

THE TIES THAT BIND

A Helsinki Commission Staff Report on Secure Supply Chains



**Wilson
Center**



The report was authored by U.S. Helsinki Commission staff. Rebecca Neff,* Senior State Department Advisor, and Paul Massaro, Policy Advisor, served as the lead authors.

The Helsinki Commission would like to thank the U.S.-China Economic and Security Review Commission, the Congressional Research Service, the Organization for Economic Cooperation and Development, the U.S. Chamber of Commerce, the Center for International Private Enterprise, the Foundation for the Defense of Democracies, Global Financial Integrity, the Atlantic Council, and others for their insights and expertise in helping to conceptualize this report.

*Rebecca Neff served as Senior U.S. State Department Advisor to the U.S. Helsinki Commission from August 2020-December 2020.

Views contained herein do not necessarily reflect those of the U.S. Helsinki Commission.



The Critical Supply Chains Initiative is The Wilson Center’s contribution to the ongoing national debate on strengthening supply chains. The core of the initiative is a series of dialogues with leading experts focusing on four key industries: critical minerals and rare earths; electric vehicles; the health sector, including pharmaceuticals and PPE; and defense and security. Relying on the expertise of industry experts, government leaders, and private corporations, this initiative brings together industry leaders, policymakers, and other stakeholders to answer some of the most pressing questions relating to America’s supply chains.

Contents

Executive Summary	1
Helsinki Commission	2
Introduction	2
Why Aren't U.S. Supply Chains More Secure?	3
Foreign Supply Chains in the United States	8
Should Certain Products or Supply Chains Be Named Critical for National Security?	8
Goal and Structure of Recommendations	9
Three Tiers of Response	10
Non-Binding Standards and Voluntary Guidelines	11
The International Framework and Development Efforts	13
Domestic Law and Executive Action	16
Conclusion	19



Executive Summary

The COVID-19 pandemic has laid bare long-standing vulnerabilities in U.S. and global supply chains, including American reliance on sole-source manufacturing and on Chinese manufacturing, in particular. This report examines threats to U.S. and global supply chains created by doing business with authoritarian regimes that flout the rule of law and recommends policies to strengthen global trade and commerce.

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is an independent U.S. Government commission created in 1976 to monitor and encourage compliance with the Helsinki Final Act and other OSCE commitments. As a part of the 1990 Charter of Paris, the Concluding Document of the Bonn Conference on Economic Cooperation in Europe, and related frameworks, OSCE participating States undertook commitments to uphold free and competitive market economies, improve corporate governance, and combat corruption. These commitments are threatened by the actions of authoritarian regimes in global supply chains.

This report identifies and examines seven threats to U.S. supply chains: (1) the theft of intellectual property, (2) defective and substandard products, (3) human rights abuses, (4) customs and border operations, (5) data privacy and security, (6) lack of transparency, and (7) free riders and illicit transactions. The report also briefly discusses foreign authoritarian investment in the United States. Finally, it analyzes whether certain goods should be considered for special status based on national security concerns. The report concludes that, rather than focusing on goods or industries, the United States should build a secure network of suppliers.

The report recommends a menu of policy options in a framework of three tiers based on (1) non-binding standards and voluntary guidelines, (2) international framework and development efforts, (3) domestic U.S. law and executive action. Recommendations aim to mitigate the threats identified by the report and ensure that supply chains become—and remain—transparent, responsible, accountable, and resilient.

The first tier focuses on the creation of a “certified secure” standard for individual companies and the establishment of a Secure Supply Chains Initiative, modeled on the Extractive Industries Transparency Initiative, which would set guidelines for participating countries.

The second tier reflects the need to apply existing international agreements to the problem; add anti-corruption provisions to new agreements; consider rule of law-based country groupings such as the D-10 concept; leverage development to create rule of law-based markets that offer an alternative to authoritarian ones; elevate the fight against authoritarian corruption; and redouble efforts at inter-parliamentary diplomacy.

Finally, the third tier recommends the passage of important anti-corruption legislation to criminalize the demand side of bribery and require professional services to uphold anti-money laundering requirements. The report also briefly discusses corporate board mandates, the role of tax policy, extraterritorial law enforcement, federal procurement, public-private partnerships, and diplomatic engagement.

Helsinki Commission

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is an independent U.S. Government commission created in 1976 to monitor and encourage compliance with the Helsinki Final Act and other OSCE commitments.

Consistent with its mandate, the Commission issues public reports concerning implementation of OSCE commitments in participating States. This report examines threats to U.S. and global supply chains created by authoritarian regimes and suggests proposals to strengthen global trade and commerce through the adoption of democratic principles. As a part of the 1990 Charter of Paris, the Concluding Document of the Bonn Conference on Economic Cooperation in Europe, and related frameworks, OSCE participating States undertook commitments to uphold free and competitive market economies, improve corporate governance, and combat corruption. These commitments are threatened by the actions of authoritarian regimes in global supply chains.

Due to the threats posed by exposure to authori-

tarian regimes, the United States and all countries that seek to safeguard the rule of law should generate a strategy to secure supply chains.

Introduction

The COVID pandemic exposed long-standing vulnerabilities in U.S. and global supply chains, including U.S. reliance on sole-source manufacturing and on Chinese manufacturing, in particular.

As COVID-19 cases spiked in the United States in March 2020, the United States lacked adequate personal protective equipment, ventilators, and other products required to safely and successfully treat patients with the virus.¹ At the time, much of the world's manufacturing of PPE was located in China, which nationalized production and withheld exports at the beginning of the crisis to deal with its own outbreak.

Once Chinese production increased, its exports of PPE included sub-standard, defective products, further endangering vulnerable and sick populations rather than assisting them. For example, Spain returned Chinese-made COVID-19 test kits after



Photo courtesy of: lev radin/shutterstock.com

learning the tests were only 30 percent accurate.² (China later introduced a new export certification process in an effort to improve the quality of its exported products.³)

The pandemic caught the United States unprepared, without the proper stockpiles and unable to acquire or produce the full extent of needed supplies from existing supply chains. Likewise, the United States' European allies suffered from similar shortages which were compounded by belated, defective Chinese supplies and equipment and lack of a coordinated transatlantic strategy⁴ Reliance on Chinese manufacturing for COVID-19 related products put the national security of the United States and its allies at risk. Though ventilators have waned in importance as the crisis has worn on—and been replaced with vaccines, which have proven less susceptible to supply chain issues—the initial failure of supply chains and even conflict between allies was eye-opening. Moreover, the theory that the COVID pandemic began by escaping from a Chinese lab has also gained new credibility.⁵

While COVID-19 laid bare the risks of China as the manufacturing hub for the world, the consolidation of goods' production in China is not a new phenomenon. In 2018, China comprised 28.4 percent of global manufacturing, while the United States, the second largest manufacturer, held a 16.6 percent share.⁶ This trend has been described by economist Thomas Palley as “Chinese-centric globalization.”⁷

For many manufacturing sectors, the cost competitiveness of producing in China has reduced redundancy in supply chains globally, making them more vulnerable to shocks that could come not just from a pandemic, but also from many other disruptors, including natural disasters, armed conflict, or other unforeseen events.

