CO_2 emissions. The miners need to use their coins to pay toward the mining costs. In the proof-of-stake mechanism, the nodes of the network are based on the number of coins that the entity "stakes" toward the relationship. The platform is virtual and consumes much less energy for validation (as consensus does not need to be created to build trust). The entities (at the nodes) do not receive any cryptocurrency for validating the transactions and blocks; rather, they are offered a transaction fee as decided by the private network. There are options to create supply chain financing mechanisms using such a network and transaction tokens. For example, when a digital token is created in a permissioned proof-of-stake environment, the entities involved in the transaction can claim shared ownership of the token. Since the token can be monetized

(as cryptocurrency), entities could cash in their share of the token against prearranged financing mechanisms in the supply chain, such as discounts, loyalty points, extended credit, and paybacks.

Blockchain in Supply Chains

Supply chains have become one of the key sectors for the implementation of blockchain technology and the move to find uses other than cryptocurrency. Its characteristics of transparency, immutability, trust, and traceability fit well with the requirements to manage supply chains effectively and efficiently. Over the past few years there have been wide-ranging developments within this domain, with the latest data showing that 81 of the top 100 public companies are developing blockchain supply networks, launching pilot projects, or working with the ecosystem to create efficient connections between physical and financial supply chains.[5] The use of blockchain in supply chains can provide value in several areas, such as by increasing the traceability of inventory, reducing losses from counterfeit goods, improving the visibility and auditing of upstream and contract supply chains, and reducing paperwork and administrative tasks in recording and managing information. Blockchain adds value at all levels of the supply chain. It provides a platform to manage and record information, inventory, and financial transactions on a single ledger rather than multiple different ledgers, thus increasing traceability and efficiency. The platform provides robust recording and auditing of transactions using smart contracts and Internet of Things (IoT) systems (for example, for data capture of inventory flows). This is facilitated using unique identifiers and digital tokens. Value is also added by the chronological string of blocks carrying a digital token that is created during each transaction (for example, order generation between retailer and supplier, confirmation of the order, and the loan from the bank to the supplier).

With the development of the blockchain ecosystem, the application and implementation of this technology within the supply chain has rapidly increased. Within a supply chain environment, blockchains can be used to track procurement, provenance and traceability, logistics (e.g., delivery information, inventory information, handling, and temperature), manufacturing (e.g., batch numbers, date of manufacture, and conditions of manufacturing), contracting, and payments. This provides the integrated connections between various entities. For example, considering a food supply chain, the blockchain ecosystem will connect producers, processors, distribution centers, wholesalers, retailers, regulators, banks, and payment portals. It is also essential to analyze which type of blockchain platform—permissioned or permissionless—is suitable for the supply chain. Presently, the permissioned blockchain platform using proof of stake is preferred for supply chains.[6]

Smart Contracts

Smart contracts are one of the leading ways in which blockchain is incorporated into supply chains. Defined in 1994 as a "set of promises, specified in a digital form, including protocols within which the parties perform on the other promises," smart contracts are mechanisms to

[5] Lucas Schweiger, "81 of the Top 100 Public Companies Are Using Blockchain Technology," Blockdata, September 22, 2021, https://www.blockdata.tech/blog/general/81-of-the-top-100-public-companies-are-using-blockchain-technology.

[6] Hanns Christian Hanebeck, Nadia Hewett, and Paul A. McKay, "Inclusive Deployment of Blockchain for Supply Chains: Part 3," World Economic Forum, July 2019, https://www3.weforum.org/docs/WEF_Inclusive_Deploymentof_Blockchain_for_Supply_Chains.pdf.

execute transactions that are set with certain rules and regulations.[7] Smart contracts are programs containing certain rules and conditions for the transaction, and they remain in the blockchain once deployed. When these conditions are met, the contract will execute. For example, once the nodes have verified that an order has been delivered, the smart contract may execute for payment to the supplier. This will then provide a new transaction that the network will need to validate. The smart contract mechanism will benefit in the future through the use of automation and AI technologies. For example, AI technology will enhance trend analysis and reaction to supply chain risks, which will enable intelligent decision-making. This decision-making will in turn enable smart contracts based on prenegotiated conditions for supply chain transactions. Smart contracts will work effectively in the blockchain environment as they cannot not be tampered with. However, if the contract needs to be modified, the blockchain will notify members in the network regarding the change and thus require validation. Smart contracts will be designed based on enforceable legal principles that will provide the conditions for execution. They will also be useful for procurement contracts and can facilitate the deployment of the transactions.