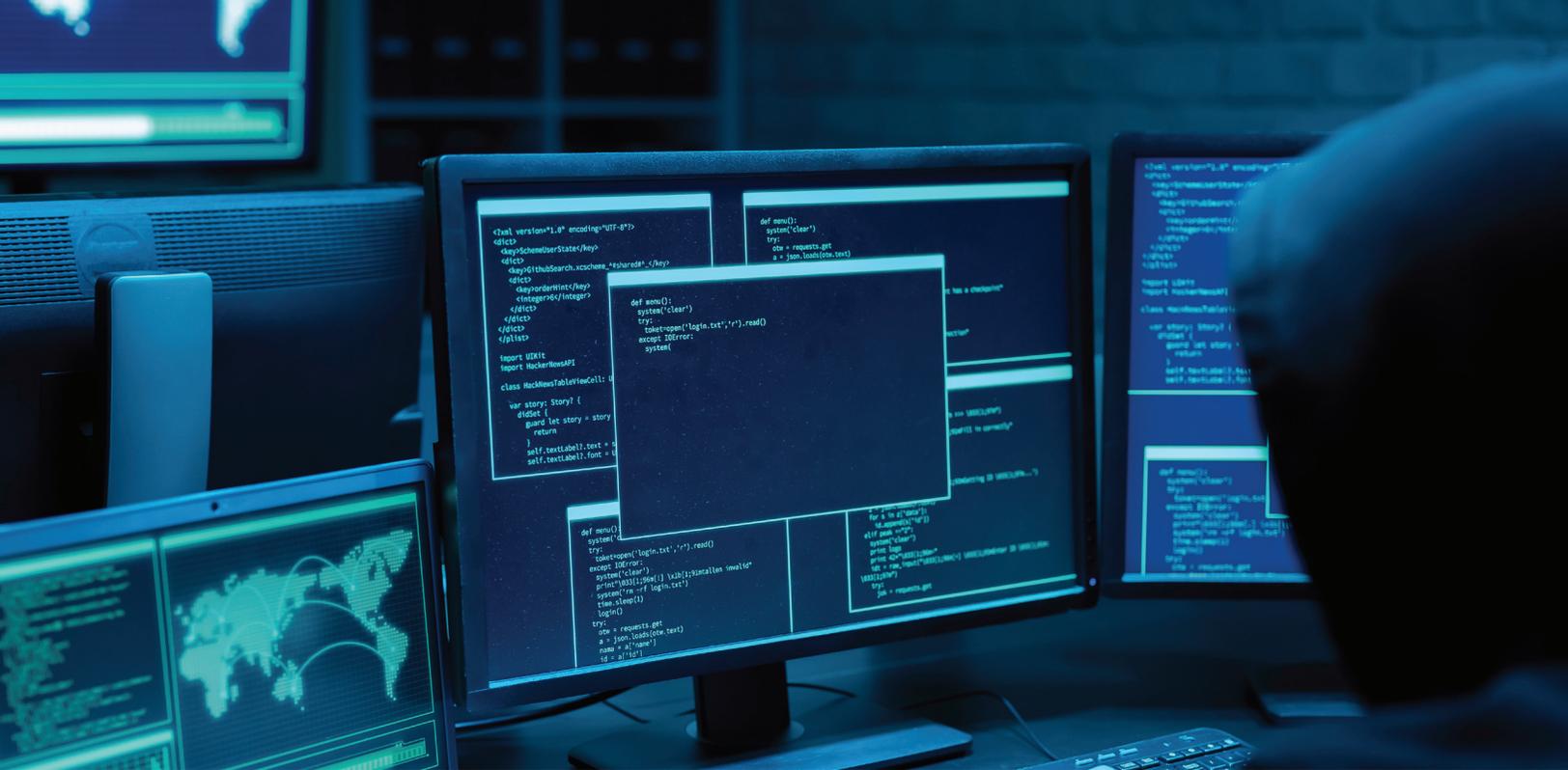
More generally, relying upon states in which the rule of law is not present is a risk that permeates global supply chains. Though China may be one of the most prominent examples, it is not the only state that seeks to participate fully in global supply chains while freeriding off the rule of law provided by global institutions.

While it is an oversimplification to conclude that supply chains located in democratic countries are inherently more secure than those located in authoritarian states threats to U.S. supply chains are heightened and compounded by the weak rule of law and poor governance that are characteristic of authoritarian governments. This is because authoritarian governments rule through corruption—dictators rely on it to ensure that the loyalty of cronies is secure.

Why Aren't U.S. Supply Chains More Secure?

In accordance with the mandate of the Helsinki Commission, this report examines the following threats to U.S. supply chains:

1. Theft of intellectual property
2. Defective and substandard products
3. Human rights abuses
4. Customs and border operations
5. Data privacy and security
6. Lack of transparency
7. Free riders and illicit transactions



1. THEFT OF INTELLECTUAL PROPERTY

One of the threats to U.S. supply chain security is the theft of intellectual property (IP) of U.S. firms. IP protection is essential to the economic productivity and growth of the United States. It allows a fair return on investment for innovators, creators, designers, and others who bring new ideas and products to the marketplace.

According to studies by the U.S. Chamber of Commerce, the positive effects of strong intellectual property rights protection include higher rates of investment in research and development, job growth in knowledge-intensive sectors, higher rates of investment in the life sciences and higher rates of innovative economic activity.⁸ All of these are vital components of a vibrant economy.

When IP protections are not enforced, there are serious consequences for U.S. firms and the American economy. Due to the innovative nature of U.S. businesses and the high demand for U.S. products, U.S. companies suffer some of the highest rates of counterfeiting in the world, according to OECD studies.⁹ In some sectors, such as high-tech infor-

mation technology goods, about 40 percent of fake goods infringe on the IP rights of U.S. firms.¹⁰ It is estimated that counterfeit goods and pirated software cost the U.S. economy more than \$225 billion each year. If theft of trade secrets is also included, the loss to the economy could be as much as \$600 billion annually.¹¹

Authoritarian regimes often turn a blind eye to IP violations. In many cases, they predicate technology transfer and data localization as a condition of market access and encourage and abet the theft of U.S. trade secrets from U.S. companies.

The U.S. Trade Representative publishes two annual reports on IP violations: the “Special 301” Report,¹² which evaluates the status of IP protection and enforcement in the countries of U.S. trading partners, and the Notorious Markets Report,¹³ which publishes the location of prominent online and physical markets engaged in piracy and counterfeiting. Both reports identify the worst violators of American IP as China, Indonesia, India, Algeria, Saudi Arabia, Russia, Ukraine, Argentina, Chile, and Venezuela.

Not surprisingly, these countries also suffer from weak rule of law. According to the World Justice Project Rule of Law Index 2020¹⁴, eight of the 10 countries ranked below the median point, except Indonesia (which ranked slightly above the median) and Saudi Arabia (which was omitted from the ranking).

As the rankings indicate, IP violations are not only a problem attributable to authoritarian regimes, and patent issuance and protection are of particular concern for India and Chile. However, the size and scale of the IP violations in authoritarian regimes should trouble the United States.

Firms that operate supply chains in authoritarian countries risk theft of IP and unfair competition from counterfeit and pirated products based on stolen IP. China (including Hong Kong) accounted for 83 percent of counterfeit goods seized by U.S. customs in 2019.¹⁵

In January 2020, the United States and China signed a Phase One trade agreement which committed China to undertake structural economic reforms, including greater protection of American IP. The U.S. Trade Representative has described the Chinese commitments as “fully enforceable.”

Prior to this agreement, IP enforcement in China was already improving, in part because China is developing its own IP it seeks to protect. Nonetheless, China’s industrial policies and IP theft, including cyber theft, remain a serious problem and China continues to seek to compromise U.S. systems to surveil and gather data.

2. DEFECTIVE AND SUBSTANDARD PRODUCTS

Beyond economic losses due to IP theft, counterfeit products frequently are defective or substandard, which threatens U.S. supply chains because of potential grave harm to American consumers.

For example, the threat posed by substandard medication that does not do what it purports or defective auto parts can lead to injury or even death.

With the ongoing COVID-19 crisis and the growing demand for medicines and personal protective equipment, there has been a sharp growth in illicit trade of fake goods that pose serious health and safety risks to citizens.¹⁶ The Organization for Economic Cooperation and Development has extensively analyzed the threats to public health and safety and the enrichment of organized crime from the \$4.4 billion industry of counterfeit pharmaceutical products.¹⁷

Identifying and rooting out counterfeit products from a supply chain has become more difficult as supply chains become more decentralized, stretching across borders with multiple tiers of suppliers. A counterfeit item in an otherwise legitimate supply chain causes damage to consumers, poses legal liabilities for a firm, and undermines public trust in the government regulation. For example, the U.S. firm Baxter International fell victim to adulteration of its drug herapin, which the FDA later traced to Chinese suppliers. The counterfeit ingredient in the drug was linked to 19 deaths and hundreds of allergic reactions in the United States alone.¹⁸

3. HUMAN RIGHTS ABUSES

Authoritarian regimes that disregard universal human rights also pose risks to U.S. supply chains. Significant human rights abuses, combined with a lack of transparency and accountability, can leave U.S. companies vulnerable to knowingly or unknowingly becoming entangled in practices of forced labor. Uncovering such practices could disrupt production as well as damage a company’s reputation and leave it vulnerable to lawsuits, sanctions, or other financial penalties. The Biden administration has condemned China’s treatment of the Uyghurs in Xinjiang as “genocide.”¹⁹

For example, according to a report by the Australian Strategic Policy Institute (ASPI), 11 Chinese companies sanctioned by the U.S. government for use of forced Uyghur labor in production facilities in Xinjiang province²⁰ were part of the supply chains of at least 83 well-known global brands in the technology, clothing, and automotive sectors.²¹ The U.S. government did not disclose whether any of the U.S. firms identified in the ASPI report were sanctioned, but the risks of continuing production and manufacturing in Xinjiang clearly remain quite high.

4. CUSTOMS AND BORDER OPERATIONS

Considering how goods, both intermediate and finished, frequently move across oceans and borders, U.S. supply chains can be threatened by corrupt or ill-performing customs and border operations.

Lack of transparency in customs and shipping can threaten cargo security and facilitate illicit funds transfers. In 2013, the World Trade Organization (WTO) adopted a Trade Facilitation Agreement that aimed to reduce costs and improve efficiency through automation, simplification of customs procedures and other measures, as well as improve governance and limit opportunities for bribery and corruption. To date, implementation of this agreement has progressed slowly. High-income countries, in general, have achieved a greater degree of implementation than low-income countries.²²

In countries where customs practices are automated, like the United States, the threat to cargo security results from a lack of analytical information that would give a fuller picture of patterns over time about who is associated with a particular shipment and which countries it may have transshipped before arriving on U.S. shores. Access to this type of data would improve the ability to detect and analyze threats to the border security.

Customs operations also can be threatened by the data gathered and stored by customs authorities

and service providers. One Chinese state-owned firm, NucTech, which provides screening systems for cargo, luggage, and passengers at airports, appears to be gaining significant market share in Europe.²³ Concerns about the extent to which the Chinese Communist Party could gather and access data gathered by NucTech led the Transportation Security Administration to ban the use of NucTech equipment from most airports in the United States in 2014.²⁴ Given the global nature of supply chains, improving the security for U.S. supply chains requires convincing top trading partners, such as Europe, of existing threats and the need to take action.

5. DATA PRIVACY AND SECURITY

The NucTech example demonstrates the vulnerability of enterprises that can be influenced by or compelled to act on orders of an authoritarian regime. The danger is not a state-owned enterprise *per se* but a state that can access a private firm's data, for reasons it deems appropriate, without a right of refusal by the firm. This is a threat to U.S. supply chains that store or process the personal data of U.S. persons in these environments. Recognizing concerns that have been raised about Chinese practices related to data privacy and security, China has recently released a draft law aimed to increase data protection, although how it will work in practice is yet to be seen.²⁵

The U.S. State Department has actively sounded the alarm about the threat posed to the United States and its allies by Chinese telecommunications companies. In response to this threat, the State Department has launched the "Clean Network," which established an industry-vetted set of digital trust standards to ensure the safety and security of digital transmissions. The standards, which aim to provide "clean" carriers, apps, app stores, cloud computing, and more, disqualify Chinese companies such as Huawei or ZTE from providing these services in the United States and

partner countries. Thus far, more than a dozen countries and telecommunications firms from Europe, Asia and the Western Hemisphere have pledged to join the Clean Network.²⁶

6. LACK OF TRANSPARENCY

U.S. supply chains face heightened risks when they depend on inputs, labor, or capital from opaque regimes. Due to the interconnected nature of the global trading system, what happens in one country can threaten the health and security of other countries.

A country's lack of transparency impedes a U.S. firm's ability to conduct due diligence and can result in risky deals that create liabilities for the U.S. firm. The risk is even greater if the country hosts "corrosive capital" in its economy. This type of investment is opaque, unaccountable to local stakeholders, and not locally driven or market oriented.²⁷ It undermines rule of law and good governance and can have a degrading effect on the overall economy of a country and its trading partners. Over time, this type of investment erodes the business climate in such a way that it severs links with foreign direct investment connected to firms that rely on Western markets, which operate in a more transparent manner. In addition, lack of foreign investment limits opportunity for citizens

to engage in the international economy, and for domestic firms to grow.

Another example of the threat posed by lack of transparency is state-to-state agreements, such as China's Belt and Road Initiative, which 34 countries in Europe and Central Asia have signed. While the details of each agreement vary, the agreements are characterized by easy access to financing under opaque conditions which have included predatory investment and lending practices, and state support for Chinese state-owned enterprises, resulting in unsustainable business models and disadvantaged local businesses communities.²⁸ These practices, which are not transparent to the country or companies involved in the loans, can lead to large debt burdens, bankruptcy, and insolvency, and are often referred to as "debt-trap" diplomacy.²⁹

7. FREE RIDERS AND ILLICIT TRANSACTIONS

Perhaps the most serious threat to the global economy is what some have called the "freerider" challenge to the rules-based global economic system. Free riders benefit from the economic architecture existing since World War II, including bilateral or multilateral trade agreements under the World Trade Organization (WTO) that set the foundation for a rules-based, open, market-led economy and limited enforcement mechanisms.³⁰



The problem arises when countries selectively follow the rules, or worse, pass all the necessary legislation to adhere to the system but fail to enforce it. For example, the United Arab Emirates (UAE), a WTO member, has become a global hub for wealthy investors, with fast-growing real estate and retail sectors. However, lax regulations and rent-seeking officials seeking to profit from corrupt customs practices in this active transshipment point reportedly have made the UAE a hub for illicit transactions and dirty money.³¹

Illicit transactions threaten both the greater global economic system and small-town America. In the 2019 Helsinki Commission briefing³² “*Asset Recovery in Eurasia: Repatriation or Repay the Patron*,” former FBI special agent Karen Greenaway captured the impact on the average citizen:

“I’m not sure people understand how damaging taking dirty money really is to the United States. I like to use the analogy of a dry streambed. Dirty money is like a rainstorm coming into a dry streambed. It comes very quickly, and a lot of it comes very fast, and the stream fills up, and then it gets dry again. So what if you are a company that’s purchased by dirty money? That dirty money is not going to be a steady flow into and out of the account so that you can run that company the way – or the business the way it’s supposed to.

So what happens? Well, maybe you don’t pay the electric bill, the FedEx bill, or the tax bill on time. Over time, the safety standard [of the business] goes down. But people don’t want to say anything because they want that job, and they need that job in their community. After 2008, when the financial institutions collapsed, essentially, in the United States—here was a fire sale for a lot of our properties.

And as a result, what we have is people who don’t live in the United States, who don’t have

any intention of really investing in the United States, but they needed a place to put their money. And that business down the road was a perfect place to put it. Now the money is drying up. And now those businesses are going into default. And maybe that’s the only business in that community that’s employing people. So, I think it’s hurting small town America. I just don’t think that we’ve come to that realization yet.”

Foreign Supply Chains in the United States

Threats to U.S. supply chains apply to investment of U.S. companies abroad, but also to foreign investment in the United States. For instance, foreign investors and more recently foreign students have reportedly sought to steal American IP while working and living in the United States.³³

However, the United States has strong mechanisms in place, such as the Committee on Foreign Investment in the United States (CFIUS), which was recently strengthened by the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), to protect against acquisitions that threaten U.S. national security.

In contrast, national security-related investment screening in Europe is not a competency of the EU but of its Member States, which have approached this challenge unevenly. However, a new agreed-upon EU framework on investment screening published in October may improve the overall situation.³⁴

Should Certain Products or Supply Chains Be Named Critical for National Security?

Traditionally, defense sector products have been designated as critical for national security, which means the U.S. government regulates any exports and verifies the end use of the products. In the

context of COVID-19, there have been calls to expand the definition of national security critical products and to call for onshoring production of some of the manufacturing of these goods.