Smart contracts are self-enforcing and are governed through the network without requiring further intermediaries. When the smart contract is completed, it forms part of the block (within the blockchain) and hence cannot be altered at a later date, even if the entities agree to a change. Instead, a new smart contract would need to be executed for the change. Along with the ability to record the movement of industrial assets and transactions associated with them, the blockchain environment can be utilized effectively for managing IP and digital assets. This can be done by recording the transactions in blocks with the appropriate tokens, as well as by using smart contracts for payments, commissions, and royalties. These records can then be used as evidence in court during IP disputes as well as during the legal registration of the IP. Yet legal issues must be addressed before this technology can be applied on a large scale, such as "questions of governing laws and jurisdictions, enforceability of smart rights, data security and privacy concerns, reliable rules and definitions for smart contracts."[8]

Other Uses of Blockchain in Supply Chains

The uses for blockchain in supply chains extend far beyond smart contracts, and many global companies are implementing this technology in creative ways. Some examples include the verification of the provenance of high-value items such as diamonds, gems, and gold; ethical sourcing and traceability for food and pharmaceuticals; and documentation and insurance. The remainder of this section discusses some specific examples of the use of blockchain technology within anti-counterfeiting and IP protection.

Tracr. The Tracr blockchain platform was initiated by De Beers group in collaboration with the diamond industry to instill trust within the diamond supply chain through provenance, authenticity, and traceability of the mined diamonds. The process creates a digital asset for each physical diamond that enters the supply chain from the diamond mine. The initial registration records the country of origin and authenticity characteristics. The physical flow of the diamond from the mine to the next process of cutting and polishing to manufacturing (in the case of jewelry), retailer, and finally end consumer is recorded on the digital asset as it transfers from

[7] Andreas M. Antonopoulos and Gavin Wood, *Mastering Ethereum* (Sebastopol: O'Reilly Media, 2018).

[8] Birgit Clark, "Blockchain and IP Law: A Match Made in Crypto Heaven?" World Intellectual Property Organization, WIPO Magazine, February 2018, https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html.

entity to entity. The ownership of the diamond is recorded at all stages of the process within a permissioned blockchain system.

TrustChain. TrustChain is a blockchain environment created through the collaboration of IBM and a consortium of jewelry and diamond companies. This platform will register, track, and authenticate diamonds and precious metals from the mines to the retailers and provides provenance and traceability of the jewelry and its components.

BernsteinIP. The blockchain platform has IP applications through timestamping, providing proof of existence, and securing the IP right of the holder. Platforms such as Orbit Blockchain and companies such as P&TS provide blockchain timestamping. The BernsteinIP platform uses Bitcoin blockchain and timestamping mechanisms to create a digital trail of record for the IP owner's innovation and creativity. The IP will be registered on the platform to prove existence, ownership, how the IP evolved over time, and the current state of the IP. The process creates a digital asset for each iteration of the evolution of the IP (or project), generating a chain of ownership and existence of the IP.

Aura. The Aura Blockchain Consortium comprises LVMH, Prada, Richemont, and Cartier. The platform was created for providing authenticity, ownership, and product history information to clients. This helps build trust with the client and protect against counterfeiting. During manufacturing each product is provided a unique digital identifier. This digital identifier has the required cryptographic record of the flow of the product to the end consumer from design, raw material supply, manufacturing, and distribution. The end consumer has access to an online certificate that provides provenance and authenticity.

Blockchain Implementation Challenges

Blockchain implementation within supply chains has been slow due to lack of digital skills, a general lack of awareness of this technology, and the complexity between public and private systems. The blockchain ecosystem is rapidly evolving with several pilots and startups being set up. The level of understanding of this technology is gradually evolving with further implementation. Some challenges to consider include the following.