Some analysts suggested that the 16 critical sectors defined in Presidential Policy Directive 21 could form the basis of national security sensitive products. Those sectors include chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. These sectors have been extensively analyzed by government and industry, and plans have been drafted which identify risks (including supply chain risks) and propose mitigation strategies.³⁵ Perhaps more could be done to implement these strategies and to ensure rigorous CFIUS processes for any proposed foreign investment affiliated with authoritarian regimes into these sectors, but it seems redundant and unnecessary to create such a sweeping list of new national security critical products.

Congress and the U.S. administration are already examining the inherent risks of China's role as a global supplier of PPE, antibiotics, and active pharmaceutical ingredients and considering actions to help spur domestic production and diversify U.S. supply chains.³⁶ During its own COVID-19 outbreak, China nationalized production of COVID-19-related supplies and restricted their export, including products made by U.S. firms located in China. It was not the only country to do so. January-February 2020, the governments of Taiwan, Thailand, France and Germany also boosted domestic production of some COVID-19-related supplies and restricted their export – however, these countries were transparent about their decision and notified the WTO, while China did not.

China's lack of transparency and disregard for international norms negatively affected its trading partners, including the United States, while countries with a strong rule of law upheld international norms and obligations. For those countries, a global set of agreed norms and standards on how to continue cooperation and information sharing during an event like a pandemic would have gone a long way to mitigating a winner-take-all attitude that characterized most countries' response to COVID-19.

Assembling a list of national security critical products based on the experience of COVID-19 is unlikely to be effective, given the unpredictability regarding the nature of any future global disruption to U.S. supply chains. The United States needs a new strategy that will build a secure and trusted network of suppliers, rather than supplies.

Goal and Structure of Recommendations

The four criteria below should all be met for a supply chain to be considered "secure." They represent the ideal criteria that supply chains should meet and the goal for which the United States should strive. They are interlocking and should all be met simultaneously. For example, to be responsible, supply chains must be transparent. If supply chains are transparent but not accountable, that results in deep injustice as crimes go unpunished. The recommendations seek to pursue all of these aims equally.

1. Transparent

Transparency is crucial to secure supply chains as it is key to security in many economic and financial matters. Transparency means that authorities can readily trace the origin, transit, and destination of goods and services journeying through all levels of the supply chain. It is also important to know

the ownership structure of manufacturing entities and the role of non-market players who may have non-commercial aims. Ideally, journalists and civil society would have full access to pertinent information to serve as a further disincentive to corrupt or authoritarian efforts to interfere with secure, open exchange.

2. Responsible

Responsibility in supply chains means compliance with the highest international standards promulgated by international organizations with deep expertise and strong credentials in this space.³⁷ Supply chains should also be compliant with the voluntary standards proposed and promulgated below and other standards as set out by U.S. laws and regulations, save for the rare cases when the supply chain does not touch the U.S. market, financial system, or private sector.

3. Accountable

Accountability means that there are reliable and just mechanisms in place to punish and deter non-compliance. Even when supply chains are mostly compliant, there will be actors who attempt to cheat. In those cases, accountability is central to ensure that the actor in question is punished and supply chains are set back into compliance. Otherwise, the lack of penalties for the cheating of one party will result in the cheating of others.

4. Resilient

Finally, supply chains should be resilient. They should be able to withstand various shocks, primarily through supply chain diversification. If parts of supply chains are based entirely in one authoritarian jurisdiction, then it no longer matters that the supply chain is transparent, compliant, and

accountable—this state, as the sole source, will be able to apply pressure to generate outcomes it considers favorable.

Three Tiers of Response

The United States can seek to establish supply chains that conform with these criteria via three tiers of policy response. These tiers begin with non-binding efforts and move through ever more legally binding initiatives.

The tiers are not meant to be sequential but rather provide a menu of options for lawmakers and policymakers to consider in order to achieve more secure supply chains. The first tier encompasses voluntary efforts. This tier seeks to set out guidelines and frameworks that companies and countries may bind themselves to of their own accord to reap the benefits, both real and reputational. The second tier encompasses international law and country-to-country agreements, both bilateral and multilateral. These recommendations include the potential for new provisions in international agreements. Finally, the third tier encompasses national law binding on the U.S. government, U.S. companies, and all companies listed on a U.S. stock exchanges.

The successful generation of secure supply chains will empower the pursuit of other U.S. foreign policy objectives like combating transnational organized crime, human trafficking, and kleptocracy. Kleptocrats and transnational criminal figures regularly rely on the weak points in supply chains to achieve their goals. The current global-consensus system is not working when international regulatory bodies shy away from needed standards because a handful of states block these measures.

1. NON-BINDING STANDARDS AND VOLUNTARY GUIDELINES (FIRST TIER RESPONSE)

The first tier of response involves the creation and promulgation of non-binding standards and voluntary guidelines for companies and countries. Though non-binding and voluntary, such standards and guidelines will carry reputational weight.

For such standards and guidelines to be effective, a system must exist to rate companies and countries by compliance—or lack thereof—and provide meaningful reputational advantages to those that comply.

This report proposes two sets of standards and guidelines—one for companies and one for countries. The overarching goal is to create a norm of secure supply chains that these entities willingly comply with. This norm will follow broadly the four criteria set out in the previous section that, taken together, define a secure supply chain: transparency, responsibility, accountability, and resiliency.

a. Standards and Guidelines for Companies

While a simple ranking system is precluded by the sheer number of companies and their variety in industry and size, companies might be incentivized by being offered the opportunity to be “certified secure.” This designation would be certification provided by a reliable private sector entity or non-governmental organization for companies of a certain size and would be earned by application of the company. Over time, it would create a community of companies that would be considered secure.

Participating companies would provide documentation that demonstrates their commitment to secure supply chains and the work they were doing to ensure that they are not contributing to the problem. Minimum standards would focus on transparency and resiliency, and include:

Transparency

- Collecting beneficial ownership information of suppliers and clients.
- Fulfilling basic “know your supplier/customer” requirements, such as ID and verification documents as to the identity of the individual as well as basic information that the money being used to pay for the good or service was not gained illicitly.

Resiliency

- Committing to a resilient “China plus one” or otherwise “authoritarian plus one” approach, i.e. contracting with at least one market outside of the China or other large authoritarian market to ensure that PRC or that market, as the largest and most influential authoritarian market for the United States, is not able to exercise undo leverage upon the company and certain sectors of the U.S. economy.

While these requirements may not be appropriate for every company, even many small businesses with only domestic operations may rely on global supply chains and would benefit from the knowledge that their partners are “certified secure,” or the marketing opportunity that might be result from being “certified secure” themselves. Such a certification could be synchronized across borders with countries that are willing to commit to the same or similar system, culminating in a transnational “certified secure.” Management by a private sector or non-governmental entity that is already transnational would be most appropriate.

b. Standards and Guidelines for Countries

The development of standards and guidelines for

countries for secure supply chains can be modeled on the Extractive Industries Transparency Initiative (EITI).³⁸ The EITI is a non-governmental entity that promulgates a listing of requirements that countries sign up to in order to fight corruption and build integrity in the extractives sector, and could be a useful model for a similar system relating to supply chains.

A Secure Supply Chains Initiative (SSCI) would require countries to commit and implement a set of conditions, based on the four criteria above, that would earn them the status of SSCI member in good standing. The initiative would be governed by a board made up of countries, businesses, and appropriate civil society actors, much like the EITI board. Fundamentally, the goal of this initiative would be to prevent freeriding by states that seek to take advantage of global rule of law without any contribution. Sorted by criteria, such conditions could include:

Transparency

- Mandating country-level collection of beneficial ownership information upon incorporation of companies.
- Mandating anti-money laundering gatekeeper requirements (reporting of suspicious activity by all banks, lawyers, accountants, consultants, real estate professionals, investment advisors, and other professional services providers).
- Establishing trade transparency units—governmental outfits tasked with fighting trade-based money laundering by invoicing.
- Requiring a clear accounting of state-directed, state-subsidized, and state-supported activity among companies.
- Requiring transparency around the use of forced labor.

Responsibility

- Providing resources for regulation of not just “hard illicit” activity—weapons, drug, and human trafficking—but also “soft illicit” activity, such as counterfeiting.
- Taking action on fighting theft of intellectual property.
- Allowing market access without imposing conditions of coercive technology transfer.
- Committing to fighting corruption, especially in customs (e.g. trade-based money laundering, bribery at ports of entry, and falsification of data).
- Providing ample resourcing to customs.³⁹
- Mandating shipping “track & trace” programs.

Accountability

- Resourcing law enforcement to enforce health, safety, IP, and other regulations and punish and deter attempts to undermine secure supply chains.
- Safeguarding independent judicial systems that are clearly not under the influence of politics.
- Providing facilitated Mutual Legal Assistance Treaty (MLAT) process with participating countries to pursue corruption and trade crimes rapidly.
- Targeted sanctions authorities that are actively used to deter and punish attempts by non-compliant state and non-state actors to undermine secure supply chains.

Resiliency

- Mandating government procurement policies that prohibit reliance upon a single supplier, except for cases where a single supplier is also a participating state of SSCI.
- Establishing supply chain diversification requirements for boards of publicly listed companies.

Countries must remain in compliance in order to keep their membership. Evaluation would occur via a board review of participating countries.

Accession will be the point at which the SSCI has the most leverage, and criteria should be very strict. Once a country is in the SSCI, it will be difficult to expel it.

SSCI members in good standing should enjoy “fast-lane” customs systems in other SSCI countries, which would provide an opportunity for faster trade with fewer checks and lower transaction costs. Customs officials could then focus on riskier, non-SSCI countries. Though fraud and corruption might be employed to get around the system, transparency standards should mitigate such challenges.⁴⁰

The International Framework and Development Efforts (Second Tier Response)

There are a large groups of existing trade agreements, including bilateral investment treaties, that could be amended to include provisions guaranteeing transparency, responsibility, accountability, and resiliency of supply chains. Additionally, trade agreements currently under negotiation could include provisions to guarantee similar provisions. Though such provisions would be new, they would not be unprecedented.

a. Existing Provisions

The United States should begin by leveraging existing international frameworks and dispute settlement mechanisms to combat the undermining of supply chains, including the World Trade Organization Trade Facilitation Agreement and various standing free trade agreements (FTAs).

The United States should use all trade policy tools and dispute settlement options at its disposal to actively pursue violations of secure supply chains. Where possible, such actions should be pursued in coordination with allies. Though the United States and the European Union sometimes find themselves at odds concerning trade policy, their differences are small compared to their common differences with authoritarian countries. For instance, the United States and Europe have agreed to expand their bilateral discussions on China to better align strategies and increase cooperation, though it remains unclear if that agenda will include supply chains.⁴¹

The United States can also use its participation in multilateral organizations to prioritize secure supply chains. Multilateral organizations should not be the center of the U.S. strategy, given the membership of authoritarian states. However, efforts to redirect these organizations toward the creation of secure supply chains would still serve a purpose, not only in the case of organizations focused on law enforcement like INTERPOL, but also in organizations such as the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), and the Food and Agriculture Organization (FAO). Authoritarian states have invested considerable resources into these organizations precisely due to their potential for legitimacy-generation and standard-setting.⁴²

b. New Provisions in Trade Agreements and Other Bilateral & Multilateral Agreements

The United States-Mexico-Canada Trade Agreement (USMCA) ratified in January 2020 is the first active U.S. FTA to include a chapter on anti-corruption.⁴³ This chapter sets forth a binding, enforceable commitment to fight corruption and keep accountable international trade:

“Each Party shall adopt or maintain legislative and other measures as may be necessary to establish as criminal offenses under its law, in matters that affect international trade or investment, when committed intentionally, by a person subject to its jurisdiction... (b) the solicitation or acceptance by a public official [an individual: (a) holding a legislative, executive, administrative, or judicial office of a Party... (b) who performs a public function for a Party, including for a public agency or public enterprise], directly or indirectly, of an undue advantage for the official or another person or entity, in order that the official act or refrain from acting in relation to the performance of or the exercise of their official duties.”⁴⁴

Similar—and similarly enforceable—passages regarding secure supply chains could be inserted based on initiatives outlined for the SSCI. Such

provisions should become the norm for the United States and the country should insist upon them in future agreements, thereby leveraging its market access to generate secure supply chains.

Separately, the United States should join the United Kingdom and the European Union in pushing for beneficial ownership registers throughout the world. The Helsinki Commission has been active in exploring these models, including through holding a hearing on the topic and hosting an event with the UK’s Anti-Corruption Champion, MP John Penrose.⁴⁵ Though many abusive shell companies that facilitate fraud and corruption in supply chains are incorporated in the United States itself, many others are incorporated in jurisdictions such as the British Virgin Islands. This jurisdiction, in particular, has recently pledged itself to establishing a public beneficial ownership registry.⁴⁶ If the United States were to join these efforts, it could not only keep its own system from abuse, but also monitor the implementation of others.

c. International Development and New Markets

The United States can leverage its development capability and international development assistance to support and strengthen the rule of law in

President Trump, Canadian President Trudeau, and Mexican President Enrique Peña Nieto sign the U.S.-Mexico-Canada trade agreement during a ceremony in Buenos Aires, on the margins of the G-20 Leaders’ Summit on November 30, 2018. Photo courtesy of: U.S. Department of State from United States



foreign markets in order to give companies alternatives to authoritarian markets. Recent actions in this space in the form of the Development Finance Corporation, created by the BUILD Act, as well as the Blue Dot Network—a set of countries that will certify infrastructure projects as compliant with global standards—provide a strong base from which to expand U.S. efforts.⁴⁷ These efforts could be further built upon through the explicit policy of expanding to include a grouping of democracies and countries that achieve the four key criteria that ensure secure supply chains.

The Development Finance Corporation gives the United States the ability to take a stake in overseas investments. The United States should work with major western financial institutions to strategize large-scale quality development for projects that lack commercial interest and may be courted by authoritarian regimes.

The Export-Import Bank could also potentially play a role by adopting secure supply chain standards that would have to be met in order to obtain financing. The role of the U.S. Agency for International Development would be critical as the primary agency tasked with foreign aid. Finally, the various rule of law programs managed by the Department of State Bureau of International Narcotics and Law Enforcement can be retooled to take into consideration the importance of supply chain security. Already, many of these programs aim to counter corruption in customs.

Implementation of the Blue Dot Network should be prioritized and expanded. The network represents the most robust effort yet to prioritize quality, rules-based development over the poor-quality, corrosive development on offer by the China in the form of the Belt & Road Initiative. The Blue Dot Network shares the certification-based approach of the SSCI and “certified secure” designations of the guidelines and standards aspects of the recommendations. The Blue Dot Network itself is a certification framework, which provides a “blue dot” for quality development projects.

The United States also should use its influence at the World Bank, the International Monetary Fund, and other multilateral development organizations to prioritize the development of alternative markets based in the rule of law. The goal would be for development projects to help countries strengthen their systems to such an extent that they can join in the structures being built to create and uphold secure supply chains.

d. Global Corruption & Authoritarian Companies

Global corruption and supply chain security are inextricably linked. In particular, the rise of global companies that can be manipulated in the service of authoritarian regimes is undermining an even playing field based on the rule of law. While U.S. companies and other companies based in countries that respect the rule are legally obligated not to pay bribes abroad, China and Russian companies, for example, are encouraged by their governments to do so to gain a competitive edge.

The recent 2020 Transparency International Exporting Corruption index that tracks the enforcement of foreign bribery laws found that only four countries—the United States, the United Kingdom, Switzerland, and Israel—were enforcing their laws under the OECD Anti-Bribery Convention to prevent their companies from paying bribes abroad.⁴⁸ This constitutes a serious supply chain risk.