Smart contracts. To implement smart contracts widely and effectively, the skills gap needs to be closed. Testing of contracts will require an experimental setup before they can be deployed on the live network.

Computational cost. The entities within the network will need to pay a cost associated with verification (hashing). Within the Ethereum platform the cost incurred is known as gas, and this is paid by using "ether." The cost is calculated on three criteria—how quickly the contract needs to be completed, how much the original party is willing to pay, and the complexity of the transaction.[9] The cost associated with the use will have an influence on future operational and business models.

Private vs. public blockchains. Due to the level of complexity within the consensus mechanism, the time required for processing transactions within a permissioned system will be less than that of a permissionless system. Although the permissionless system offers more decentralization, anonymity, and transparency, a permissioned system offers better scalability. Scalability is a challenge that will influence adoption of this technology within supply chains.

[9] Abdul Jabbar and Samir Dani, "Investigating the Link between Transaction and Computational Costs in a Blockchain Environment," *International Journal of Production Research* 58, no. 11 (2020): 3423–36.

Security and privacy challenges. Although the basic advantage of the blockchain network is immutability and verifiability of information (transactions), a 51% attack within a permissionless system may be possible. In such a scenario, a group of miners may be able to control over 50% of the network's mining hashing rate. This then provides them an opportunity to control the work of other miners and interrupt the recording of new blocks, thus controlling the blockchain and the reward. Permissioned systems provide stronger security. The current blockchain system also poses challenges in terms of integration with legacy systems, which could cause issues within extended supply chains.

As with any online networked system, there are also potential challenges associated with network speeds, network capacity, capacity of the ledger, and data quality. In addition, blockchain technology could disrupt a supply chain's operational and information systems. The initial implementations will be industry sectors that require mandatory traceability and transparency (requiring trust). The technology is developing rapidly and has moved from being focused on cryptocurrency to proof-of-stake and smart contracts. The next stage of the evolution of this system is the development of distributed applications (DApps), which will be useful for tracking inventory, managing data integrity, and integrating correct data with the blockchain platform. This will be supported by the evolution of future IoT devices and sensors enabling scanned data to engage directly with the blockchain platforms.

Samir Dani is Professor of Operations Management and Deputy Director of the Keele Business School at Keele University. He can be reached at <s.dani@keele.ac.uk>.

APPENDIX 3: THE ROLE OF ARTIFICIAL INTELLIGENCE IN SUPPLY CHAINS

Robert Boute

The integration of artificial intelligence (AI) in supply chains has the potential to improve operational efficiencies. AI may replace manual work through increased automation, or it may support complex supply chain optimization decisions, thereby augmenting human work. Enhanced information transparency through blockchain technologies may facilitate further application of AI.

AI refers to the ability of a computer or computer-controlled robot to perform tasks commonly associated with human beings. The "intelligence" in the term implies that the task being performed by a machine, script, or algorithm would require the use of intelligence if a human were to do it. AI has been around since the late 1950s, yet the recent and rapid improvements in computing power, combined with the availability of big data, provide new opportunities for the application of AI in business, including to improve supply chain visibility and decision-making.

Although analytics and computer support have been used for a long time in logistics and supply chains, "digital control towers" have recently been introduced that monitor machines, vehicles, and devices via sensor technologies in real time. Similar to an airport control tower, digital control towers can provide visual alerts that warn of inventory shortfalls or process bottlenecks before they happen. This extensive connectivity, known as the fourth industrial revolution and referred to by the term Industry 4.0, is critical to improve supply chain continuity and predictive risk management. Problems with suppliers or material shortages can cause critical disruptions in the supply chain.

The next section of this appendix details how AI can automate certain workflows in supply chains. The following section then describes how the availability of historical data may give rise to increasingly sophisticated algorithms that add additional predictive intelligence. The final section highlights how blockchain technologies can facilitate AI applications through trusted data-sharing among multiple supply chain partners and improve supply chain security.