The United States can use its membership in the treaties that make up the international anti-corruption law architecture, to push for stronger enforcement, especially as concerns corruption in supply chains. Ideally, this would culminate in a set of informal and formal agreements between democratic states for the rapid tracing and persecution of corruption. This is of particular importance given it is Chinese policy via the Belt & Road Initiative and other government initiatives to corrupt supply chains.⁴⁹

The United States can also make anti-corruption a central part of its foreign policy. Although the topic features in many initiatives, it has not gotten the prioritization it deserves given its importance in securing supply chains. A Helsinki Commission-supported piece of legislation, the Countering Russian and Other Overseas Kleptocracy (CROOK) Act, would begin to address this by mandating anti-corruption points of contact at every U.S. embassy.⁵⁰ This would reflect the UK Serious and Organized Crime Network (SOCnet), a new initiative of the UK to staff its embassies with anti-corruption interlocutors. SOCnet has been a resounding success for the UK, enhancing the country's presence in anti-corruption circles and elevating anti-corruption in their foreign policy.

a. Inter-Parliamentary Efforts

Inter-parliamentary efforts represent a strong avenue to begin a process of prioritization and change. There are numerous parliamentary outlets and groups that could push secure supply chains forward. Legislators that make up these bodies have the power at home to pass the laws agreed to be necessary. Their combined efforts can also exert pressure on governments to undertake suggested initiatives. One grouping is the Interparliamentary Alliance on China, which has been active recently in pushing back on Chinese efforts to use its economic influence to exert pressure on other countries.

Another grouping is the OSCE Parliamentary Assembly. This 323-member parliamentary grouping votes annually on resolutions by majority vote that can then impact policymaking in the 57 countries of the OSCE, from Vancouver to Vladivostok. As previously mentioned, the OSCE already embraces a comprehensive definition of security, and it is a known forum where leading democratic, free-market economy countries can confront authoritarian countries that can and do manipulate their economic levers for less-than-benign political purposes.

Thanks largely to the Helsinki Commission, the U.S. Congress has actively engaged and helped shape the OSCE Parliamentary Assembly since its inception in 1991. As a result, the Assembly has already adopted resolutions on combatting corruption, respecting rule of law and increasing transparency in the extractive industries, and one could imagine in our current environment a resolution on secure supply chains, laying out and seeking agreement on the principles of "certified secure" or SSCI. Such a resolution could build the groundwork for political commitments at the intergovernmental OSCE-level.

Domestic U.S. Law and Executive Action (Third Tier Response)

The United States finds itself momentarily behind the curve in best practices to ensure that critical supply chains are secure. The United States should work to lead the way in legislating and enforcing the policies it hopes to see around the world. This legislation would be wide-ranging, encompassing anti-corruption and transparency legislation, legislation affecting the organization and duties of companies and corporate boards, and finally legislation affecting tax and trade. The primary committees of jurisdiction would be the House Financial Services Committee and Senate Banking Committee, in addition to the House Ways & Means Committee and the Senate Finance Committee.

The executive branch would also play a major role with its enforcement and procurement functions. The executive branch can lead by example in the creation of secure supply chains by adopting transparency, responsibility, accountability, and resiliency in its procurement process. It also can use various sanctions and export controls enforcement mechanisms strategically to generate behavioral change in those countries non-compliant with internationally recognized guidelines, standards, and

law on secure supply chains. In the most extreme case, it could cut off U.S. market access to the countries that are the most consistent violators.

1. LEGISLATIVE BRANCH

i. Anti-Corruption & Transparency Legislation

The U.S. legislative framework should also reflect the four criteria of transparency, responsibility, accountability, and resilience. Congress recently passed beneficial ownership transparency legislation, which would prevent U.S. shell companies from being abused by those who would use them to undermine supply chain security. The executive branch must now enforce the new law. A Financial Accountability and Corporate Transparency (FACT) Coalition study shows how U.S. shell companies are threatening the security of supply chains.⁵¹

Another critical piece of anti-corruption legislation is the Foreign Extortion Prevention Act, which would criminalize the demand side of bribery, enabling the Department of Justice to prosecute those who attempt to extort U.S. companies. This would provide companies with a critical means to resist the bribery that corrodes supply chains as well as IP theft, which is often extorted by authoritarian countries in exchange for market access.⁵²

Finally, the United States should implement anti-money laundering requirements on professional services that provide the backbone for both money laundering and illicit supply chain operations. These professional services firms include lawyers, real estate professionals, consultants, accountants, and others.

ii. Company Mandates & Requirements for Corporate Boards

The United States can mandate—and previously has mandated—requirements for publicly listed companies under the Securities Exchange Act.⁵³ In the case of secure supply chains, the United States should make the quality of resiliency a requirement

for public listing. Mandating a diversification and resilience plan could mitigate concerns by companies that leaving China's market will put them at a competitive disadvantage. This mandate would include that boards plan for supply chain resiliency and specifically have at least one secondary market to ensure that supply chains cannot be put under authoritarian pressure. Other possible mandates to fight supply chain risks could include reporting of instances of IP theft or cyberattack and commercial ties to Chinese companies on the Commerce Department's Entity List or DOD list of People's Liberation Army (PLA) firms operating in the United States.

The United States can also mandate that boards develop plans in case of severe supply chain disruption—be it the case of a second pandemic or another form of disruption. Similar to the “China plus one” commitment to prevent authoritarian pressure, this requirement would focus on enhancing supply chain resiliency via diversification.

iii. Tax Policy

The United States should be ready to use tax policy to incentivize companies to move out of authoritarian jurisdictions where supply chains are in danger. At the same time, the country and its allies should be very careful about provoking a race-to-the-bottom and a push to on-shore. Rather, the United States should seek to provide incentives to bring production and supply chains into the sphere of countries compliant with the SSCI.

iv. Explicit Extraterritorial Jurisdiction

Given the centrality and openness of the U.S. financial system and economy, many transactions that occur touch U.S. correspondent banks or some other space of the U.S. market at some point. Courts have continuously ruled that this grants U.S. law enforcement extraterritoriality in these cases, most recently in the case of the bribery of FIFA officials that happened outside the country but

touched the financial system via wire fraud.⁵⁴

However, in other cases, U.S. extraterritoriality has been limited by U.S. courts. For the Foreign Corrupt Practices Act, the critical U.S. anti-foreign bribery law, the case law is thin; nearly all cases are resolved outside of court or via a mechanism such as deferred prosecution agreements. It is hard to predict how courts would decide to rule if a case actually was brought to court.

As such, it is becoming jurisprudentially ever more important that Congress legislate with explicit reference to “extraterritoriality,” as has been done with the bipartisan Rodchenkov Anti-Doping Act. The Rodchenkov Act was spearheaded by Helsinki Commission Co-Chairman Sen. Roger Wicker (MS) and Commissioner Sen. Sheldon Whitehouse (RI) in the Senate and former Commissioners Rep. Sheila Jackson Lee (TX-18) and Rep. Michael Burgess (TX-26) in the House of Representatives. It recently completed its course through Congress and is on its way to the President for signature. The bill defines doping as a fraudulent act and would criminalize it in international competitions when conducted by transnational criminals and corrupt administrators, government officials, coaches, and doctors (non-athletes).⁵⁵ By legislating explicit extraterritoriality, there will be no question in court as to the law’s application.

2. EXECUTIVE BRANCH

i. Federal Procurement

The United States has a rather poor track record in ensuring the security of federal procurement outside of defense technology. In particular, buildings leased by the General Services Administration (GSA) for national security-sensitive agencies such

as the FBI and the DEA have been found to be foreign-owned because GSA was not required to collect beneficial ownership information.⁵⁶

The federal government can immediately begin the collection of beneficial ownership from its suppliers and use its purchasing power to only purchase from those suppliers “certified secure,” once this framework is in place. Using purchasing power in this way will also provide an initial incentive for businesses to certify.

ii. Public-Private Partnerships & Country Dialogues

The executive branch can better work with the private sector to share data and intelligence on illicit supply chains and should find ways to overcome the challenge of providing information back to the private sector. It should not be a one-way street. A strong model for this is the British Joint Money Laundering Intelligence Taskforce, which brings the representatives of UK law enforcement with the UK banking establishment together on a weekly basis to share face-to-face information and suspicions. Information Sharing and Analysis Centers (ISACs) provide a strong example for critical infrastructure.⁵⁷

Formal exchanges of information back and forth are a critical way to stay on top of those attempting to undermine secure supply chains.⁵⁸ Though a “Fin-CEN Exchange” framework designed to facilitate similar exchange exists in the United States, it has thus far not been built out to do so. There has been greater success with back and forth exchange at the State Department’s Overseas Security Advisory Council, which may be able to serve as an effective U.S. model.⁵⁹ One could imagine similar

exchanges beyond money laundering that involve industries beyond banks—a Joint Counterfeiting Intelligence Taskforce or a Joint IP Theft Intelligence Taskforce, for example.

High-level bilateral dialogues also are powerful ways for the United States to engage with other countries and signal to the global private sector

an effort to find common ground. Engaging in “high-level dialogues on secure supply chains” can generate an atmosphere for further engagement. These dialogues could be entered into as part of the SSCI process.

Conclusion

COVID-19 has dramatically reshaped the world, but it will not be the last such shock that puts the current fragile system of insecure supply chains to the test. The next shock may be even more severe and unravel the entire system, especially if it is the result of targeted authoritarian action against the United States or its allies. The COVID pandemic has ultimately been blunted by the human incentive to cooperate on science and health, but that will be lost in the case of a shock imposed by conflict. It is critically important that the United States begin to rethink the current supply chains systems that so freely enables authoritarian states to take advantage of countries, companies, and other actors seeking to adhere to the rule of law.

Supply chains will only become more important for U.S. national security. The Biden administration should incorporate this platform into its national security strategy. No matter what path is followed and recommendations enacted, the central tenet should be to work closely with like-minded countries that also seek to uphold global rule of law and supply chains that are transparent, responsible, accountable, and resilient. The United States cannot ensure secure supply chains on its own—the task of doing so is an inherently global one. But it is one based deeply in U.S. values. The vision of an open world of free commerce bolstered by the rule of law could not be more American. It is a vision worth striving for.

Endnotes

- 1 Andrew Jacobs, Matt Richtel, and Mike Baker, "'At War With No Ammo': Doctors Say Shortage of Protective Gear Is Dire," *New York Times*, March 19, 2020, <https://www.nytimes.com/2020/03/19/health/coronavirus-masks-shortage.html>.
- 2 Sinéad Baker, "Spain is sending back faulty coronavirus tests to China that were supposed to be replacements for the first faulty batch," *Business Insider*, April 22, 2020, <https://www.businessinsider.com/coronavirus-spain-returns-second-batch-faulty-tests-bioeasy-china-2020-4>.
- 3 U.S. Library of Congress, Congressional Research Service, *COVID-19: China Medical Supply Chains and Broader Trade Issues*, by Karen M. Sutter, Andres B. Schwarzenberg, and Michael D. Sutherland, R46304 (2020). <https://crsreports.congress.gov/product/pdf/R/R46304>.
- 4 Tim Lister, Sebastian Shukla and Fanny Bobille, "Coronavirus sparks a 'war for masks' as accusations fly," *CNN*, April 3, 2020, <https://www.cnn.com/2020/04/03/europe/coronavirus-masks-war-intl/index.html>.
- 5 John Ruwitch, "Theory That COVID Came From A Chinese Lab Takes on New Life in Wake of WHO Report," *NPR*, March 31, 2021, <https://www.npr.org/2021/03/31/983156340/theory-that-covid-came-from-a-chinese-lab-takes-on-new-life-in-wake-of-who-repor>
- 6 Felix Richter, "China Is the World's Manufacturing Superpower," *Statista*, February 18, 2020, <https://www.statista.com/chart/20858/top-10-countries-by-share-of-global-manufacturing-output/>.
- 7 Thomas Palley, "The Perils of China-Centric Globalization," *The Journal of International Security Affairs*, (December 18, 2013): 11-14.
- 8 "2015 GIPC International IP Index Fact Sheet," U.S. Chamber of Commerce, last modified February 4, 2015, <https://www.uschamber.com/issue-brief/2015-gipc-international-ip-index-fact-sheet>.
- 9 OECD/EUIPO (2019), *Trends in Trade in Counterfeit and Pirated Goods*, Illicit Trade, OECD Publishing, Paris, <https://doi.org/10.1787/g2g9f533-en>.
- 10 OECD (2017), *Trade in Counterfeit ICT Goods*, Illicit Trade, OECD Publishing, Paris, <https://doi.org/10.1787/9789264270848-en>.
- 11 The National Bureau of Asian Research, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (2017). https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.
- 12 Executive Office of the President, The United States Trade Representative, 2020 *Special 301 Report* (April, 2020), https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf.
- 13 Executive Office of the President, The United States Trade Representative, *2019 Review of Notorious Markets for Counterfeiting and Piracy* (2019),
- 14 World Justice Project, *Rule of Law Index* (2020), https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2020-Online_0.pdf.
- 15 Homeland Security, U.S. Customs and Border Protection, *Intellectual Property Rights: Fiscal Year 2019 Seizure Statistics* (2019), <https://www.cbp.gov/sites/default/files/assets/documents/2020-Sep/FY%202019%20IPR%20Statistics%20Book%20%28Final%29.pdf>.
- 16 OECD, *Illicit Trade in a time of crisis* (April, 2020), <http://www.oecd.org/gov/illegal-trade/oecd-webinar-illicit-trade-time-crisis-23-april.pdf>.
OECD, *Trade in Fake Medicines at the Time of the COVID-19 Pandemics* (June, 2020), <http://www.oecd.org/gov/illegal-trade/oecd-webinar-illicit-trade-time-crisis-23-april.pdf>.
- 17 OECD/EUIPO (2020), *Trade in Counterfeit Pharmaceutical Products*, Illicit Trade, OECD Publishing, Paris, <https://doi.org/10.1787/a7c7e054-en>.

-
- 18 Walt Bogdanich, "Heparin Find May Point to Chinese Counterfeiting," *New York Times*, March 20, 2008, <https://www.nytimes.com/2008/03/20/health/20heparin.html>.
 - 19 Jonathan Ponciano, "Biden Secretary of State Condemns China's 'Acts of Genocides' Against Muslim Uyghurs," *Axios*, April 11, 2021, <https://www.forbes.com/sites/jonathanponciano/2021/04/11/biden-secretary-of-state-condemns-chinas-acts-of-genocide-against-muslim-uyghurs/?sh=6140cc4850ca>.
 - 20 U.S. Department of State, *Xinjiang Supply Chain Business Advisory* (July, 2020), <https://www.state.gov/xinjiang-supply-chain-business-advisory/>.
 - 21 Jill Disis and Philip Wang, "'US sanctions 11 Chinese companies over human rights abuses in Xinjiang,'" *CNN*, July 21, 2020, <https://www.cnn.com/2020/07/21/business/us-sanctions-china-companies-xinjiang-intl-hnk/index.html>.
 - 22 OECD (2018), *Trade Facilitation and the Global Economy*, OECD Publishing, Paris, 30, <https://doi.org/10.1787/9789264277571-en>.
 - 23 Laurens Cerulus, "Meet the Huawei of airport security," *Politico*, February 11, 2020, <https://www.politico.eu/article/beijing-scanners-europe-nuctech/>.
 - 24 Rohan Abraham, "US accuses Chinese screening tech firm Nuctech of passing passenger info to Beijing," *Politico*, July 3, 2020, <https://economictimes.indiatimes.com/magazines/panache/us-accuses-chinese-screening-tech-firm-nuctech-of-passing-passenger-info-to-beijing/articleshow/76769001.cms>.
 - 25 Rogier Creemers, Mingli Shi, Lauren Dudley, and Graham Webster, "China's Draft 'Personal Information Protection Law,'" *New America*, October 21, 2020, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/>.
 - 26 U.S. Department of State, *The Clean Network* (2020), <https://www.state.gov/the-clean-network/>.
 - 27 "Foreign Meddling in The Western Balkans," Commission on Security and Cooperation in Europe, last modified January 30, 2018, <https://www.csce.gov/international-impact/events/foreign-meddling-western-balkans>.
 - 28 Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," Council on Foreign Relations, last modified January 28, 2020, <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>.
 - 29 "Chairman Risch Opening Statement at Hearing on Advancing U.S. Engagement and Countering China in the Indo-Pacific and Beyond," Committee on Foreign Relations, U.S. Senate, last modified September 17, 2020, <https://www.foreign.senate.gov/press/chair/release/chairman-risch-opening-statement-at-hearing-on-advancing-us-engagement-and-countering-china-in-the-indo-pacific-and-beyond>.
 - 30 U.S. Library of Congress, Congressional Research Service, *World Trade Organization: Overview and Future Direction*, by Cathleen D. Cimino-Isaacs, Rachel F. Fefer, and Ian F. Fergusson, R45417 (2020). <https://www.crs.gov/Reports/R45417>.
 - 31 Matthew Page and Jodi Vittori, Carnegie Endowment for International Peace, *Dubai's Role in Facilitating Corruption and Global Illicit Financial Flows* (July, 2020), <https://carnegieendowment.org/2020/07/07/dubai-s-role-in-facilitating-corruption-and-global-illicit-financial-flows-pub-82180>.
 - 32 "Asset Recovery in Eurasia," Commission on Security and Cooperation in Europe, last modified February 13, 2019, <https://www.csce.gov/international-impact/events/asset-recovery-eurasia>.
 - 33 U.S. Department of State, *Letter from Under Secretary Keith Krach to the Governing Boards of American Universities*, by Keith Krach (August, 2020), <https://www.state.gov/letter-from-under-secretary-keith-krach-to-the-governing-boards-of-american-universities/>.
 - 34 "EU foreign investment screening mechanism becomes fully operational," The European Commission, last modified October 9, 2020, <https://trade.ec.europa.eu/doclib/press/index.cfm?id=2187>.