Robotic Process Automation

Robots and automation allow work to be performed by a machine instead of a human. They are well-integrated in factory and warehouse operations. Today we witness their appearance in back-office operations, where the automation of tasks is referred to as robotic process automation (RPA). RPA is a software application, known as a bot, that performs automated tasks. By interacting with applications in the same manner that a human would, software bots can open email attachments, complete electronic forms, record and rekey data, and perform various other tasks that mimic human action.

RPA is particularly efficient in automating very specific, highly repetitive tasks that follow predefined rules. When bots run autonomously (unattended), their workflows should be preprogrammed such that human involvement is not required in the processes that they perform. To work independently, these bots follow a rules-based process to completion. Such a process is today only possible for relatively simple tasks.

For complex logistics tasks arising from judgmental decisions that require context awareness (and perhaps even qualitative factors), RPA bots may run in supervised (attended) mode.

Human employees work side by side with the bots, which may be likened to virtual assistants providing support to an individual employee to boost productivity. Attended bots increase the productivity of the planner by performing time-consuming repetitive tasks, while leaving the contextual and judgmental decision-making to the human.

RPA is used in logistics accounting teams to process invoices. By extracting billing amounts, account information, dates, and addresses directly from invoices into accounting software, it can send confirmation emails and execute payments, among other tasks, without human intervention. Similarly, RPA is used to support and automate customs declarations by retrieving a customer's shipment information and directly translating it into customs codes, tax statements, and other documents. This not only relieves human workers from performing these effort-intensive manual processes, but also may reduce human mistakes, resulting in less noncompliance fees or demurrage charges.

Data Analytics and Machine Learning

Most supply chain applications rely on data, such as historical demand, current inventory levels, or supplier data. If these data points remain countable, one can implement or even program if-then instructions to support or automate decision-making. The increased use of digital supply chain applications, as well as the connectivity of assets through sensors and digital control towers, generates large amounts of data, possibly in real time. When the number of data sources grows rapidly, the ensuing mountain of data makes the explicit enumeration of if-then instructions infeasible. This is where machine learning comes into the picture.

Machine learning is the subset of AI where an algorithm "learns" to perform a task without using explicit instructions. To understand the possible applications in supply chains, it is helpful to distinguish between the different forms it can take. Broadly speaking, one can divide machine learning into supervised, unsupervised, and reinforcement learning.

Supervised learning algorithms learn to make predictions based on an extensive set of training data with the "correct" answers that serve as supervisors. The goal is to make sufficiently accurate predictions on a new data set. Supervised learning is used in supply chains to forecast demand based on a large data set with multiple input variables, such as the marketing mix (price, promotions, discounts, advertising), seasonality, calendar events, weather forecasts, lagged sales data (sales from previous periods), and even social media reviews, using tools such as text mining and natural language processing. It is also used in transport and logistics to predict transit time delays based on temporal factors like departure day, weather or traffic information, and real-time information that keeps track of the realization of the planning. This predictive intelligence allows supply chain managers to take corrective action and avoid disruptions in the supply chain.

The same intelligence is used in supply chains to predict when a computer-based prescription is likely to be overruled by a human. In the review of sales forecasts, for instance, a supervised learning algorithm can predict whether the decision-maker will modify the recommendation and whether such a modification will improve or impair the performance of the system. Using these predictions, a significant portion of the order recommendations can then be automated with little, or even a positive, impact on performance, thereby freeing up the decision-makers for other value-added activities.

Unsupervised learning algorithms describe patterns or groupings of data given a set of unlabeled observations—i.e., without knowing the correct answers. The goal of such analysis is

to group a set of data points such that data points in the same group or cluster are more like each other than those in other clusters. Often, such clusters represent data groups with distinctive characteristics for which specific operational policies can be designed. In supply chains, customers can be grouped according to purchasing behavior or common profiles through combinations of customer characteristics. Likewise, data can be used to cluster products into groups according to, for instance, their product-life-cycle stage or items that are frequently purchased together. Such clustering is useful to segment customers or products where a distinct logistics distribution approach or different target inventory levels are required. It can also be used to identify supply chain risk based on supplier or component data. In many industries, including the automotive, technology, and engineering manufacturing sectors, managing the flow of components involves thousands of worldwide suppliers. Problems with suppliers, from material shortages to poor labor practices and even legal investigations, can cause disruptions in the supply chain.