- 35 "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency, accessed November 23, 2020, <https://www.cisa.gov/critical-infrastructure-sectors>
- 36 U.S. Library of Congress, Congressional Research Service, *COVID-19: China Medical Supply Chains and Broader Trade Issues*, by Karen M. Sutter, Andres B. Schwarzenberg, and Michael D. Sutherland, R46304 (2020). <https://crsreports.congress.gov/product/pdf/R/R46304>.
- 37 Such standards include, but are not limited to: <https://www.iso.org/standard/44641.html>; <https://www.iso.org/iso-31000-risk-management.html>; <https://www.oecd.org/corporate/mne/GuidanceEdition2.pdf>.
- 38 The Extractive Industries Transparency Initiative, accessed November 23, 2020, <https://eiti.org/>. One of the major pieces of implementing legislation for U.S. fulfillment of EITI standards was the Cardin-Lugar provision of Dodd-Frank, which the U.S. Helsinki Commission was instrumental in passing. This provision requires that listed companies disclose amounts paid to foreign countries to access natural resources.
- 39 For example, the current C-TPAT program could be expanded to include economic security threats.
- 40 Inspiration here could be taken from U.S. CBP Trusted Trader and Trusted Traveler programs: <https://ctpat.cbp.dhs.gov/trade-web/getCtpat.html?modelNumber=12534&tabNumber=5>
<https://www.cbp.gov/travel/trusted-traveler-programs>.
- 41 U.S. Department of State, *Launch of the U.S.-EU Dialogue on China* (October, 2020), <https://www.state.gov/launch-of-the-u-s-eu-dialogue-on-china/>.
- 42 Tom Ginsburg, "How Authoritarians Use International Law," *Journal of Democracy* 31, no. 4 (October 2020): 44-58.
- 43 Renee A. Latour, "First-Ever Anticorruption Chapter Included in USMCA," *The National Law Review* 10, no. 37 (February 2020).
- 44 "Anticorruption," Executive Office of the President, The United States Trade Representative, *The Agreement between the United States of America, the United Mexican States, and Canada*. (July, 2020), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/27_Anticorruption.pdf.
- 45 "Curbing Corruption Through Corporate Transparency and Collaboration," Commission on Security and Cooperation in Europe, last modified May 29, 2019, <https://www.csce.gov/international-impact/events/curbing-corruption-through-corporate-transparency-and-collaboration>.
"Incorporation Transparency: The First Line of Financial Defense," Commission on Security and Cooperation in Europe, last modified October 4, 2018, <https://www.csce.gov/international-impact/publications/incorporation-transparency>.
"Combating Kleptocracy With Incorporation Transparency," Commission on Security and Cooperation in Europe, last modified October 3, 2017, <https://www.csce.gov/international-impact/events/combating-kleptocracy-incorporation-transparency>.
- 46 David Pegg, "British Virgin Islands commits to public register of beneficial owners," *The Guardian*, October 1, 2020, <https://www.theguardian.com/world/2020/oct/01/british-virgin-islands-commits-public-register-beneficial-owners-tax-haven>.
- 47 "Build Act," USAID, last modified December 12, 2018, <https://www.usaid.gov/work-usaid/private-sector-engagement/build-act>. U.S. Department of State, *Blue Dot Network*, <https://www.state.gov/blue-dot-network/>.
- 48 "Exporting Corruption," Transparency International, accessed November 23, 2020, <https://www.transparency.org/en/projects/exporting-corruption>.
- 49 Elaine K. Dezenski, "Below the Belt and Road," Foundation for Defense of Democracies, last modified May 6, 2020, <https://www.fdd.org/analysis/2020/05/04/below-the-belt-and-road/>.
- 50 Abigail Bellows, "Revamping U.S. Anti-Corruption Assistance," *The American Interest*, June 15, 2020, <https://www.the-american-interest.com/2020/06/15/the-case-for-the-crook-act/>.

-
- 51 David M. Luna, "Anonymous Companies Help Finance Illicit Commerce and Harm American Businesses and Citizens," The Fact Coalition, last modified May 2019, <https://thefactcoalition.org/report/anonymous-companies-help-finance-illicit-commerce-and-harm-american-businesses-and-citizens/>.
 - 52 "Anti-Kleptocracy Initiatives Supported by The Helsinki Commission," Commission on Security and Cooperation in Europe, last modified January 23, 2020, <https://www.csce.gov/international-impact/anti-kleptocracy-initiatives-supported-helsinki-commission>.
 - 53 "Requirements for Public Company Boards," The Fact Coalition, last modified May 2015, https://www.weil.com/~media/files/pdfs/150154_pcag_board_requirements_chart_2015_v21.pdf.
 - 54 Robert J. Anello and Richard F. Albert, "FIFA Decision Confirms Long Arm of Honest Services Fraud," *Law.com*, March 8, 2017, <https://www.law.com/newyorklawjournal/2020/08/12/fifa-decision-confirms-long-arm-of-honest-services-fraud/>.
 - 55 Paul Massaro, "Getting Off the Sidelines," *The American Interest*, February 18, 2019, <https://www.the-american-interest.com/2019/02/18/getting-off-the-sidelines/>.
 - 56 U.S. Government Accountability Office, *Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners*, GAO-17-195 (Washington, DC, 2017), accessed November 23, 2020, <https://www.gao.gov/assets/690/681883.pdf>.
 - 57 "About ISACs," National Council of ISACs, accessed November 23, 2020, <https://www.nationalisacs.org/about-isacs>. "Presidential Decision Directive 63: Protecting America's Critical Infrastructures," Homeland Security Digital Library, last modified February 8, 1999, <https://www.hsdl.org/?abstract&did=3544#:~:text=Presidential%20Decision%20Directive%2063%20is%20the%20culmination%20of,new%20structure%20to%20deal%20with%20this%20important%20challenge>.
 - 58 "Future of Financial Intelligence Sharing," Global Coalition to Fight Financial Crime, last modified August 2020, <https://www.gcffc.org/wp-content/uploads/2020/08/FFIS-Report-Five-Years-of-Growth-of-Public-Private-Partnerships-to-Fight-Financial-Crime-18-Aug-2020.pdf>.
 - 59 "Who We Are," Overseas Security Advisory Council, U.S. Department of State, accessed November 23, 2020, <https://www.osac.gov/About/WhoWeAre>.

One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, N.W.
Washington, DC 20004-3027

 www.wilsoncenter.org
 wwics@wilsoncenter.org
 facebook.com/woodrowwilsoncenter
 [@thewilsoncenter](https://twitter.com/thewilsoncenter)
 202.691.4000