A final example is the identification of observations that do not conform to an expected pattern, known as "anomaly detection" or "outlier analysis," such as abnormal delays in lead times or supplier reliability. Their detection can spur further analysis to predict—or even better, to prevent—future disruption.

Reinforcement learning algorithms prescribe which decision or action to take based on the current state of the system, while taking the future impact of these decisions into account. By performing numerous trials and reinforcing specific actions that generate high rewards (or low costs), the algorithm learns which actions provide the best results in any given state. In contrast to human beings, a reinforcement learning algorithm can gather experience from thousands of parallel trial runs if it is run on sufficiently powerful computer infrastructure.

Such algorithms may support logistics planners to build more resilience into the supply chain through higher responsiveness and agility to real-time events or disruptions. When firms have access to multiple sources to replenish their inventory, reinforcement learning can support the decision of how much to replenish from a cheap offshore supply and how much to source locally at higher cost. It can also be used to combine multiple transport modes in parallel, where part of a shipment is shipped using a slow transport mode such as rail or waterways, and the other part is shipped using a more responsive mode such as road or air freight. Similarly, it is used to prescribe which items should be shipped from the central warehouse and which should be shipped locally to combine timely delivery with cost efficiency. By making use of a digital twin of its physical operations, numerous simulations can be run in the cloud to prescribe how to respond to a disruption.

Machine learning may be seen as a general-purpose technology where one is only required to outline the prediction objective along with the data sources needed to make the prediction. As software development kits are being designed to facilitate the interaction between programmers on the one hand and end users on the other, the focus of machine learning applications is reverting to the collection of clean data. The more labeled data can be fed to an algorithm, the better it becomes at generating accurate predictions.

Blockchain Technologies

Blockchain, the digital record-keeping system developed for cryptocurrency networks, can further facilitate the application of AI in the supply chain by creating a complete, transparent, tamperproof history of transactions among a trusted group of partners. Rather than integrating

enterprise resource planning systems, which is considered expensive and time-consuming, blockchain record keeping tracks the relevant flows of information, inventory, and money in a specific supply chain transaction. Each string of blocks is encrypted and distributed to the participants of choice, who maintain their copy of the blockchain. The integration of various flows of transactions makes it easy to collect data across firms, typically in real time, which in turn facilitates the application of AI. Applications include tracing food or pharmaceutical products through the supply chain—for instance, by equipping a refrigerated container with a sensor that monitors the temperature or any other relevant features. Likewise, tracking shipments can improve predictions on lead times or potential disruptions.

Blockchain technologies can also improve supply chain security. Supply chain security is the dimension of supply chain management that focuses on the risk management of external suppliers, vendors, logistics, and transportation. Through the logging and tracking of shipments, physical risks such as theft or sabotage can be rapidly identified, analyzed, and mitigated.

Conclusion

AI has much potential to increase operational efficiency by automating repetitive manual processes and shifting to proactive operations with predictive intelligence. The increased visibility of real-time operations through digital control towers or blockchain technologies may also build more resilience and reduce supply chain risk by avoiding disruptions or material shortages. As supply chain leaders continue in their digital transformation journey and as AI technology is maturing and becoming more accessible, the number of applications in logistics and supply chains will only increase in the years to come. Yet, while AI opens new opportunities, there are also potential downsides of digital connectivity: namely, cyber risk and ransomware. Security management systems and mitigation plans, therefore, remain indispensable to protect against such threats.

Robert Boute is Professor of Operations Management in the Vlerick Business School and Northwestern University. He can be reached at <r-boute@kellogg.northwestern.edu>.

NBR THE NATIONAL BUREAU *of* ASIAN RESEARCH

Seattle and Washington, D.C.

1414 NE 42ND STREET, SUITE 300
SEATTLE, WASHINGTON 98105 USA
PHONE 206-632-7370, FAX 206-632-7487

1819 L ST NW, NINTH FLOOR
WASHINGTON, D.C. 20036 USA
PHONE 202-347-9767, FAX 202-347-9766

NBR@NBR.ORG, WWW.NBR.ORG